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: Thursday, August 20, 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

PAGE NO.

August 19, 2026

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

PAGE NO.

August 20, 2026

LIST OF EXHIBITS

LIST OF UNDERTAKINGS

LIST OF UNDERTAKINGS

Halifax, Nova Scotia

--- Upon commencing on Tuesday, August 20, 2026 at 9:00 a.m.

THE CHAIR: Good morning, everyone. Any preliminary matters before we resume?

Mr. Roberts?

MR. MAHODY: Mr. Chair, I'm sorry, if I may.

THE CHAIR: Yes.

MR. MAHODY: Just for the Panel's information, Tricia Ralph, who will be testifying later today, has joined us in the public gallery so the Panel's aware of that. And Mr. Kayter has just stepped out; he has to attend to a matter, but he is fine with us proceeding.

THE CHAIR: Thank you, Mr. Mahody.

MR. ROBERTS: Just waiting for Mr. Mollard. There we go.

Thank you.

Good morning, Mr. Mollard.

MR. MOLLARD: Good morning.

MR. ROBERTS: You're Ed Mollard, and you're currently employed as ---

THE CHAIR: Sorry, Mr. Roberts. I'll just affirm him.

ED MOLLARD, Solemnly Affirmed:

THE CHAIR: Thank you.

Sorry, Mr. Roberts.

MR. ROBERTS: No. Thank you.

EXAMINATION ON QUALIFICATIONS BY MR. ROBERTS

Q. Mr. Mollard, you're employed as an associate consultant with InterGroup in Winnipeg?

A. That is correct.

Q. And you've been employed in that capacity since January of 2026?

A. Yeah. I did a couple of project-specific contracts in 2025, but my formal arrangement as an associate began in January of 2026.

Q. Okay. Thank you.

And you were retained by the Consumer Advocate in this proceeding to prepare a report on the impact of the 2025 cyberattack on Nova Scotia Power on the customers of the utility?

A. That is correct.

Q. And your report has been received in evidence in this proceeding as Exhibit N-13?

A. Yes.

Q. Okay. Now, just -- you have not yourself appeared before this Board in the past?

A. No, this is my first appearance.

Q. Okay. I'm going to, then, just briefly review your background.

Attached to your report, and it's after page 24, is an appendix which briefly sets out your résumé.

A. Yes.

Q. And it states that you received your Certified General Accountant designation in 1993.

A. Correct.

Q. And for a period of nine years following that, you worked for the Office of the Auditor General of Canada?

A. Yes.

Q. After that point, you were employed for a period of time by the Government of the Northwest Territories?

A. Yes.

Q. And from 2001 until 2023, you were employed by Yukon Energy.

A. That is correct.

Q. And between the years 2006 and 2023, you served as Vice President, Chief Financial Officer of Yukon Energy with a number of different responsibilities.

A. Correct.

Q. Okay. And I'm just going to refer back -- at page 1 of the report, you provide a brief -- or some detail on your work with Yukon Energy. You were senior executive responsible for revenue requirement and rate-related matters before the territorial regulator?

A. That is correct.

Q. And this, again, is in your

capacity as Vice President, Chief Financial Officer.

A. Yes.

Q. And as well for a number of years during that time, you also acted as the Privacy Officer for Yukon Energy, in accordance with the provisions of *PIPEDA*, the federal legislation that also applies to Nova Scotia Power.

A. Yes.

MR. ROBERTS: Mr. Chair, at this point I'd like to request that Mr. Mollard -- or I'm sorry, I should just make one more reference.

BY MR. ROBERTS:

Q. You have -- although you've never appeared before this Board, you were previously qualified to provide expert opinion evidence before the Alberta Utilities Commission?

A. That is correct.

Q. And that was in November of 2025?

A. Yes.

Q. And you gave evidence on behalf of the Consumer Advocate in that proceeding?

A. Yes.

Q. Okay.

MR. ROBERTS: I would like, then, Chair, to request that Mr. Mollard be qualified as an expert witness, able to give opinion evidence on the regulation of electrical utilities, including in matters related to the management of personal information pertaining to customers of the utility and the application of privacy policies.

THE CHAIR: Any questions on qualifications?

MR. CLARKE: Mr. Chair, I have some questions for Mr. Mollard.

THE CHAIR: Anyone else have questions?

Go ahead, Mr. Clarke.

CROSS-EXAMINATION ON QUALIFICATIONS BY MR. CLARKE

Q. Mr. Mollard, good morning to you.

A. Good morning.

Q. You are educated and trained as an accountant; is that correct?

A. Yes, sir.

Q. You're not a lawyer.

A. No, I am not.

Q. Prior to your current role, you worked for Yukon Energy as Vice President, Finance, and Chief Financial Officer. Do I have that right?

A. Yes.

Q. And when did you hold the position of Privacy Officer?

A. Challenging my memory a bit, but I believe it was roughly for a three-year period between 2016 and 2019.

Q. And do I have it right that the role of Privacy Officer was wrapped into your position as

CFO?

A. Correct.

Q. Mr. Mollard, in your work experience you've never led a security breach investigation before, you have?

A. I did have at least one breach that I had to deal with as Privacy Officer with Yukon Energy Corporation. It was, just to be clear, a one-off customer event. It wasn't near the scope of what we're talking about here, but I did have to deal with the Privacy Officer in Yukon with respect to a client information breach.

Q. Okay. Would you describe your involvement in that incident as leading a security breach investigation?

A. Well, I had the corporate responsibility for representing the company in respect of the breach investigation. I'm not sure what you mean by "leading". There was myself and one other staff support

from Yukon Energy dealing with the Privacy Officer on the breach.

Q. I'm going to suggest that you've never advised an organization in real time respecting credit monitoring or identity protection. Is that correct?

A. That's a fair statement.

Q. And you've never directed notification efforts involving hundreds of thousands of individuals. Would that be correct?

A. Yes.

Q. And you've never overseen a ransomware response involving current and former customers?

A. No. We had a ransomware event for one employee on one corporate machine, but it did not have implications for customers.

Q. And you don't have any professional certifications respecting cybersecurity, do

you, Mr. Mollard?

A. No, I do not.

Q. And you don't have any professional certificates in the area of privacy generally?

A. No.

Q. The one time that you acted as an expert before the Alberta Utilities Commission, what area were you offering evidence?

A. That was a general tariff application from a utility. My primary focus in that regard was with respect to operational expenses.

Q. Thank you, Mr. Mollard. I have no other questions.

THE CHAIR: Any objections to qualifications?

Okay, Mr. Roberts, he's so qualified.

MR. ROBERTS: Thank you.

DIRECT EXAMINATION BY MR. ROBERTS

Q. Mr. Mollard, as we stated at the outset, you've provided Exhibit N-13 as your report in this matter. Are you the principal author of that report?

A. I am.

Q. And is the information contained in your report true to the best of your knowledge and belief?

A. Yes.

Q. Do you adopt your report as your evidence in this proceeding?

A. I do.

Q. Do you wish to make any corrections to your report?

A. No.

Q. Okay. Now, since you prepared your report, Nova Scotia Power has filed rebuttal evidence, which is Exhibit N-17, and you've reviewed N-17?

A. I have.

Q. Does the rebuttal evidence of Nova Scotia Power cause you to change any of the recommendations you've made in your report?

A. It does not.

MR. ROBERTS: Okay. Mr. Chair, Mr. Mollard is ready for cross-examination.

THE CHAIR: My understanding is that no parties other than Nova Scotia Power has questions for Mr. Mollard?

MR. CLARKE: Mr. Chair, we have no questions with respect to the content of the opinion.

THE CHAIR: Okay. Sorry, Ms. Rudderham?

MS. RUDDERHAM: The Industrial Group does, and I believe ---

MS. MacADAM: I have one.

[9:10:50] **THE CHAIR:** Okay. So we'll start with the Small Business Advocate.

CROSS-EXAMINATION BY MS. MacADAM

Q. Good morning, Mr. Mollard. Melissa MacAdam on behalf of the Small Business Advocate.

Could we bring up Exhibit N-13, which is your evidence, at page 21, specifically Recommendation 9?

So in this recommendation, just above the specific recommendation itself, you talk about the issue of potential future liability damages that could occur after the expiry of the credit monitoring period, and then in your recommendation you recommend NSP be directed to examine longer-term options for credit monitoring.

And I'm just wondering, do you have any specific options that you're referring to with respect to the longer-term options?

A. Certainly, yeah. I mean, I think in the report we talked about, you know, that -- just backing up, NSPI has generously offered credit monitoring

services to be paid through TransUnion. They have arrangement with that company.

When I say longer-term options, we also mention that we feel that customers who already have credit monitoring should be compensated by NSPI because they've one out on their own and done that. So that would be sort of the two options, either a direct offer from NSPI to customers for credit monitoring or the customers would have options to secure their own credit monitoring.

Q. Okay. So no specifically dealing with after the expiry of the credit monitoring period?

A. No, Ma'am.

Q. Okay. And I'm just wondering, are you familiar with a credit freeze?

A. I am not.

Q. Thank you. That's my question.

THE CHAIR: Thank you.

Industrial Group?

MS. RUDDERHAM: I believe the public

intervenor also has questions.

MS. AKCAKIRYAN: We have a question.

THE CHAIR: All right. Come on up. Sorry.

MR. CLARKE: Mr. Chair, we may have some questions.

THE CHAIR: I'll come back to you.

MR. CLARKE: Thank you.

CROSS-EXAMINATION BY MS. AKCAKIRYAN

Q. Good morning, Mr. Mollard.

A. Good morning.

Q. Canada has two main credit bureaus, TransUnion and Equifax. Is that your understanding?

A. Yes.

Q. And lenders don't necessarily report to both, is that right?

A. That's my understanding, yes.

Q. Okay. So something can appear on an Equifax file that never appears on a TransUnion file. Would that be correct?

A. To the best of my understanding, yes.

Q. Okay. But Nova Scotia Power is offering monitoring for only the TransUnion credit monitoring; is that correct?

A. That's my understanding, yes.

Q. Okay. So a fraudulent account reported only to Equifax would not necessarily trigger an alert on a TransUnion file?

A. As I understand it. Again, my understanding is based largely on the testimony from yesterday about how this works. I'm not an expert in credit monitoring.

Q. Okay. Thank you for that.

Can we turn to PDF page 21 of Exhibit N-13, please?

So you go on to say that:

> ...credit monitoring [services] does not fully resolve potential future liability damages which could occur after the expiry of the credit monitoring period.

The monitoring period here expires after five years, but the risk of a stolen SIN being misused doesn't expire with it. Is that correct?

A. Yes.

Q. So someone's SIN could be misused

in the sixth year, say?

A. Yeah, that's my understanding. It can happen.

Q. Okay. And is that continuing risk why you recommended Nova Scotia Power examine longer monitoring term options?

A. Yeah, I mean, this is clearly a subjective evaluation on one level in the sense that the regulation doesn't prescribe a number for us. Two years used to be acceptable at one time. It's now, I think, generally accepted that five years is more the standard, and while there's not a large body of evidence to support 10 years at this point, our research tended to lead us to believe that longer periods of time are on the horizon.

Certainly, I mean, I had a brief look at the new federal legislation, and I would say the onus on stewards of customer data or private information is going to increase, not decrease. So I would say that recommendation reflects the trend in the industry for

longer responsibility for this.

Q. Okay. Thank you.

And you've also worked in the regulated electricity industry for 25 years?

A. Yes.

Q. Over those 25 years, the cyber threat facing utilities has grown. Would you say that that's accurate?

A. Yes.

Q. Would you also say that utilities are attacked more often today than, say, a decade ago?

A. Yes. You know, as an anecdotal reference, I mean, I remember I had IT reporting to me and I remember when I took over the portfolio in the late teens, our IT manager had been there for about 15 years, and we talked a lot about the level of attacks that they experience daily on the systems, and it's much more higher.

And to the experts who testified

yesterday, Ms. Valdetero, the hacks are much more sophisticated. We used to talk about teenagers in parents' basements and now it's foreign powers that are very, very organized and the breaches are much more severe.

