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: Tuesday, August 18, 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

LIST OF EXHIBITS

EXHIBIT NO.	DESCRIPTION	PAGE NO.
	August 18, 2026	
N-22	Equifax data breach settlement	150

LIST OF UNDERTAKINGS

LIST OF UNDERTAKINGS

Halifax, Nova Scotia

--- Upon commencing on Tuesday, August 18, 2026 at 9:00 a.m.

THE CHAIR: Good morning. This is a hearing of the Nova Scotia Energy Board related to the cybersecurity breach at Nova Scotia Power Incorporated and its impact on Nova Scotia Power's customers.

The Board's investigation into the incident is being conducted through two proceedings, one focused on the technical aspects of the incident and the other, the one being heard today, focused on Nova Scotia Power's policies and practices relating to the collection and retention of customer information, customer service, communications, billing and other impacts on operations and regulatory processes.

My name is Stephen McGrath. I'm the Chair of the Board. I use the pronouns he/him, and the Board encourages the sharing of pronouns and titles by persons who choose to do so.

I'm joined on the Panel hearing this matter by Vice Chair Roland Deveau on my left and Board Member Richard Melanson on my right.

Assisting the Board with the hearing today are the Board's Public Proceeding Assistants, Robert Norwood and Svitlana Lykhina, and the Board's Information System's Technician, Jordan Long.

International Reporting is transcribing the proceeding.

A Notice of Hearing for this proceeding was published in the *Chronicle Herald* and the *Cape Breton Post* on March 14th, 18th, and 21st. Proof of Advertising was filed with the Board and marked as Exhibit N-5.

The hearing is being livestreamed and is being conducted in a hybrid fashion with some participants in the Board's hearing room in Halifax and some electing to appear virtually. To accommodate the streaming of the hearing, cameras have been set up at the

front of the room and parties are invited when giving opening statements or when asking questions of witnesses to come to the table up front so that anyone watching remotely can see you.

I'll go down the list of parties in a moment to ask for representatives to identify themselves for the formal record for the hearing, but that can be done from the microphones at your tables. You don't have to come up to do that.

Some information in this proceeding has been filed confidentially. If it's necessary to go into a confidential session with any of the witnesses, the public streaming of this matter will be discontinued for the duration of the confidential session and the hearing room will be cleared of anyone who has not been approved to access confidential information in this proceeding.

For hearing participants who are connected virtually, a separate link has been sent for a confidential virtual session, and it will be necessary for

those people to sign off of the public broadcast and connect to the confidential session.

The Board received a number of letters of comment in this matter, and these have been compiled and marked as Exhibit N-1. The Board did not receive any requests to speak, so the evening session that had been scheduled for tonight has been cancelled.

We'll try to have 15-minute breaks midmorning and midafternoon, and a break for an hour for lunch some time around 12:30. And we'll target breaking the day for some time between 4:30 and 5:00 p.m. These times may vary or be extended depending upon the flow of evidence and the pace of the proceeding.

Gender-neutral washrooms are available on this floor and gender-specific washrooms are available on other floors in the building.

If there's a fire alarm, there are staircases off the halls on either side of the elevators and everyone is asked to take the stairs to the ground

level and exit the building at the back on the harbour side and gather at "The Wave" on the boardwalk on the left of the door as you exit.

I'm now going to go down through the list of parties and ask for introductions on the record, beginning first with Nova Scotia Power.

MR. CLARKE: Good morning, Mr. Chair, Board Members, Colin Clarke, Jennifer Power and Geoff Breen here for Nova Scotia Power.

THE CHAIR: Consumer Advocate...?

MR. ROBERTS: Good morning, Chair, Panel. David Roberts and Michael Murphy for the Consumer Advocate.

THE CHAIR: Small Business Advocate...?

MS. MacADAM: Good morning. Melissa MacAdam and Rebekah Powell for the SBA.

THE CHAIR: David MacLeod...?

Sorry. Could you just key the mic

when you speak?

MS. AKCAKIRYAN: Thank you.

Good morning. My name is Elisa Akcakiryan, and I'll be asking questions on behalf of Mr. MacLeod.

THE CHAIR: Good morning.

Industrial Group...?

MS. RUDDERHAM: Good morning, Mr. Chair, Board Members. Brianne Rudderham for the Industrial Group, and I'm joined by my colleague, Isaac Cain.

THE CHAIR: And Nova Scotia Department of Energy...?

MR. KAYTER: Good morning. Thomas Kayter, legal counsel for the Department of Energy.

THE CHAIR: And did I miss anyone before going to Board counsel?

Counsel.

MR. MAHODY: Good morning, Mr. Chair.

Bill Mahody, Board counsel, and I am assisted in this matter by Board advisory staff Somesh Singh, who is monitoring the matter remotely.