Q. Thank you for that.

And for the customers here, the harm didn't necessarily end when the attack ended. Is that correct?

A. Yeah, generally our position is that that liability continues, yes.

Q. Okay. And that's because their SINs are still out there?

A. Yes.

Q. Okay. And the fact that a monitoring package reflects what companies typically offer today doesn't necessarily end the question of what these customers should receive going forward?

A. Yes. I think we probably share

the opinion of Ms. Valdetero in the sense that credit monitoring is probably not the best solution, but to quote her, it's the best of a series of bad options. So this is what we have today.

Q. Okay. And part of the regulatory process is learning lessons from events like this?

A. Yes.

Q. Okay. And asking whether what's offered to affected customers should improve?

A. Yes.

Q. So what a utility offers customers after ---

MR. CLARKE: Excuse me. Mr. Chair, I'm reluctant to interject, but it's long been the policy of the Board that soft cross is not permitted. I suppose it's a judgment call whether this constitutes soft cross. I'm concerned that it does.

THE CHAIR: It may, but to this point, Mr. Clarke, I think the questions are quite similar to the

questions that she did ask the other expert witness as well. So in terms of consistency, I think I'm inclined to at least let her be consistent with what she's asked the other witness.

MR. CLARKE: Thank you very much.

MS. AKCAKIRYAN: Thank you.

BY MS. AKCAKIRYAN:

Q. So utility offers to customers after a breach can evolve as utilities and regulators learn from events like this one?

A. Yeah, I think we've seen that happen with respect to credit monitoring. As I said, the standard in the industry used to be two years, now it's five.

Q. Okay, thank you, Mr. Mollard, that's all of my questions.

THE CHAIR: Ms. Rudderham?

[9:19:54] **MS. RUDDERHAM:** Yes, thank you, Mr. Chair.

CROSS-EXAMINATION BY MS. RUDDERHAM

Q. Good morning, Mr. Mollard. My name is Brianne Rudderham, and I'm going to be asking you some questions this morning on behalf of the Industrial Group.

A. Good morning.

Q. Good morning. My questions relate solely to your Recommendation 12, which appears in your evidence at Exhibit N-13, page 24 or PDF page 26. I'm not sure we need to bring it up but I'm going to be asking you questions with respect to that, your conclusions made on that page and your Recommendation 12; okay?

A. Okay.

Q. Now, just to be clear, you've recommended that NSPI be directed to provide a report specifying all costs associated with the incident in as much detail as possible, and confirm that NSPI will not seek to recover those costs from customers; a fair

summary?

A. Yes.

Q. And am I correct that that recommendation is based mainly on your review of NSPI's response to CA IR-6, the confidential attachment that we've been referring to throughout the proceeding which summarizes costs in 2025 and 2026; correct?

A. Correct.

Q. Now, I want to understand your evidence. Are you saying that the figure that's provided, and I'm not trying to get into the specific amount as it's currently confidential, but are you suggesting that the figure that's there is not an accurate representation of costs arising?

A. No, I am not.

Q. Okay. So I want to understand the distinction between the phrase you're using, "All costs associated with the incident," drawing a distinction between the phrase that's been used by NSPI of

"Remediation costs arising from the incident."

A. I'm sorry; I'm not following. Could you restate, please?

Q. So you're aware that NSPI has provided an assurance that no remediation costs arising from the cybersecurity incident are going to be recovered from customers; correct?

A. Correct.

Q. So I want to understand whether you're making a distinction between that description of remediation costs versus your phrase that you're using in Recommendation 12 of all costs associated with the incident?

A. Yes, so everything that they are charging to their account with respect to the recovery exercise, we understand they have committed to not include that in revenue requirement in the future. So getting this cost report then informs the Consumer Advocate on potential areas they may want to explore in the next

revenue requirement based on what they say are their all-in costs for this event.

Q. So when you say, "All in costs," are you saying that the only costs associated are in relation to getting back or remediating?

A. Yes.

Q. Yes, okay.

A. Direct costs.

Q. Their direct costs. Would you agree that there are indirect costs as well arising from a cybersecurity incident?

A. I mean, I'm not in a position to say that today. I have no looked at their books or studied their costs or any of that required research to be able to conclude on that question.

Q. So I guess what I want to understand is, when you're recommending to have a report of all costs associated with the incident, what's the difference between that report and what was provided in

response to CA IR-6, which is confidential? So I don't want to know the specific numbers, but I just want to understand what's the difference, if it's already been remediated.

A. Yeah, to be clear, I'm not saying that there is anything missing from that report as reported. This is more future forward looking in terms of I would like to understand what they're saying is a direct cost so that if I go into the next GTA and are testing what they're claiming for their costs, is there things in there that I think should have been included in the incident and therefore not charged to ratepayers. So I'm not concluding on whether that number is right, wrong, or otherwise at this point, it's more forward looking in terms of testing a future revenue requirement.

Q. Is it fair to say that -- well, you weren't asked to assess whether that number was right, wrong, or the other; correct?

A. I was not.

Q. And there isn't currently sufficient information on the record for you to make that determination; fair?

A. Correct.

Q. Okay. Now, I just want to confirm, have you been in attendance or listening in to each day of the proceeding, so Tuesday, Wednesday?

A. Yes.

Q. Okay. Now, on Tuesday I assume you heard the Industrial Group's cross-examination of the NSPI panel and the fact that the witness declined to commit that costs related to defending or settling any class action claim would be excluded from future rate recovery; do you recall that?

A. Yes.

MR. CLARKE: Mr. Chair, I'm not sure that I agree with that summary, but certainly the panel heard the evidence, and I'll leave it to the panel to recall what evidence was given on that point.

MS. RUDDERHAM: And there's a transcript and I'm just referring to the transcript, just trying to summarize what the understanding is that the evidence was given. I'm not trying to change the evidence at all.

THE CHAIR: Okay. And I think from what I took from Mr. Clarke's comment is you're okay to proceed; he just wanted to flag that it wasn't quite consistent with what his recollection was, but I think you're good to go.

MS. RUDDERHAM: All right.

VICE CHAIR DEVEAU: It's at page 265 of the transcript if you're looking for it.

THE WITNESS: Could we call up that transcript, please?

MS. RUDDERHAM: Mr. Norwood, if you don't mind calling that up? Apologies.

And thank you, Mr. Deveau.

BY MS. RUDDERHAM:

Q. And I can just give you a moment to review that. If you need the pages turned, just let me know. I just wanted you to familiarize yourself with that.

MS. RUDDERHAM: I think if you just scroll down there, Mr. Norwood, it's the question at the very bottom, "Will NSPI commit that any costs associated with defending or settling or paying..." And then the next page there.

BY MS. RUDDERHAM:

> **Q.** ...damages in relation to that claim arising from the incident won't be recovered from ratepayers?

And then the answer there is:

> Nova Scotia Power is prepared to commit to - it already has - in that customers will not pay for costs of restoring the utility as a result of the cyberattack.

And then I asked -- scroll down, "Would these be considered remediation costs?" And I can give you a moment to just review that rather than reading it all into the record.

A. "Would these be considered restoration costs"; from that point?

MR. CLARKE: Just a second, Mr. Chair.

My recollection is Mr. Williams said we don't know yet; it's a forward issue. I thought that's what I just saw in the transcript on the previous page.

VICE CHAIR DEVEAU: At the bottom of that page there was a direct question there.

MS. RUDDERHAM: This page here it says:

> ...do I understand that means NSPI is not going to commit that none of these costs in defending, or settling or paying those damages will not be recovered from ratepayers?

If you don't mind scrolling to the next page there.

> As I said at the start of my response, Nova Scotia Power has made [a] commitment already that customers will not pay for the restoration and that those costs are intended to be incurred in 2025 and 2026.

And then it goes on:

> Is this considered a restoration cost...are

> you going to commit that none of those costs associated with this action will be recovered from ratepayers?
>
> Scroll down. So if -- there, yeah.

Rather than reading this all in, I'll give you a moment to read, it says, "So if [those are] incurred in '26 -- '25, '26, '27, then it's immaterial." And I said:

> But they could be incurred later, correct? ...that would be a discussion that we would [have to] have as part of that proceeding, [and] if we were to seek recovery of them.
>
> ...So I was asking whether you're going to commit if at any time in the future. I understand that your answer is no?
>
> My answer is...[and] I've already provided twice already, that we've made a commitment we're prepared to make.

MR. CLARKE: So I stand by my interpretation of the transcript, Mr. Chair.

MS. RUDDERHAM: And perhaps the -- I can reword my question.

BY MS. RUDDERHAM:

[9:30:22] **Q.** When NSPI was given an opportunity to commit that it would not be recovering

costs of defending or settling that claim at any time in the future, including beyond 2027, it did not to do so. That's a fair summary?

A. Honestly, I don't think I'm in a position to respond to that question.

Q. Okay.

MR. CLARKE: Mr. Chair, we know what -- we know what the questions were. We know what the answers are. There's no need for a summary, with respect.

MS. RUDDERHAM: I can move on here.

THE CHAIR: Yeah, okay. Thank you.

BY MS. RUDDERHAM:

Q. In your Recommendation 12 when you've said, "All costs associated with the incident," are you suggesting that costs associated with -- should -- in your opinion, should the costs associated with the class action, if there are any, be included in that reporting?

A. I am not in a position to respond to that question at this time.

MR. CLARKE: Mr. Chair, I understood the witness to say this wasn't something that he considered or thought of. I don't know whether we call this soft cross. It's clearly an attempt to bolster the position that the Industrial Group has tried to create, and really I don't see it as appropriate cross-examination.

THE CHAIR: Ms. Rudderham?

MS. RUDDERHAM: I've asked Mr. Mollard a number of questions about what the boundaries are of this report that he's described. I don't think it's sweetheart cross given that he said no. I'm not saying anything that was given by NSPI is incorrect. I'm just saying moving forward, there should be reporting on these costs, not making a distinction.

I don't think that that's sweetheart cross, and so I'm asking whether the costs that I've phrased here should be included in those "All costs associated with the incident." I'm not asking for him to

expand. I'm understanding what is his recommendation to report on costs associated with it.

MR. MOLLARD: And I'm just not in a position to respond. That wasn't in my scope. I was -- I was engaged to comment on the effect of this incident on customers, and we weren't tasked with doing any kind of analysis of costs, whether they were complete or accurate.

MS. RUDDERHAM: And that's fair if that's the answer. I'm not trying to ask him to expand or opine on things. I'm trying to understand what that report would include, whether it's beyond what's been provided so far or not.

THE CHAIR: Okay. So I think in his testimony -- well, you just heard the answer he gave. I think previously he said his comments were related to direct costs.

MS. RUDDERHAM: Yes.

THE CHAIR: Yes.

BY MS. RUDDERHAM:

Q. In terms of the reporting that you're recommending, can you explain for me, have you turned your mind to when or how this reporting ought to be done?

A. No, that really is the discretion of the Board.

Q. Okay. So you've not -- you have no opinion with respect to -- it's not -- you're not suggesting it should be part of, like, a compliance filing. You're just saying into the future there should be reporting. Is that what I'm understanding you're saying, without any ---

A. Yes.

Q. --- description of when and how?

A. Yes.

Q. Okay. Now, when you were retained, the scope of your review was focused mainly on matters that related to the interests of residential customers, consistent with the Consumer Advocate's

mandate; correct?

A. Correct.

Q. And Recommendation 12 doesn't specifically say shouldn't be charged to residential customers. Fair that that language isn't in there?

A. I think the language is "Recover such costs from customers."

Q. Yes. So I want to understand, when you say not to recover costs from customers, are you referring to all customers or only residential customers?

A. Well, to be fair, at this point we didn't put that much thought into it.

Yeah. Obviously, the mandate of the Consumer Advocate is with respect to residential customers; that would be our primary concern. But regardless, customers shouldn't be paying these costs.

Q. So you haven't really necessarily turned your mind to that, but you're not saying your opinion is solely related to residential customers.

You're saying customers in general; is that fair?

A. Yes.

MR. CLARKE: I think he just answered the question.

MS. RUDDERHAM: Yeah.

BY MS. RUDDERHAM:

Q. I guess -- and it's not clear in my -- in my review of your evidence. Can you explain to me why, in the absence of a finding of prudence or imprudence, why you're recommending that these costs shouldn't be borne by customers?

A. I'm sorry. That was the commitment of NSPI, to not charge customers for the direct -- for these costs.

Q. So it's just based on the assurance that's been given. You're not making -- that's just based on the assurance. Sorry.

A. I'm sorry; let's start over. Could you try the question again? I

think I got off track there.

Q. So part of your Recommendation 12 is that no costs should be recovered from customers related to or associated with the cybersecurity incident; correct? That's your recommendation.

A. Yes.

Q. So I wanted to understand why that's part of your recommendation. And I believe your answer was, "That's the assurance that's been given."

So my understanding that that is included in your recommendation in relation to the assurance that's been given. Is that correct?

A. Well, I would say, adding on to that, that generally in the regulatory space where costs like this arise that really are caused by the utility and provide no benefit to the customer, those costs are typically borne by the utility. That would be just normal regulatory practice in Canada.

MS. RUDDERHAM: Just give me a moment

to review my notes.

(SHORT PAUSE)

MS. RUDDERHAM: Those are all my questions. Thanks.

THE CHAIR: Thank you.

Mr. Clarke?

MR. CLARKE: Mr. Chair, if you'd just give me a minute.

[09:39:48] **THE CHAIR:** Sure.

(SHORT PAUSE)

MR. CLARKE: Thank you, Mr. Chair. Ms. Power has a few questions.

THE CHAIR: Thank you.

Ms. Power?

MS. POWER: Thank you, Mr. Chair.

CROSS-EXAMINATION BY MS. POWER

Q. Hi, Mr. Mollard.

A. Good morning.

Q. I just want to confirm that you would have heard evidence over the last two days that Nova Scotia Power's rates are established for 2026 and 2027 as per its last GRA?

A. Yes.

Q. And so my question is, what basis would there be for bringing any of the costs incurred in this period forward in subsequent GRAs? What's your understanding of whether that would be possible?

A. Possible. To the extent that the utility chooses to defer any of these costs incurred and bring them forward at a future application, that's generally a normal practice for a utility seeking to recover costs that are incurred in this year and a future period.

Q. And Mr. Mollard, you'd understand

that any deferral would have to be approved by the Board?

A. Yes.

Q. I want to go back to your statement that costs caused by the utility and provide no benefit to customers would be borne by the utility.

You've heard no evidence that any of these costs were caused by the utility; correct?

A. I would agree that the utility does not -- did not directly cause these costs, yes.

Q. Thank you, Mr. Mollard. Those are all my questions.

THE CHAIR: Thank you.

Mr. Mahody?

MR. MAHODY: Thank you.

No questions, Mr. Chair.

MEMBER MELANSON: No questions.

THE CHAIR: And I have no questions either.

So Mr. Mollard, that concludes your

testimony. Thank you very much for your report and your participation today. You're excused.

Thank you.

MR. MOLLARD: Thank you for the opportunity.

(WITNESS WITHDRAWS)

THE CHAIR: Sorry. My apologies, Mr. Roberts.

You have no questions?

MR. ROBERTS: No, thank you.

THE CHAIR: Thank you.

Mr. Mahody?

MR. MAHODY: Thank you, Mr. Chair.

The Consumer Advocate would call Tricia Ralph.

I'm sorry. Board counsel would call Tricia Ralph.

Only took a couple years to fall into that trap. Thank you, Mr. Roberts.

Good morning, Ms. Ralph.

Mr. Chair, if I could have Ms. Ralph affirmed, please.

TRICIA RALPH, Solemnly Affirmed:

THE CHAIR: Mr. Mahody?

EXAMINATION ON QUALIFICATIONS BY MR. MAHODY

Q. Ms. Ralph, could you confirm that you filed evidence in this matter and that your pre-filed report has been marked as Exhibit N-14, and that you responded to Information Requests, and those responses have been marked as Exhibit N-15?

A. I don't know the exact exhibit numbers, but yes, I did provide my opinion and responses to the Information Requests.

Q. Thank you.

And in your report, Exhibit N-14, you have included...

MR. MAHODY: If we could go to N-14, please, Mr. Norwood?

BY MR. MAHODY:

Q. Included, beginning at PDF page 27, a detailed history of your professional qualifications

and experience?

A. Yes.

Q. And could you please provide the Board with a brief outline of your professional experience and qualifications, please?

A. Sure.

I've been practising in privacy for just over 15 years. I have a Bachelor of Science and a law degree and a Master's in Health Administration.

I started my career in -- I articled in Toronto and then -- oh, sorry, I'm a practising lawyer. I started my career in the Northwest Territories, where I worked for the Territorial Government for approximately nine years, I believe.

I started as a legislative and legal advisor for the Department of Education, Culture, and Employment where I led the Access to Information and Privacy team, and then I moved over to practice as legal counsel with the government. And there -- we're a bit of

a jack-of-all-trades in the Northwest Territories, but I focused my career on health and privacy law.

And I was responsible for assisting the government with implementing its privacy practices and procedures, advising on compliance with privacy legislation, including privacy breaches.

And that's it, I think, from that job.

And then I went on to be the Information and Privacy Commissioner for Nova Scotia from 2020 to 2025. In that role, I led the office. I was involved in leading major privacy breaches, including a breach -- a cyberattack breach in 2023.

I was responsible for leading public education materials to educate the public on privacy-related matters.

After that, I joined INQ Law and INQ Consulting; we have two branches to our firm.

We are a boutique firm that focuses on privacy, governance, data governance, cybersecurity, AI,

and in this role, I advise clients on compliance with various privacy laws, including PIPEDA. I help companies set up their privacy programs and, you know, do a lot of things related to privacy. It's sort of all over the place, but yeah, that's where I am now.

[9:50:04] **MR. MAHODY:** Thank you, Ms. Ralph.

Mr. Chair, I would request that Ms. Ralph be accepted as an expert qualified to give opinion evidence in privacy, including privacy policies and governance.

THE CHAIR: Any questions on qualifications? Any objections?

She's so qualified.

DIRECT EXAMINATION BY MR. MAHODY

Q. Ms. Ralph, in relation to your report and IR responses, are there any corrections to that evidence you would like to make?

A. Yeah, there's one. So at the time that I wrote my opinion, I did not have a copy of the personal inventory, and since that time, I've been -- I've received a copy and I have no concerns about the actual document itself, although I do still have concerns about communications in terms of identifying what information was impacted with customers.

Q. Ms. Ralph, is that a reference to the personal inventory information that was included as an attachment to Nova Scotia Power's rebuttal evidence in this matter?

A. Yes.

Q. Are the opinions that you've expressed in your report your own?

A. Yes.

MR. MAHODY: Okay. Thank you, Ms. Ralph.

Mr. Chair, Ms. Ralph is available for questions.

THE CHAIR: Mr. Clarke, I'm not sure if you have questions, but if you do, I could give you the option to go either first or last?

MR. CLARKE: Just one second, Mr. Chair.

I think I'll defer and go last.

THE CHAIR: Okay. Consumer Advocate?

MR. ROBERTS: Just a couple of brief points.

CROSS-EXAMINATION BY MR. ROBERTS

Q. Ms. Ralph, you indicated in discussing your background and experience that you were involved, in your capacity as the Privacy Commissioner for Nova Scotia, in a cyber breach in 2023?

A. M'hm.

Q. Could you tell us what that was?

A. Sure. It was with the provincial government. The government used a file transfer system called MOVEit, and MOVEit was attacked, underwent a cyberattack. I don't remember the exact number, but it was all over the world. It wasn't just Nova Scotia; it was many companies that were impacted. And for that breach, we investigated Nova Scotia -- our government, Nova Scotia's actions in terms of its use of MOVEit and how it responded to the privacy breach.

Q. And when you describe a privacy breach, are you talking about the personal information of individuals or some other form of privacy breach?

A. Yes, it was the personal information of individuals that were impacted, and it was a cyberattack.

Q. And did you make any recommendations regarding remediation for the -- as a result of that privacy breach?

A. Yes.

Q. Can you describe what they were?

A. You're testing my memory a bit here, but we provided recommendations in terms of notification, in terms of responsiveness to, you know, how quickly notifications happened, the government's actions in terms of communications with customers, its actions in terms of remediation and that sort of thing.

Q. The other point I wanted to ask you about, you indicated that in reference to the evidence that's been filed here you wished to correct certain comments you made regarding the personal inventory -- of personal information, I should say?

A. Yes.

Q. Can you tell us again, you found -- what your conclusion was having reviewed the actual inventory that was attached to the rebuttal?

A. The inventory itself is standard. It's -- no, I don't have any concerns about it. It's what I've seen with other organizations.

Q. And what about the rest of your evidence regarding the personal information inventory?

A. I'm not sure what you ---

Q. Does it stand as well, or are you making any other changes to the use of the personal information -- of the personal inventory in this case?

A. I think -- sorry, I'm ---

Q. Sorry. When you brought the matter up, you referred to the fact that you were satisfied with the actual inventory as it was attached, but there were other matters that you would still have brought forward?

A. Yes. So in terms of communications with customers about what information may have been impacted, as the letters indicated, to affected customers, in my opinion, there was room for improvement in terms of how that was communicated with customers in terms of certainty as to what may have been impacted. It seems to me that there was some certainty in terms of what was impacted with respect to the SINs in particular and, in my opinion, there could have been more clarity in terms of communications with customers in that regard.

Q. All right. Thank you.

THE CHAIR: Small Business Advocate?

CROSS-EXAMINATION BY MS. MacADAM

Q. Good morning. Just following up on the question from my friend with respect to the personal information inventory, at paragraph 19 of your report, and we can bring it up, if you'd like. That would be Exhibit 14, page 7 of 29.

And so in this you say other than with respect to the PI inventory, which I understand you're now satisfied with:

> ...the contents of NSPI's privacy governance program were [those] expected [by] industry standard and as suggested by [the] regulators...

A. Yes.

Q. Okay. In its rebuttal, NSPI has proposed a number of enhancements to its privacy governance framework. Have you reviewed those?

A. Yes.

Q. And do you have any comments with respect to those enhancements?

A. I believe that they're good enhancements, and I don't have any comments in terms of furthering them.

Q. Okay. If we can go to Exhibit N-15, which is your response to IRs from the CA, IR-2, which is on page 3 to 4, so this question is with respect to periodic audits of internal access to personal information.

I understand from your response part of that audit, as you understand it, has to do with ensuring that there's the least amount of access to personal identification necessary -- or personal information necessary to perform a person's job function. Is that true?

A. Yes, that's typically referred to as roles-based access, meaning that only people who need to view personal information should have access to it.

Q. And is the purpose of the audit to ensure that if that necessary access requirement

changes over time, that that's picked up and properly dealt with?

A. Yes.

Q. Okay. And you say in this response that:

> ...as internal access was not a factor in the breach (rather it was an external cyber security attack), the lack of audit in the two years leading up to the Incident was not likely a factor in the breach.

A. Yes.

Q. Would you agree with me that there's issue -- that once a breach is made, if individuals have excess access to personal information, that could create a bigger problem?

A. Oh, when a breach happens?

Q. Yes.

A. Yes, but only in terms of if that -- if the person who breached was internal to the company. So this is about employees within the company having access, not about external cyberattacks coming in, because

in that case, it's not quite -- it's not relevant.

Q. Okay. And with respect to the audit process, NSPI provided an explanation in the rebuttal about the 2024 audit of Data Lake.

A. M'hm.

Q. Does that address your comments about the fact that internal audits had not been done?

A. When I drafted this in terms of the information requests, we had talked about the audit only in terms of internal access, so I wasn't speaking to the external audit at the time. I didn't -- that wasn't what the information request was related to.

Q. Okay. And in your evidence, you also refer at Issue 5 with respect to credit monitoring. Would you agree with me that credit monitoring is a reactive notification in the event something occurs?