THE CHAIR: Okay. Are there any preliminary matters from any of the parties before we move into opening statements?

Okay. Not seeing any, we'll turn to opening statements.

The Nova Scotia Power statement, I believe, is for the panel. Is that correct, Mr. Clarke?

MR. CLARKE: That's correct, Mr. Chair, and we'd prefer to go last, is that's okay with the Board.

THE CHAIR: Yes, thank you.

We'll start with the Consumer Advocate, then.

Mr. Roberts.

OPENING STATEMENT BY CONSUMER ADVOCATE

MR. ROBERTS: Good morning again.

This proceeding was initiated following concerns expressed by the Minister of Energy about how the cybersecurity attack against Nova Scotia Power was affecting the customers of the Utility.

As the Chair just outlined, after the Board received Nova Scotia Power's incident report on the attack, the Board determined that it would be appropriate to divide the review of the cyber incident into two segments: an inquiry into the technical aspects of the attack, which was already under way at the time, and the current proceeding, which is a review of -- dealing with the impact of the attack on the customers of Nova Scotia Power, including the collection and retention of customer information, measures to mitigate the risks of fraud and identity theft as result of the attack, the billing of customers and communication with customers about the incident.

A number of important questions have been identified in reports that have been submitted by the Board Counsel Consultant, Tricia Ralph of INQ Law, and by Ed Mollard of InterGroup, the consultant retained by the Consumer Advocate.

Among those questions are the following.

Did the privacy policies of Nova Scotia Power meet industry standards?

Why did Nova Scotia Power collect and retain sensitive personal information it gathered from its customers?

Were Nova Scotia Power employees adequately trained to protect personal information from the risks of cyberattack?

Did the customers and former customers of Nova Scotia Power receive adequate notice of the attack and the risks it presented to their personal information?

Did Nova Scotia Power do enough to

mitigate the risks of identity theft and fraud its customers faced as a result of the cyberattack?

Are the measures currently in place to review and update privacy policies and staff training adequate to meet the ever-changing threat environment in which utilities such as Nova Scotia Power operate?

And did Nova Scotia Power adequately handle the billing impact on customers and could alternative methodology have been introduced?

Again, these are some of the questions that arise in the evidence before the Board.

On August the 10th of -- two weeks ago, approximately, Nova Scotia Power filed a robust rebuttal of the evidence before the Board, including pointed criticism of the work of Ms. Ralph and Mr. Mollard. Nova Scotia Power also filed separate evidence of Jena Valdetero prepared for the utility.

To be clear, we do not take an adversarial approach to this proceeding. No one would

suggest that Nova Scotia Power was responsible for the cyberattack or that they did not treat the matter with the urgency and seriousness that it deserved.

However, the important issues raised by the Board in initiating this hearing warrant a constructive discussion about the steps that were taken in the aftermath of the attack and how similar incidents could be avoided in the future.

We have provided, through the report of our consultant, Mr. Mollard of InterGroup, recommendations for measures that could be included to support Nova Scotia Power's preparedness for future incidents and mitigate impacts to customers.

We thank the Board for the opportunity of making this opening statement.

THE CHAIR: Thank you.

Next would be the Small Business Advocate. I believe that's been marked as N-20.

OPENING STATEMENT BY SMALL BUSINESS ADVOCATE

MS. MacADAM: Mr. Chair and Board members, please accept this opening statement on behalf of the Small Business Advocate.

In a world of increasing technological advancement, the security of our private, confidential and personal information, for both individuals and businesses, is of paramount importance. We rely on the holders of that information to maintain a strong defence and to take all reasonable steps to protect our data. We recognize, however, that we cannot expect perfection.

[9:10:05] The matter before the Board today is meant to examine and consider the actions of Nova Scotia Power Inc. with respect to the protection of its customers' information, its customer service, communication, and billing processes, as well as the impact on business and regulatory matters arising from the cybersecurity incident that took place in the spring of 2025.

It is crucial that the Board, intervenors, and all NSPI customers understand what NSPI did before, during, and after the incident to protect the interests of customers, and to determine what should be done going forward.

The SBA looks forward to hearing from NSPI, its experts, and the experts retained by the Consumer Advocate and Board Counsel on these very important issues, and thanks the Board for this opportunity to provide this opening statement. Thank you.

THE CHAIR: Thank you.

Next is the statement on behalf of David MacLeod, which has been marked N-19.

OPENING STATEMENT BY MR. DAVID MacLEOD

MR. MacLEOD: Good morning, Mr. Chair, and Members of the Board. My name is David MacLeod, and I'm before this Tribunal as a public interest intervenor in Matter 12600.