A. Yes.

Q. Okay. Are you familiar with credit freezes?

A. No.

Q. Okay.

MS. MacADAM: Thank you, those are my questions.

THE CHAIR: Thank you.

Ms. Akcakiryan?

(SHORT PAUSE)

CROSS-EXAMINATION BY MS. AKCAKIRYAN

[10:00:18] **Q.** Good morning, Ms. Ralph.

A. Good morning.

MS. AKCAKIRYAN: Could we pull up Exhibit N-14, please?

BY MS. AKCAKIRYAN:

Q. Ms. Ralph on page 6 you say Nova Scotia Power's proxy framework is designed to keep up with evolving regulatory expectations and industry standards. Is that correct?

A. Sorry; which paragraph is this?

Q. Paragraph 10, I believe, just at the end there, the last sentence.

A. Yes.

Q. Okay. When you say, "Evolving," do you mean that the proxy expectations of a company is not necessarily fixed?

A. Yes, for sure, it's changing a lot.

Q. Okay. So it can change over time?

A. Yes.

Q. And a real world cyberattack is one thing that can change those expectations, right?

A. Yeah.

Q. Okay. So a decision from a Tribunal like this Board can also change them?

A. Assuming the company decides to implement changes. I'm not sure, in terms of directing orders and whatnot, but at the company's own prerogative, I suppose, it would be a good idea to modify practices.

Q. Thank you. At page 8 and 9, you note Nova Scotia Power treated this incident as a learning exercise and updated its plans based on what actually happened.

So it's your opinion that a company should change its practices when it learns something from a real incident?

A. Yes, assuming that, you know, it learned that the practices need to be changed, you know, or that there was a deficiency with their practices.

Q. Okay. And practices that met old standards aren't necessarily good enough once that risk changed, and that's part of what you mean by evolving?

A. Yeah.

Q. Okay. Turning to page 17 now, please, you call a Social Insurance Number particularly sensitive information.

A. M'hm.

Q. So for example, if a credit card is stolen, the bank cancels it and sends you a new one, but a SIN doesn't work that way; it can't be cancelled and replaced simplistically; is that correct?

A. Not as simplistically. I understand there is a possible avenue but it's quite difficult. It's meant to be a life-long number.

Q. Okay. So once a SIN is exposed,

that exposure can never be undone?

A. Yeah. No.

Q. Okay. Is that why you say that the harm is not easily remediated?

A. Yeah. Yes, I would say that.

Q. Okay. And then on page 22 you go on to say the risk of misuses persists indefinitely. It never expires. Is that still your opinion?

A. Yes.

Q. Okay. So a threat actor or a criminal could use a stolen SIN two years from now or 10, let's say?

A. Yes, assuming they had access to it.

Q. Okay. But the credit monitoring offered here ends after five years?

A. Yes.

Q. Okay. So the monitoring would end but the risk continues, in your opinion?

A. Yes.

Q. Okay. So cyberattacks on organizations have become more common in recent years, not less common; is that your understanding?

A. Yes.

Q. Okay. And for the last couple of years AI tools have become widely available; is that fair?

A. Yes.

Q. Would you agree that those tools make attacks easier to carry out?

A. I don't think I'm in a position, like, qualified to answer that question.

Q. Okay. Maybe just for an example, a convincing phishing email used to take a skilled, you know, person and now AI can write one in seconds; is that fair to say?

A. Yes. I mean, I wouldn't comment on the quality, but I suppose AI can be used for things like that, yes.

Q. Okay. Would you agree that easier attacks would correlate to more attacks, perhaps?

A. I'm not certain. I think that's a fair assumption but, you know, I think there's a lot of factors that influence whether there's a cyberattack, like political factors and monetary factors and whatnot.

Q. Sure, okay. Would you agree that the threat environment today is worse than it was five years ago, say?

A. Yeah, I would say so.

Q. Okay. And then nothing suggests that it would be safer five years from now?

A. No, nothing suggests that in my opinion.

Q. Okay. So just circling back, a SIN is a keystone piece of a person's identity, and paired with a name and a date of birth it can be used to open accounts in somebody else's name?

A. Yes.

Q. Okay. And AI tools are making identity fraud easier to commit at scale, let's say?

A. Again, I would say the same thing, AI is not my practice and I'm not an AI expert.

Q. Okay.

A. You know, but -- I think I would leave it at that, yeah.

Q. Okay. I'm just wondering because you have a certification of AI in law completed at Queen's University on your CV.

A. Yes, that was a one-week course, and I did take that course but it was more about -- well, it was more about using AI tools and using AI in terms of privacy.

Q. Okay.

A. Not cyberattacks.

Q. Okay. Thank you for the distinction there.

So would you agree, though, that a SIN

taken in this breach wouldn't necessarily lose its value to a threat actor in years ahead?

A. Yeah, I would agree with that.

Q. Okay. And there's an industry standard for how companies protect data before an attack.

A. M'hm.

Q. Okay. And there's also a standard for what a company does for its customers following a breach?

A. Sorry; I think I should possibly qualify that. It's not like an actual standard in the way you might think of. Like, I was using the term as best practice and what's common in the industry.

Q. Okay. For these customers the danger isn't that, you know, another attack on Nova Scotia Power is imminent, it's that their SIN is already out there?

A. I think it could probably be both. Certainly, yes, their SIN is out there and I don't

think there's -- I think it's possible that any company can have another attack over the years.

Q. Okay. And that danger belongs to the customer now and not necessarily just the company?

A. The danger in terms of the impacts?

Q. Yes.

A. Yeah, that would be with the customer.

Q. Okay. And the industry standard and breach response tells us what companies are generally offering right now?

A. Yeah.

Q. Okay. And best practices and breach response can move ahead as everyone learns from new incidents as they arise?

A. Yeah, and it is -- you know, there's different recommendations from different commissioners across the country, in terms of amount of

time, depending on the facts and whatnot as well. And also there's companies who aren't subject to -- or, well, at least some governments aren't subject to orders and so they can take a recommendation there and they might not accept a recommendation from a regulator, for example.

Q. Okay. Would you agree that an offer that goes beyond today's typical breach response can become tomorrow's best practice?

A. Sure, yeah.

Q. Okay. And when the danger to those customers is growing, the protection offered has to keep up with that pace?

A. Yes. That would be my opinion, yes.

Q. Okay. Thank you, Ms. Ralph, those are all of my questions.

A. Thank you.

THE CHAIR: Thank you.

Industrial Group?

MS. RUDDERHAM: No questions, Mr. Chair.

THE CHAIR: Department of Energy?

MR. KAYTER: No questions. Thank you.

THE CHAIR: Mr. Clarke?

MR. CLARKE: Thank you, Mr. Chair.

CROSS-EXAMINATION BY MR. CLARKE

Q. Ms. Ralph, good morning.

A. Good morning.

Q. Am I correct that your work experience does not involve advising companies on responding to data security incidents?

A. No, I've only involved -- or sorry; I've only advised the Government of the Northwest Territories in terms of that, and -- sorry; and not cyberattacks in terms of privacy breaches.

Q. Am I correct that you've never led a security breach investigation before?

A. That's correct. Although in my role as Commissioner I've, you know, led an investigation into the actions of a company. In that role I was privy to, you know, a lot of information about how the company responded to the breach.

Q. Okay. And how many times did you do that?

A. We had the one major breach in 2023, and aside from that I do not believe we had any other cyber -- not a major breach like that; we didn't have any other cyberattacks. We did receive a lot of privacy breaches over the years but not another cyberattack.

Q. So you've never worked for an organization that had a breach where you were part of the incident response team; would that be correct?

A. Except for the Northwest Territories privacy breaches, yeah.

Q. And you've never advised an organization in real time respecting credit monitoring and identity protection; would that be fair?

A. No, I have not done that.

Q. And you've never directed notification efforts involving hundreds of thousands of individuals; would that be right?

A. That's right. Just, you know,

provide recommendations on that approach in the breach. I think it was like 168,000. I don't remember, somewhere in that range.

Q. You've never overseen a ransomware response involving both current and former customers?

A. No, I have not.

Q. So would it be fair to say that your opinion is not based on any direct operational experience managing a breach of the scale that we're talking about here?

A. Sure, but my understanding of what my role here was, was to speak to the impacts of the customers, not, you know, focusing on -- not giving my -- how can I say that -- you know, I wasn't focused on compliance, I was focused on -- I understood my role to be looking at the engagement with the customer.

[10:10:29] **Q.** Thank you.

Have you ever acted as an expert

before on cybersecurity matters?

A. No.

Q. Have you ever acted as an expert before on privacy issues?

A. I've never acted as an expert before. This is my first time.

Q. Okay. If we go to your opinion, which I believe is N-14, and if we can go to page 5, and if we can go to paragraph 6, I think it's the fifth line in, beginning "However".

A. M'hm.

Q. Let me know when you're there.

A. Yeah, I'm there.

Q. Okay.

> However, I express no opinion on questions of legal interpretation or statutory compliance, which fall outside my role.

So that's accurate, in terms of your analysis of this case?

A. Yes, I did look to that as sort

of a benchmark because I wanted to have something, you know, reasonable and not subjective in terms of my role in assessing the communications and interactions with the customer, but no, you know, I'm a former regulator. I understand that's the role of the regulator.

Q. Okay. And in the very next sentence, you say:

> It is the role of the Office of the Privacy Commissioner of Canada ["OPC"] to make findings as to whether NSPI complied with PIPEDA.

And you stand by that comment?

A. Yes.

Q. Do you agree that when reviewing the actions of NSPI, one must consider their actions in the context of a real-time response to the cyberattack?

A. Yes.

Q. And when I say, "Real time," their actions must be considered with respect to a number of factors. For example, number one, trying to stop the

attack in real time, and in this case, where all of Nova Scotia Power's IT systems were encrypted, correct?

A. Yes, I understood they were encrypted.

Q. Trying to determine the cause of the cyberattack, that's another factor?

A. Yes. When I was Commissioner, you know, we had a document called, "Four Key Steps to Responding to a Privacy Breach," and absolutely, you know, the sequence of that was to ensure that the breach was contained. That was the first thing that we would recommend that a company focuses on.

Q. Right. And with respect, another factor would be retaining external experts?

A. Yeah. I mean, not every company does, but certainly that's a good idea.

Q. Trying to determine the scope and breadth of the data access?

A. Yeah.

Q. Trying to determine the scope and breadth of data exfiltrated?

A. Yeah.

Q. Trying to determine who the actual cyber criminal is?

A. Yes.

Q. Restoring affected systems safely and securely?

A. Yes.

Q. Communicating with law enforcement and necessary government entities and regulators?

A. Yes. It's not always required to engage with law enforcement, but in a cyberattack, there likely is.

Q. And then obviously continuing the operations of the utility and providing service to its customers?

A. Yes.

Q. So those are just a few of the factors in terms of real-time issues that have to be considered when looking at the actions of Nova Scotia Power. Would you agree with that?

A. Yeah.

Q. Ms. Ralph, if we can turn to page 10 of your opinion, and paragraph 39, please. And it's the fourth line from the bottom beginning with "While". Tell me when you're there; "While the Incident Report"?

A. Yeah.

Q. Okay.

A. I see it, yeah.

Q. Okay.

> While the Incident Report says this update happened promptly, it does not specify exactly when the update was provided. Thus, is it unclear whether this happened on May 1, 2025, or some other period of time that NSPI would consider as prompt.

If we turn to page 6 of the NSPI rebuttal evidence, N-17, page 6 ---

MR. NORWOOD: N-17, did you say?

MR. CLARKE: Yeah, the rebuttal evidence of NSPI, N-17, and I'm looking at page 6 of 65.

BY MR. CLARKE:

Q. And on line 19, it says:

> In addition to direct notification via letter mail, NS Power issued communications and releases to media which occurred on the following dates:...
>
> April 28, May 1, May 14, May 23, June 4, June 25.

You'll see those references?

A. Yeah.

Q. And when you were preparing your opinion, did you look at the Nova Scotia Power website?

A. No.

Q. Okay. So will you accept that there was in fact a notification on May 1, 2025?

A. Yes.

Q. And in fact, that would answer the question with respect to what you've just raised as you weren't sure about what happened with respect to May

1? **A.** Sorry, I'm not sure ---

Q. Okay, sure. Going back to your paragraph, you say:

> While the Incident Report says this update happened promptly, it does not specify exactly when the update was provided. Thus, is it unclear whether this happened on May 1, 2025, or some other period of time that NSPI would consider as prompt.

And I'm going to suggest to you it happened on May 1.

A. Okay.

Q. Which is the notification which is identified here and on its website as well.

A. Okay, yeah, yeah, that's ---

Q. You accept that?

A. Yeah, for sure.

Q. And then if we turn to page 11 of your opinion, please, paragraph 43, you let me know when you're there.

A. Okay.

MR. CLARKE: Page 11, paragraph 43. Yes. No, no, I'm sorry, it's Ms. Ralph's opinion, N-14. I beg your pardon. I'm not very good with the exhibit numbers.

MS. RALPH: Me neither.

BY MR. CLARKE:

Q. Okay. And so here ---

A. Sorry; which paragraph?

Q. Paragraph 43, please. And so here we're talking about information with respect to May 22, 2025, and at the bottom of this paragraph you say:

> While NSPI said this took place promptly, it did not specify whether this took place on May 22, 2025, or a later date.

And again, this is in reference to notification?

A. Yeah.

Q. So I think what you told me earlier was when you were reviewing to prepare this opinion, you didn't look at the Nova Scotia Power website?

A. I did not go to the website. I looked at what was -- I looked at the Incident Report.

Q. Okay. So are you aware now that there was notification on May 25 with respect to this?

A. Oh yeah, yes. I think I just wasn't exactly sure of the exact date here, and now, having heard the evidence, I understand it.

Q. I'm sorry; I need to correct myself. It was Friday, May 23. So in terms of the information on May 22, it was conveyed on Friday, May 23?

A. Sure. I don't know the exact date, if it was the 23rd or the 25th, based on memory, but certainly right at that time. Yeah, I'm aware of that now, yes.

Q. Okay. Well, let's go back just for absolute clarity because I fumbled that a bit. Page 6 of 65 in the rebuttal evidence, which is N-17 ---

A. Okay. I see it.

Q. And you've -- we've itemized in

notices and you'll see Friday, May 23. So that would answer the question in relation to the paragraph I took you to in your opinion?

A. Yes.

[10:20:00] **Q.** Ms. Ralph, in your opinion you indicate that the June 25, 2025 notification to former customers constituted unreasonable delay?

A. Yes.

MR. CLARKE: So if we could first turn to page 46 of the Nova Scotia Power rebuttal evidence.

MR. NORWOOD: Page what?

MR. CLARKE: Page 46 of the rebuttal evidence.

BY MR. CLARKE:

Q. And at the top of the page we see:

> **June 25, 2025:** Via substitute notice on its website, in the media, on social media, stakeholders, paid advertising, national paid search optimization, [Nova Scotia] Power notified the public that former

> customer information had also been impacted. NS Power simultaneously extended its credit monitoring offer from two years to five years for all current and former customers. Affected customers who had already enrolled in the two-year product offer were automatically extended...five years.

You don't take issue that all of that happened on June 25, Ms. Ralph?

A. I'm not sure what you mean by "Take issue".

Q. Well, do you accept that all of those things happened on June 25 as identified here?

A. That's my understanding, yes.

Q. Okay.

A. Like, I assume that's the evidence of Nova Scotia Power?

Q. It is.

A. Okay.

Q. I guess I just want to make sure you don't take issue with respect ---

A. Oh yeah. No, I don't take issue

with that.

Q. All right. And if we go over to page 47, which is the next page, and pick up at line 18. This is again the rebuttal evidence:

> The most immediate issue to be addressed following a major security incident is the threat of ongoing threat actor access and incursion and potential disruption of operations. [Nova Scotia] Power's top priority was ensuring continuity of services to customers.

You don't disagree with any of those comments, do you?

A. No, I don't. I think I was focused on, you know, these things can happen simultaneously, and it did happen simultaneously with the current customers, or at least somewhere around -- like I'm not sure exactly -- you know, I'm not privy to the forensic investigation but certainly notifications were happening quite quickly after Nova Scotia Power learned of the attack.

Q. Sure. And I think you

identifying your opinion that in relation to a cyberattack there's always a constant sort of push and pull between the speed with which you get information out versus ensuring that the information being released is accurate; would you agree with that?

A. Yeah.

Q. And so with respect to information to former customers, all of those factors that I described earlier would affect getting information out to former customers as well; correct?

A. Yes, just as it would in getting the information out to current customers.

Q. And with respect to former customers beyond those various factors you also need to try to determine what personal information may have been exfiltrated or that cohort, which are the former customers?

A. Yeah, impacted and exfiltrated, I suppose, as well.

Q. And would you agree that you also have to try to locate addresses for those former customers as well; that would be a normal action of the company?

A. Yeah.

Q. So if we can turn to Ms. Valdetero's opinion which would be an attachment to the rebuttal opinion. So this is page 11 of 32 of Ms. Valdetero's evidence. It's the rebuttal evidence.

THE CHAIR: It's in N-17.

MR. CLARKE: N-17. It's the attachment.

THE CHAIR: It's in the back half of the document, in the bottom of the page.

It was what again, Mr. Clarke, page?

MR. CLARKE: So I'm on page 11 of 32 as a hard copy.

A. I've reviewed this, yeah.

BY MR. CLARKE:

Q. Yeah, okay. And so Ms. Ralph, if

we look beginning on line 10:

> [Nova Scotia] Power worked with the assistance of third-party experts highly experienced in responding to large scale cyber security incidents to determine whether it was possible to identify current addresses for former customers, ultimately determining [that] it could not do so with any degree of confidence.

Do you accept that evidence?

A. Sure, yeah.

Q. And then still on that page, going down to line 32 -- I'm sorry; line 15, I beg your pardon. Line 15:

> Tasked with notifying former customers indirectly, [Nova Scotia] Power sought assistance from TransUnion, who in turn connected [Nova Scotia] Power with Sogica, an IT services company with extensive experience in incident notifications to ensure that [Nova Scotia] Power was prepared for [the] thousands of people to seek more information about the Incident on its website and obtain credit monitoring services.

Again, do you accept that evidence?

A. That it worked with Sogica?

Q. Right.

A. Yeah, that was my understanding.

Q. Okay. And would you agree with me that the steps that were taken with respect to TransUnion and Sogica, that would have taken some time?

A. Yes. Although I will say that the direct notifications, in my understanding, were never provided. There was indirect notification for former customers.

Q. Yes, that's right, that's right. But nevertheless these steps were taken with respect to the former customers?

A. I'll accept that, yeah, that's Nova Scotia Power's evidence.

Q. If we can go to page 8 of Ms. Valdetero's evidence, please. And here, Ms. Ralph, if we go to line 21.

A. I don't -- okay.

Q. Are you with me?

A. I didn't have it up there; just a

sec.

Q. It's there on the screen now. So she writes:

> Any assessment of reasonableness is contextual and should distinguish between the timing of [Nova Scotia] Power's determination that former customer information may have been implicated and the operational feasibility of reaching that population with meaningful, accurate, and usable notice.

A. M'hm.

Q. And I'm assuming you don't disagree with those comments?

A. No, but again, it wasn't as if the Nova Scotia Power issued direct -- like, used the addresses to notify former customers.

Q. No, I understand that, but you don't dispute that they -- as part of this process, with everything else that's going on, one of the steps, they tried to locate addresses for these former customers and were unsuccessful in those efforts?

A. Yeah, that's my understanding

that's Nova Scotia Power's evidence.

Q. Now, with respect to the steps that a utility has to take, or Nova Scotia Power had to take, context is important in terms of reviewing their actions; that seems fundamental to me?

A. Yeah.

Q. Okay. And you'd agree that this was a sophisticated, coordinated cyberattack?

A. Yeah, I'm not subject to the forensic investigation, but, yes, I believe so.

Q. Understood. And this constituted an exfiltration of 13 terabits of data?

A. I see that was the evidence, yes.

Q. If we can go to page 12 of your opinion, please. So it's 14, I think; N-14. And in paragraph 47, so here we're talking about the 97,000 customers that ---

A. Additional, yeah.

Q. --- received notice, I think,

on October 31. So paragraph 47, the last sentence:

> The Incident Report does not state when this was identified but does state that [NS Power] sent direct notices to these individuals on October 31...

So I should read the entire paragraph to you:

> In Section 4.2 of the Incident Report, NSPI explained that as it continued its investigation into the scope and nature of the impacted data, it identified approximately 97,000 additional customers in addition to the above who were impacted by the Incident. The Incident Report does not state when this was identified but does state that NSPI sent direct notices to these individuals on October 31, 2025.

[10:30:10] You then say in the next paragraph:

> For the same reasons set out above with respect to former customers, in my opinion this delay was unreasonable.

You came to that conclusion about unreasonableness without knowing when NSPI became aware of the 97,000 customers; correct?

A. Yeah, because, I mean it wasn't clear to me in the evidence when they actually became

aware, but what -- my perspective in this, my understanding of my role, was to look at the perspective of the customer, in terms of the customer. For them, I -- in my opinion they would find that to be a quite a long period of time, six months, to be notified, especially when they'd seen other groups being notified in advance of that.

Q. Okay. I'll come back to that. But you also came to this conclusion without knowing of the complexity involved in trying to locate these additional customers; correct?

A. I mean, I'm aware of the complexity, but I didn't have their forensic report. I didn't know exactly what was -- you know, I don't have the specific details, no, of exactly what was going on. But for me, you know -- sorry; that's not fair, exactly what was going. For me, what I'm thinking of is, you know, Nova Scotia Power, in terms of its actions prior to the attack, should have had this -- like, should have,

especially with former customers, you know, kept track of like what information, contact information, or disposed of that information that it no longer needed anymore.

Q. Yeah. Well, with respect to these 97,000, I guess my concern is that you've made a determination about unreasonableness when in fact you didn't even -- you didn't know when they actually located the information about the 97,000.

A. Yes. But again, I was focused on what a customer would interpret, and you know, from a customer's perspective six months is a long time to wait to know that they were impacted by a privacy breach.

Q. And you made the determination that the delay was unreasonable, again, without knowing of the complexity involved in trying to determine and find out about these 97,000 other customers.

A. Yes. I did not have the forensic report, but I'm certainly, you know, familiar, from my past experience, that this is a highly complex situation.

Q. I want to turn to the notification to customers, Ms. Ralph. And ---

A. The contents, you mean?

Q. Yes.

A. Okay.

Q. Sorry; what did I say?

A. Just notification.

Q. Sorry. Yeah, the content.

So you appreciate that Nova Scotia Power sent out two forms of letters to customers, and that communication went out on May 13, or within approximately 24 hours of May 13. I think that was the evidence.

A. M'hm.

Q. And these two letters were virtually identical, although one version included a reference to Social Insurance Number; correct?

A. Yeah.

Q. Can we go to page 13 of your opinion, and page 50 -- sorry; paragraph 54.

And here you've written:

> Best practice for contents of notification letters is for them to be as specific as possible and identify which data points were in fact breached. However practically, depending on the nature of the breach, this scenario of not being able to say with certainty whether [an] individual data point was in fact accessed by [the] threat actor may arise.

You stand by that comment?

A. Yeah. I was trying to distinguish here between, in terms of the data that was breached, as opposed to being exfiltrated by the threat actor.

MR. CLARKE: Okay. Can we turn, I believe it's N-2, and it's NSPI Responses to the Energy Board, IR-1. And this is for Matter 12273. And it's Attachment 2.

THE CHAIR: IR-1, Attachment 2, so it's earlier.

BY MR. CLARKE:

Q. And so Ms. Ralph, this is ---

THE CHAIR: Sorry; I may have misspoke, Mr. Clarke. I think I said Attachment 1. We're looking for Attachment 2?

MR. CLARKE: I was, yeah.

MR. MAHODY: And I think that's what we have on the screen.

THE CHAIR: Okay. Thank you.

MR. CLARKE: Yes, I think that's right.

MS. RALPH: M'hm, the one with the sentence.

BY MR. CLARKE:

Q. Right. So this is, I'll call it, the SIN letter.

A. Okay.

Q. And you'll understand, the only difference with respect to this letter, versus the one prior, is the reference to the Social Insurance Number.

A. Yeah.

Q. So this has been discussed several times during the course of the hearing. The paragraph, "The types of impacted personal information":

> The types of impacted personal information varied by individual customer and depended, in part, on the information provided by each customer. This may...[include]...

And I just want to make sure we understand what was referenced here. So the sentence reads":

> This may have included [but includes]...name, phone number, email address, mailing and service addresses, Nova Scotia Power program participation information, date of birth...customer account history (such as power consumption, service requests, customer payment, billing, and credit history...customer correspondence)...driver's license number, and Social Insurance Number. For some of our customers, bank account numbers (for pre-authorized payment) may also have been impacted, if this information was provided by these customers.

So that -- that's all of the content with respect to personal information that was identified in this paragraph; correct?

A. Yeah.

Q. Yeah. And then the next paragraph reads:

> While we have no evidence of misuse of your personal information, as a precautionary measure, arrangements have been made with the [customer] reporting agency, TransUnion, to provide you with a two-year subscription to a comprehensive credit monitoring service (TransUnion...) at no cost.

Now, we know that subsequently was moved to five years, don't we?

A. Yeah.

Q. Okay. And there's a second page to the letter, and if we can go to the second page.

A. M'hm.

Q. The first sentence says:

> We encourage you to remain vigilant and cautious about any unsolicited communications (such as emails, text messages, social posts or phone calls), including messages that appear to be from Nova Scotia Power, asking you to provide...personal information.

And then in the final paragraph

there's a recognition, "We sincerely apologize that this issue has occurred."

So that is content that you would have read, in terms of this letter?

A. Yeah.

Q. And there's also an attachment to the letter, which is the Services Description form respecting TransUnion. That's the next page?

A. M'hm.

Q. And then there's also a final page, which is the Additional Guidance, which was provided as well; correct?

A. M'hm.

MR. CLARKE: Next page.

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

BY MR. CLARKE:

Q. Okay. And so all of that was the actual letter to customers; correct?

A. Yes, I would say.

Q. Yeah. Thank you.

And do you agree with me that these letters identified all forms of personal information that may have been accessed by the cyber criminal?

A. As far as I understand, that's Nova Scotia Power's evidence. Are you referring to the "May" or...?

Q. I'm saying they said, "May" and then they identified ---

A. Yeah, yeah.

MR. CLARKE: If we can turn to Ms. Valdetero's opinion, page 16, please? So that's N-17, Attachment.

BY MR. CLARKE:

Q. And page 16, starting on line 6, Ms. Ralph, she writes:

> The record establishes clearly that the absence of customer-specific data element information in the notices was not a matter

> of organizational choice or insufficient effort — it reflected a genuine forensic impossibility when viewed in the context of providing notices to affected individuals as soon as possible.
>
> Do you accept those statements?

[10:40:40] **A.** I accept they're Ms. Valdetero's. I just want to be clear in terms of, like, the exfiltration versus what was impacted. So there is a distinguishment to me in terms -- and I'm not -- I don't -- as I said, I don't have access to the forensic report, but I certainly accept that that's different. And from my perspective, this is -- you know, again, I'm looking at it from the customer perspective, and in my opinion, there was a number of steps -- you know, it should have been available to Nova Scotia Power to identify that, and if not sure, then in my opinion, that should have been clearly communicated to customers.

And, also, it seems that some of it was -- it wasn't in May that it was impacted. From my understanding, it was when the letters were sent to the --

the SIN letters were sent, Nova Scotia Power understood that those people -- those people's SINs were involved there, and so they were impacted by the breach.

Q. Well, what they said was that all of these various forms of personal information may have been affected. That's what they said.

A. Yes, and ---

Q. And just if I could?

A. Yeah.

Q. And that's what they knew at the time?

A. That's what Nova Scotia Power knew -- yes, was the evidence. That's my understanding, yeah.

Q. I interrupted you. You were going to say something?

A. Yes, I think for me the issue is, again, from the customer perspective, it seems to me that that information was -- the use of the language "May" was

confusing for customers, as is evidenced by the letters that were -- I don't remember which exhibit it was, but all the letters from -- and emails and whatnot from customers, and I think that choice of language of it "May have been impacted" was just slightly off. Like, to me, for the customer, it would have been more transparent, more easy for them to understand if you'd said, you know, this was available to the threat actor, like, it was there.

Because I think what happened was people didn't know, right? They didn't know if they'd given their SIN. They couldn't remember that, and so the confusion arose around whether that -- like, they wanted to know whether they had provided that, not -- and to me, they were -- that caused confusion, in terms of not that the information was sitting there and it may have been -- sorry; that it was sitting there, but that it may have been impacted. Like, to me, it was. It was sitting in that system and the threat actor had access to it, so in

my opinion, I would interpret the word "Impacted" as it was impacted.

Q. But if they said "All" -- rather than "May" if they said "All" ---

A. "All" ---

Q. --- that wouldn't have been -- in terms of the personal information, as you had suggested, about saying "All personal information"?

A. Oh, I meant what was listed in the letter.

Q. I understand.

A. Okay.

Q. But if they had said "All" in terms of personal information being affected, that wouldn't have been accurate because they didn't know at that time.

A. No, but I think you would distinguish out. So you don't know for sure which one and you say "May" for those, and if you know that the SIN was

impacted, then you say this one was.

Q. But they didn't know that at the time.

A. In my opinion, from the customer perspective, it was reasonable for them to expect that Nova Scotia Power would have known that.

Q. Okay. If they hadn't known, though, the language they used was the correct language?

A. Yeah, but I think -- if I could qualify that somewhat? And even in terms of me saying it impacted, like, from the customer's perspective, I think it could have been more clear in terms of -- it's kind of -- can you pull the letter back up? It's the way it was phrased; it was confusing for customers to understand. Like, they should have understood that they had provided that information, or that Nova Scotia Power had that information, and they weren't sure whether or not they provided it and whatnot. And then the response of Nova Scotia Power when people called to ask that, which to me

it appeared that Nova Scotia Power anticipated this and had questions, there wasn't clear communication back to them about, you know, why they didn't know that. So the -- it was one of the questions in the Frequently Asked Questions where it was like -- or where it was that -- you know, "What information of mine was impacted" or "was breached?" I think it was something like that.

And the response was to -- "I don't have that information. Please refer back to the letter."

In my opinion, it would have been -- from a consumer perspective, it would have been preferrable that they were able to say, you know, "We can't tell you that for certain, and this is the reason why."

Q. You don't think that the content of this letter in its totality offers that message?

A. I think it's unclear.

Q. I see. Okay.

MR. CLARKE: Can we go to Ms.

Valdetero's opinion, page 16, please?

BY MR. CLARKE:

Q. And here on line 19 of page 16, she writes:

> Notably, NS Power did provide certainty about whether a customer's SIN could have been impacted when it sent two different letter versions to customers; one to those where NS Power possessed their SIN and one where NS Power did not. As a SIN is one of the most sensitive data elements a Canadian resident has, this decision was highly appropriate.

Would you agree with that opinion?

A. That -- sorry; which part of it? Sorry; which part?

Q. I guess the two sentences:

> Notably, [Nova Scotia] Power did provide certainty about whether a customer's [Social Insurance Number] could have been impacted when it sent two different letter versions to customers; one to those where [Nova Scotia] Power possessed their [Social Insurance Number] and one where [Nova Scotia] Power did not. As a [Social Insurance Number] is one of the most sensitive data elements a Canadian resident has, this decision was highly appropriate.

A. I certainly agree that it was appropriate to send a letter identifying a SIN, but I think where the confusion arose with customers was they couldn't remember if they had provided a SIN and, you know, that onus then fell to them to try and remember that. And particularly for former customers, that could have been a long time ago.

Q. Okay. Can we go to page 17 of Ms. Valdetero's opinion?

Just in terms of the categories, do you think the actions of the customers -- I would suggest the actions of the customers would have been exactly the same in terms of -- I guess we're having a debate about the content of the letter and what the letter says, and I think we respectfully disagree, which is fine.

A. M'hm.

Q. But I would suggest to you that the actions of the customers would have been exactly the same if the language had been tweaked as you're

suggesting.

A. I don't know. I think that it depends on each individual customer, and they may have taken -- like, some customers may have had different reasons to take different approaches. I would agree that they would have likely accepted the credit monitoring, if that's what you mean.

MR. CLARKE: Onto page 17 of Ms. Valdetero's opinion. And once we're -- are we there? Yeah, thank you.

BY MR. CLARKE:

Q. Starting on line 10, she writes:

> Reasonable practitioners can and do disagree about the appropriate balance between precautionary communication and accurate communication. However, NS Power's approach - advising customers of the largest scope of categories of information that may have been affected while acknowledging that the scope varied by customer - is both an accurate statement and a defensible choice...

Do you agree with that comment?

A. I agree certainly that we -- that

practitioners disagree, and I think for me, again, back to the customer perspective, it was clear from my reading of the information from the letters and emails and whatnot, from -- I guess it was mostly emails, but from customers, it was confusing.

Just a second; let me read this again.

[10:49:50] Also from my perspective the -- it also was the issue in terms of how this was communicated with customers when they had further questions. Like, when they came back on the Frequently Asked Questions and they were sort of -- instead of saying, you know, we can't tell you for certain that this happened, that your information was amongst that and this is why; it was for whatever reason; it was we had done the forensic analysis; I don't know. But I think there was room for transparency with consumers about the reality of the uncertainty.

Q. She goes on to say:

> ...as it certainly was within the range of decisions a victim of a large-scale cyber security incident would have reasonably made

in the circumstances.

And so, again, the premise of those comments is that reasonable practitioners can agree or disagree, but the steps were reasonable; do you accept that?

A. Yeah, I think the difference is that she is speaking in terms of ---

Q. NS Power?

A. Yeah. And I was -- you know, I was looking at it in addition, like not just -- I used compliance as the baseline, but going further in terms of what a reasonable customer would expect. And certainly, though, I agree that there's disagreement.

Q. And so beyond the letter that went out May 13, we know that Nova Scotia Power subsequently issued a further notice on May 14; correct?

A. Which one was that; can you remind me?

Q. It's part of the Nova Scotia

Power website.

A. Oh, right, okay, yeah.

Q. And there was another notice on May 23.

A. Yes, I'm going -- I'm going to rely on your memory for the exact dates, but, yes, I'm familiar with -- you mean the public notices and all of that sort of thing, yes.

Q. There's a further notice on June 4.

A. Can I look at that ---

Q. That page that I took you to earlier?

A. Yeah, I have a copy of it here, if it's okay. It's in the rebuttal, right?

Q. It's in the rebuttal, yeah.

A. Just the list you mean, right?

Q. Yeah.

A. The chronology? Yeah, okay.

Q. June 4 and June 25 as well.

A. June -- yeah.

Q. And are you aware that there was another notice on July 8th?

A. Yeah

Q. And another notice on September 19?

A. Yeah, I see that.

Q. And the letter that went out on October 31?

A. Yes.

Q. Ms. Ralph, can we turn to paragraph 52 of your opinion? It should be page 13. Are you with me?

A. Yeah.

Q. Okay, great. Here there are some bullet points with respect to concerns from customers. And so the first one reads:

> Concern that NSPI did not provide information about whether customers should

> open new bank accounts or attempt to replace their [Social Insurance Number].

It's not standard practice in breach responses to tell individuals to open new bank accounts; do you agree with that?

A. I was just listing the concerns that were in the -- yeah.

Q. Right. Yeah, but do you agree with me that that's the case?

A. That it was...? Sorry.

Q. It's not standard in breach responses to tell individuals to open new bank accounts?

A. Sure, I -- I've never seen it before, I guess, so, sure. I'm not sure that's standard but...

Q. Well, you've never seen it before?

A. I've never seen a company do that, no.

Q. And it's not standard in breach responses to tell individuals to seek to replace their Social Insurance Numbers?

A. No, my understanding is it's a quite difficult number to replace.

Q. Just one second, Ms. Ralph.

MR. CLARKE: Mr. Chair, just one second.

(SHORT PAUSE)

BY MR. CLARKE:

Q. With respect to the issue of opening banking accounts and attempting to replace their SIN, do you know how many customers complained about that?

A. Not off the top of my head, no. I reviewed the -- I think it was, like, 100 and some odd pages but I don't know exactly.

Q. Okay. And then you say -- then you identify some customers received an activation code for the credit monitoring. Do you know how many customers

complained about that?

A. No, I don't.

Q. Did you try to use the activation code?

A. Did I try?

Q. Yeah, did you try?

A. No. I will say, when we did the MOVEit breach, though, these sorts of things came up as well. There was a lot of confusion from the customer -- or from impacted individuals in this regard as well.

Q. A number of my questions you responded by saying, "I think"; and I'm paraphrasing you, so you correct me.

A. Okay.

Q. But you were saying, "Well, I kind of looked at this from a customer perspective."

A. M'hm.

Q. And I guess if the company tried to do something and, you know, they used best efforts and

it was impossible to get it done by a certain point or if something was impossible to do, that's what should be assessed in terms of the actions of Nova Scotia Power, isn't it?

A. In terms that it was impossible to do?

Q. Well, I'm just saying, there are several questions where I asked you, and you said, "Well, I'm looking at it through the prism of a customer," and I guess that is different than looking at the actions of Nova Scotia Power and what was reasonable and what was not reasonable; would you agree with that?

A. I think, you know, there was the reasonableness in terms of, like, compliance and whatnot with Nova Scotia Power, but again, I was looking from the Consumer and, you know, there may have been disagreement there, but I was trying to get across that what the consumer is expected was encompassed in this.

Sorry; I'm not sure I'm explaining it

that well. Can you say your question again?

Q. I'm fine with your answer if you are. I don't have anything more on that point.

A. Sorry; could you repeat the question, actually?

Q. I don't think I can.

A. But, yes, like there is definitely a fine balance because there is what Nova Scotia Power is doing, and also the consumers. And I think what I was trying to get across in many ways was that there was a lot of pre-steps that, you know, the consumers would have expected. And also they had, you know, additional expectations beyond what was possibly, you know, like strict compliance for Nova Scotia Power.

Q. Ms. Ralph, thanks for answering my questions today.

A. Okay, thank you.

MEMBER MELANSON: No questions.

QUESTIONS FROM VICE CHAIR DEVEAU

Q. Good morning, Ms. Ralph.

A. Good morning.

Q. I just have a few questions.

In your report, which is N-14, in paragraph 2 on page 3 of your report. So you talked about, "In my opinion, the following did not meet best practice," and you list a number there. And best practice is referred to several times in your report.

A. M'hm.

Q. And I think in the rebuttal. You'd agree this area -- this area, in terms of privacy and personal information, is an evolving field?

[11:00:12] **A.** Yeah, it's changing a lot.

Q. And so I'd just like your comments generally on your experience. What is best practice in this field? I know Nova Scotia Power referred to new -- there's new federal legislation that may be coming and so forth.

A. M'hm.

Q. So just generally your comments about how do we look at best practice in that context?

A. So again, I have to say I was tying it back to the consumer as opposed to, like -- best practice was sort of the benchmark for me assessing what the consumer would have reasonably expected. Do you mean for the whole response, the whole ---

Q. Just generally. Well, just generally in terms of the things you talked about.

A. Oh.

Q. Whether it's inventory or notification, collection -- the collection and destruction of those -- of that information; just generally, when you're dealing with best practice, how should the Board consider what is meant by best practice?

A. Sure. So the personal inventory, I'll start that off, as I said, from the beginning.

Q. Yeah.

A. In terms of best practice for former customers and additional customers, in terms of best practice in addition to what the customer would expect, it is, in my opinion, quite long, particularly with the former customer -- or sorry, the additional customers.

Q. I'm sorry; my question is probably not clear.

A. Okay.

Q. So I'm not talking about best practice in relation to each of those points, but generally, best practice in a field that's changing?

A. Oh.

Q. You know ---

A. Like ---

Q. So, you know, the privacy field, it's an evolving -- you know, customer expectations are different, regulators' expectations I think we've heard may be changing. So how do we consider, you know, the

term best practice; you know, how reactive and how responsive and how quickly ---

A. Yeah.

Q. --- should someone act in dealing with that context of something that's -- it's hard to pin down because expectations are changing all the time?

A. Oh, okay.

Q. That's what I meant by the question.

A. Yeah, okay. So -- well, first of all, paying attention to evolving laws and to evolving cases and whatnot. Typically, there's a Privacy Officer, and my understanding was there was one. That would often be their role to be keeping track with all of those changes, and then relaying that back to the government, the company, and using that to change practices and policies and procedures internally. And often, you know, we -- you know, in my work now, we help people develop privacy programs, for example, and we almost always say or

I would always say to be auditing your program and your practices, you know, like, yearly and also even an independent audit every, like, two or three years, kind of thing, from an external party.

Q. Okay. Well, that leads actually to my next question. Have you been listening in to this ---

A. Yeah.

Q. --- hearing?

A. I listened at home.

Q. So let's go to your paragraph 12.

VICE CHAIR DEVEAU: Right there, yeah.

BY VICE CHAIR DEVEAU:

Q. So in 11 you say:

> In terms of organizational commitment, at the time of the Incident, NSPI had a Privacy Officer and Office in place, which is in keeping with best practice and is important from a customer service perspective.

And then you say in 12:

> The regulators' guidance further recommends that senior management monitor and report on

> its privacy program to the Board of Directors. It is not clear to me that this was or is currently NSPI's practice but if it is not, in my opinion NSPI should implement such a practice moving forward as part of its remediation effort[s].

And you may recall yesterday I took the panel through the various steps that are being implemented. The Privacy Officer is going to be a full-time person with dedicated responsibility for these privacy matters. There's a reporting structure now to the Board of Directors as a standing item at their quarterly meetings. Issues relating to policy -- privacy will be reviewed and brought to the Board.

So my understanding -- my understanding from the evidence was that that was not a standing item at the Board, that issues were brought up to the Board as needed at the time of the -- up to the time of the incident.

So is there anything -- in terms of what was in place at the time of the incident, your

statement where you say, "It is not clear to me that this was or is currently NSPI's practice," does that -- does the evidence -- testimony that was given change your opinion, or were you able to confirm whether it was clear that it was NSPI's practice to -- for senior management to monitor and report on the privacy program to the Board of Directors? In other words, was it sufficient for them to bring it to the Board as required?

A. Again ---

Q. *Ad hoc* as opposed to a standing item?

A. For a company the size of Nova Scotia Power that holds sensitive information like SINs, I think it would have been better to have that as a standing item.

Q. There was evidence -- let's go to the rebuttal, at page 18 of the rebuttal ---

A. And sorry, I should just add ---

Q. Yes, sorry.

A. --- you know, as a standing item, like, that doesn't mean that every time it has to be ---

Q. That's right.

A. --- as scary. Like, there might be ---

Q. But the question will be asked at that quarterly meeting. It's an agenda item; correct?

A. Yeah.

Q. So you had actually asked -- you had actually asked an IR about -- it was your IR, INQ Law IR-2 about the -- you asked Nova Scotia Power for a privacy audit plan and dates of any audits of access to personal data of customers ---

A. M'hm.

Q. --- implemented by the company in the two years leading up to cybersecurity plan, and they had a -- they had a clarification to that answer, and they referred to the information protection audit of the Data Lake, and they mentioned that it was part of the company's

Annual Audit Program.

A. M'hm.

Q. So my understanding of your original question was an audit plan about employees or other unauthorized access to data. That was your question; correct?

A. Yes, at -- yes.

Q. Right. So you're smiling; I'm just wondering why you're smiling.

A. Because I think at the time, frankly, of the information request, I could have drafted it as a bigger audit, like to look at more of an audit as opposed to just ---

Q. Okay. All right.

A. --- yeah, but that's what I did at the time.

Q. Okay. So I pursued that yesterday in my questions, and I asked them about audit -- not just audit reviewing policies but audit about

compliance. And I was referred to, in addition to the audit of the Data Lake -- first of all, they answered there was no regular schedule of compliance, but there is -- the company had -- has an Annual Audit Program, and my understanding from the evidence was that that's a general audit program. It's an internal audit program, but it's not just about privacy; it could be about any policy or anything within the company.

A. M'hm.

Q. Does that -- in terms of a broader -- in terms of reviewing your policies and compliance with the privacy policies, is that sufficient for it to be lumped into the corporate general audit program, or should there be a dedicated audit/compliance review done about privacy?

A. I would say a general audit. So what I would typically advise -- or sorry; audit specific to privacy. So what I would typically advise my clients is to every year look at issues like, you know, is there

changing legislation? Have we had an incident? Like, what's going on? And then prioritize from that and make a plan for the following year as to what was most important to audit, from a privacy perspective.

Q. Yeah. And in my ---

[11:10:03] **A.** Like maybe I'll just add.

Q. Sorry, go ahead.

A. Like, I don't think it's -- I -- so I just want to focus on that. Like, it's not you have to audit every single thing every year. I mean, that would be great ---

Q. Right.

A. --- if you did that.

Q. Right.

A. But it’s usually tailored to the circumstance of what’s going on.

Q. An audit -- an audit's an audit because you don't look at everything every year. But ---

A. Yeah, I guess so. Yes.

Q. --- I suppose my question is, is would it be appropriate to have a cycle so at some point there is -- your audit is based on something or it's -- or something cycles back to a certain policy, you know, at regular intervals? Is that something that's ---

A. Yeah.

Q. --- best practice or not best practice?

A. Yeah, that's what I would normally (inaudible due to mumbling).

Q. Okay. My next -- my last question, actually, relates to your paragraph 69.

VICE CHAIR DEVEAU: That'd be N-14. Yeah.

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

VICE CHAIR DEVEAU: Paragraph 69, page 18. Yeah.

BY VICE CHAIR DEVEAU:

Q. And so that's about the issue of no longer collecting SIN numbers. You say:

> In addition, in my opinion, the steps outlined above that NSPI took once it changed its practice in 2018 to no longer collect SINs is not justifiable, reasonable, or in keeping with industry standard. In 2019, NSPI directed employees to remove SINs whenever they were encountered. Best practice would have dictated...the systems be audited so that all SINs were removed as opposed to the ad hoc approach NSPI implemented. In May of 2024, NSPI commenced a process to purge customer SINs. It should not have taken NSPI six years to commence this process. Furthermore, since SINs were still in the system when the threat actor gained access in or around March 19, ['25], this process appears to not have been complete. In my opinion, not having completed this task within 8 months was unreasonable.

So there was further evidence filed in the rebuttal on that issue, and there was testimony in the last few days.

But perhaps the most succinct way of dealing with that, let's go to Nova Scotia Power's rebuttal, 17, at page 53. And we're dealing there with lines 7 to 15.

So they indicated and they indicated in their testimony that, "...what is reasonable is contextual and this applies equally to what may..."

And again, the headline here is:

> Reasonableness of retaining [their] data beyond the time frames set out in [the] internal record retention standards.

So they say that:

> ...[what's] reasonable is contextual and...applies equally to what may be a reasonable or [a] necessary timeframe as it relates to PIPEDA.

And then it says:

> While [Nova Scotia] Power retained customer data beyond the timeframes set out in its 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. The technological evolution of how information is stored, transferred, and used within businesses is part of the relevant context that must be considered when entities are developing, operationalizing, and implementing privacy frameworks. PIPEDA, as well as NS Power's Records Management and Privacy policies and procedures recognize and account for this reality.

So they indicated there, and in their evidence, that due to the technical nature of how the information was stored on this customer -- the CIS system, they just couldn't delete it; it took some time. And they explain how that was -- the reasons for that and why they were cautious about that.

Do you remember that evidence?

A. Yeah.

Q. So what do you say to that, in relation to your opinion in paragraph 69 as to the appropriateness or -- of their response?

A. Yeah, a couple of things. I think -- I mean, stepping back, the Commissioner of -- Privacy Commissioner of Canada has said since 2004 that SINs should not be collected for authentication purposes, and that's due to the high sensitivity of SINs and because there's other ways to authenticate. And I do want to be clear, that it's fine to use SINs for legislative purposes.

Q. Yeah, yeah.

A. So ---

Q. And that was 2004.

A. Two thousand and four (2004). That's the -- well, that's the date on their website.

Q. Yeah.

A. And for guidance.

And so it's been a long time that that shouldn't have been happening.

And also, I think from the customers' perspective, you know, why was this happening when it wasn't required? Or -- well, I'm not sure if Nova Scotia Power would say it was required, but it wasn't advised by the Privacy Commissioner.

And then in terms of this, so generally, even outside of this practice, it's -- or outside of this situation, typically it's not a great idea to draft a policy that you can't comply with, and so I think, you know, there was some issue here in terms of

that.

And the technical information did give me a bit more context yesterday in terms of, like, exactly how difficult it was, so I accept that. But I think it kind of goes back to the original point of it shouldn't have been there in the first place.

And when you realize that from 2018 onwards, you know, the approach of -- I think there was issue with my saying *ad hoc*, but I meant not like a concerted -- like, it was like as you see it, you know, remove it kind of thing, I think that warranted a greater effort to deal with that at the time as opposed to taking that approach and then in 2024 starting the more -- I mean, it was great that they started the 2024 concerted effort, but I think the period of time in between that was too long.

Q. Okay. Thank you, those are my questions.

QUESTIONS FROM THE CHAIR

Q. Ms. Ralph, I just have one sort of question, line of questions, and it relates to this distinction that has come up between, I guess, the customer perspective, as you framed it. And in your responses to questions from Mr. Clarke, you seemed to be drawing a distinction between, I think you used the phrase "Strict compliance" and "Customer perspective." And I just want to make sure I understand what you're saying here, and I might use the context of the content of the notice letter as an example to kind of walk through that, so I just make sure I'm clear about ---

A. Sure.

Q. --- what you're saying.

So I understand that you're -- in your opinion, you weren't attempting in any way to talk about -- to opine on legal compliance with PIPEDA or anything like that.

So when you refer to benchmarks and strict compliance, though, is that what you mean? Like, that's table stakes; you're assuming that that was done? So I think about the letter, I'm assuming, okay, that complies with PIPEDA, but you maybe said in your opinion -- well you have said in your opinion, you believe it's unreasonable, again from the customer perspective.

So are we there sort of so far in terms of my distinction, that the benchmark or strict compliance might be what the content of the letter was, but you're suggesting perhaps something more should have been done?

A. For the -- specifically for the letter?

Q. Yes.

A. Yeah. That is a normal -- I will admit that is a normal letter to see. I just think that from the consumer perspective, there was room for improvement in terms of exact clarity.

And again, I come from a -- you know, my experience is in the regulator background where we focused as well on communications with public -- with the public. And I have seen that in my experience before, that, you know, letters that are -- letters can be more clear; like, they can be more clear.

Because we in this world understand -- like, we're in the impacted, the exfiltrated, like all of that kind of language, that's familiar for all of us working in this field, but for customers, they might not grasp that the same way, like the difference between all of those things. And so I think clarity, you know, on maybe a more plain language approach would have been better for customers.

Q. Okay. And you may or may not be able to ask that -- answer this particular question, but in terms of our role as a regulator, a different form of regulator than the one that you're talking about, but our role as a regulator, why do you feel that our approach or

our view should be requirements that perhaps are higher than what a privacy commissioner might require, in terms of notice?

A. Well, I definitely think it's a different -- you know, obviously it's a different avenue, and your role isn't strict compliance, right, with privacy laws.

But also, Nova Scotia Power offers a -- you know, a regulated service to -- a utility service to Nova Scotians, and they don't have, it's my understanding, a choice. When they -- if they want power, they go through Nova Scotia Power.

And I think from their -- from that perspective of being in the situation -- like, it's -- this is not a situation where someone's voluntarily signed up for a loyalty card program. They're in this realm where they sort of have, like I think it's fair to say, have to if they want to get power. And I think for them, you know, in terms of what your role is, it's looking a

little bit beyond that and how -- you know, how that impacted Nova Scotia Power's service delivery and the relationship with customers.

[11:20:38] **Q.** Okay, thank you for that.

THE CHAIR: Is there anything arising from Board Panel questions?

--- (No response)

THE CHAIR: Mr. Mahody, anything by way of re-direct?

MR. MAHODY: No, Mr. Chair. Thank you.

THE CHAIR: Okay.

Ms. Ralph, I think that concludes your testimony, so we'll excuse you now. But thank you very much for you report and your participation in this proceeding.

MS. RALPH: Okay, thanks.

(WITNESS WITHDRAWS)

THE CHAIR: Anything further,

Mr. Clarke?

MR. CLARKE: No, Mr. Chair.

THE CHAIR: Okay. So I think that concludes our evidence phase of the portion.

We've kind of blew through our midmorning break. So what I was going to suggest now is maybe take 15 minutes or so at this point in time and maybe give counsel an opportunity to chat about timing around undertaking responses and submissions.

MR. CLARKE: Sorry; I didn't catch the last part of what you said. I apologize.

THE CHAIR: Sorry. I was just suggesting to take a break, and then maybe during the break if counsel could caucus about timing around undertaking responses and closing submissions.

MR. CLARKE: Yes, of course.

THE CHAIR: Okay.

So we'll adjourn now. It's 20 after. We'll -- I'll do 20 minutes, just to give folks a little

bit of extra time to chat. And if you're not ready when we come back in, you can keep chatting and we'll wait for you.

So we'll come back at about 20 to 12.

--- Upon recessing at 11:21 a.m.

--- Upon resuming at 11:50 a.m.

THE CHAIR: Okay, welcome back.

So Mr. Mahody?

MR. MAHODY: Thank you, Mr. Chair.

So this is a two-parter that I have for the Panel.

The first is simple, less complex of the two, is the date for undertaking responses. And I think Mr. Clarke and Ms. Power might have a date that Nova Scotia Power proposes to be able to complete the undertakings.

MR. CLARKE: September 4.

THE CHAIR: Anyone have concerns with that?

--- (No response)

THE CHAIR: Okay. Thank you, Mr. Clarke.

MR. CLARKE: Thank you.

MR. MAHODY: The second issue, Mr. Chair, is the issue of submissions. And there are some unique aspects to this matter, as compared to more traditional matters that have been before the Board, like an application for instance, that make setting the dates of submissions somewhat more complex.

What the parties are proposing, and Board counsel joins in, is a request of the Board that the parties be given an opportunity, about two weeks' time, to have consultations among the parties to address issues, including the framework of those submissions and the potential outcomes, a range of outcomes that are at issue in the proceeding. And the parties would like an opportunity to discuss those and see whether or not a common position could be advanced.

There's also the complexity involving the interplay between this matter and the technical side of the matter, if I could call it that, that the parties would like an opportunity to further consider and to see whether or not a common position could be advanced on that as well.

I have encouraged all counsel that they be free to supplement my comments here as so that I'm accurately portraying how we see the next couple of weeks unfolding. But it is -- that is the nature of the request that's jointly being made.

THE CHAIR: Mr. Clarke, do you have any additional comments you wish to make?

MR. CLARKE: Mr. Williams will make additional comment on this.

THE CHAIR: Mr. Williams?

MR. WILLIAMS: Thank you, sir.

And I wholeheartedly agree with what Mr. Mahody has communicated. I would just offer that

obviously as part of -- and I look to my side and behind me as well, but as part of the discussions we intend to have over, like, can we reach a proposed (inaudible due to mumbling), over the coming weeks, any guidance the Board may have today or at a time of what their expectation is of the parameters or timelines for those submissions, would be very obviously welcome, but also appreciated. And if not, that's fine as well. Then the parties can have discussions and then bring forward a proposal to the Board.

THE CHAIR: So in terms of the timelines, I mean I think the Board was content to kind of leave it up to counsel to determine that, and I'm hearing it may be something that we need to defer today, and I guess my initial reaction is I don't see any issues with that. I'm a little bit more puzzled about your comments about the parameters.

MR. WILLIAMS: I think what I'm getting at there, sir, is everyone is certainly aware of

the issues list and the parameters in that respect, but I think, as has become evident over the course of the last two and a half days, there are issues that blend or bleed from one proceeding to the other, and are -- is -- it's the expectation that we would try to delineate that somehow or would we identify certain issues on the issues list that are best to carry forward through to the next proceeding. And I don't have anything specific in mind; it's just the nature of the two proceedings together.

And then the other part of that is, certainly from Nova Scotia Power's perspective, what is on the issues list is one component of the parameters or the scope of this, the other is what is the potential outcome of a process like this.

So obviously when we're making an application, it's approval, it's disapproval, or it's, you know, something in between. This is not that, and a little bit different, obviously.

THE CHAIR: Okay, thank you.

Anyone else have any comments they want to make?

Mr. Roberts?

MR. ROBERTS: Yes, thank you.

I also agree with Mr. Mahody's summary. And I think part of the concern in these very preliminary discussions that we were having, is what would -- what is permissible for us to ask the Board to do based upon what we've had in evidence in the last two and a half days? And I think that that's part of what we have to discuss, based upon the items that have been brought forward.

THE CHAIR: Anyone else have any comments?

MR. ROBERTS: And if I could just add.

THE CHAIR: Yes.

MR. ROBERTS: It may well be necessary for us to come back to the Board for some kind of guidance in the course of those discussions.

THE CHAIR: I'm not seeing anyone else with comments.

So I guess, generally speaking, the Board has no difficulty if we want to defer the setting of dates for the submissions for a couple of weeks to give counsel further opportunities to discuss. If it's determined that there's significant concern around interplay with the other proceeding, I guess we can hear from counsels' views at that point in time once you've had a further chance to view that, and we can take a look at that.

I certainly appreciate that there may be a -- you know, there may be some concerns about, you know, you could potentially look at the substantive issues that have arisen in this particular proceeding. The Board may make certain conclusions on those items to the extent that they're discrete from what might arise in the other proceeding. But I hear the concern about what the remedy might be, if any, relating to those, and I think that's

fair.

And it may be that, you know, one potential option may be to deal with it in phases, in terms of the, you know, the substantive issues. And then to the extent that there are remedies that are sought, maybe we need another appearance to address that issue in more detail.

I'm just spit-balling, but that -- you know, I think certainly there's a number of creative counsel in the room, and I'm reasonably sure that if you have a chance to discuss, you know, if you put forward something that's reasonable in that range, the Board is likely to agree with it.

MR. WILLIAMS: I would just say sir, those -- even those comments, I believe, are helpful.

THE CHAIR: Okay.

MR. WILLIAMS: Thank you.

THE CHAIR: All right. So I think we've gone as far as we can, and I appreciate the

cooperation of all parties to that.

We'll just set a -- just a touchpoint date. And it may be -- maybe, Mr. Mahody, if I could ask you maybe -- let's see, if we're looking for a couple of weeks from now, that's probably around that September 4th timeframe as well.

Is that -- do we want to coordinate it with undertaking responses or maybe give parties an opportunity to review the undertaking responses and then maybe respond a week later or so, around September the 11th, maybe with a view to just -- and expectation would be just an update in terms of where the parties stand on it at this point in time?

MR. MAHODY: That would seem reasonable from my perspective.

I'm seeing agreement in the room as well.

THE CHAIR: Okay. All right, so we'll do that. We'll get the undertakings in on September 4th,

and then an update, to the extent that one exists, on the 11th, and we'll take it from there. Thank you.

So we'll conclude. We'll adjourn for the day. And we're just going to pack up here and please do so yourself.

Thank you.

--- Upon adjourning at 11:58 a.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
Thursday, August 20, 2026