I served 27 years in the Canadian Armed Forces, and during my service as an intelligence operator I held a top-secret clearance. I've requested to become a public interest intervenor to add perspective of over 75,000 Nova Scotians who have had a federal security reliability screening or clearance. This demographic includes public service employees, retirees, veterans, military personnel, research staff, and those working in the manufacturing of military equipment.

Our intervention focuses specifically on the severe, long-term vulnerabilities created for this group due to the 2025 November -- Nova Scotia Power cyber breach.

THE CHAIR: I'm sorry, Mr. MacLeod,

it's not a touchscreen. Mr. Norwood up here will scroll it up for you.

MR. MacLEOD: My bad.

Usually, the public does not consider holding a security clearance to be a risk factor. However, in our information-saturated world, mosaic methods of intelligence collection and analysis make security clearance holders a uniquely vulnerable population.

The compromise of personally identifiable information does not merely expose clearance holders to standard commercial fraud. Instead, it hands foreign threat actors and criminals, the criminal networks, a permanent weaponized mosaic of data to target, track, social engineer, and blackmail clearance holders.

For an ordinary citizen, a data breach means an administrative headache and financial exposure. But security clearance holders must meet the demanding, and continuously intrusive vetting of the *Foreign*

Interference and Security of Information Act. The consequences of failing to meet the requirements are severe and potentially career-ending.

Throughout this proceeding, we intend to demonstrate that standard of corporate remedies are fundamentally inadequate for this demographic. Commercial credit monitoring flags whether someone opens a fraudulent credit card. It does not protect against dark web dossier assembly, target spear phishing, lifestyle profiling, or foreign coercion. A Social Insurance Number is a static and -- sorry; is static and lasts a lifetime. The dark web does not erase data after a few years. Offering a basic commercial credit report to an individual whose PII has been leaked to criminal or foreign intelligence entities is performative at best.

We look forward to cross-examining the witnesses to ensure proportional remedies are found to address the actual personal security and livelihood risks faced by Nova Scotians who have or have had federal access

or security clearance. Thank you.

THE CHAIR: Thank you very much, Mr. MacLeod.

Did I miss anyone other than Nova Scotia Power?

Okay. Mr. Clarke?

MR. CLARKE: Mr. Chair, I was thinking in terms of steps. Perhaps you could swear in the panel, I could ask the usual short direct questions, and then Ms. MacDonald could give the opening statement. Does that sound okay?

THE CHAIR: Sounds great. Thank you very much, Mr. Clarke.

So beginning down at the -- my far end.

GLEN MacLEOD, Solemnly Affirmed:

CHRIS LANTEIGNE, Solemnly Affirmed:

LIA MacDONALD, Solemnly Affirmed:

BLAKE WILLIAMS, Solemnly Affirmed:

THE CHAIR: Thank you very much.

Mr. Clarke.

MR. CLARKE: Thank you, Mr. Chair.

EXAMINATION ON QUALIFICATIONS BY MR. CLARKE

Q. Mr. MacLeod. Mr. MacLeod, you are the Director of Customer and Grid Intelligence for Nova Scotia Power. Is that correct?

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

Q. Have you appeared before the Board as a witness in the past?

A. (MacLeod) No, this is my first appearance as a witness before the Board.

Q. Can you please describe your background, qualifications, and experience?

A. (MacLeod) Yes. I have a Bachelor

of Arts in economics from Dalhousie University, and a college diploma in computer programming.

I joined Nova Scotia Power in 2000 as a technology analyst and subsequently transitioned to leadership roles in energy delivery and customer workgroups.

I've been in my current role as Director of Customer and Grid Intelligence, responsible for operating technologies, including advanced metering infrastructure, since June 2023.

Q. Mr. Lanteigne. Mr. Lanteigne, you are the Senior Director of Customer Care for Nova Scotia Power. Is that correct?

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

Q. Have you appeared before the Board as a witness in the past?

A. (Lanteigne) No, this is my first appearance as a witness before the Board.

Q. Can you please describe your

background, qualifications, and experience.

A. (Lanteigne) Yes. I have a Master's in business administration from the University of Liverpool. Prior to joining Nova Scotia Power, I worked for 19 years at CIBC in a variety of progressively senior roles supporting their customers.

I joined Nova Scotia Power in 2021 as Director of Customer Care and have been in my current role since May of 2026. I lead our Customer Care Centre, Permit Centre, Billing, Credit Services, Payment Services, Customer Relations, Customer Communications, and Customer Engagement teams.

Q. Mr. Williams. Mr. Williams, you are the Vice President of Legal and Regulatory Affairs for Nova Scotia Power. Is that correct?

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

Q. Have you appeared before the Board as a witness in the past?

A. (Williams) Yes, I have previously

appeared before the Board as a witness at the 2026-2027 General Rate Application.

Q. Can you please describe your background, qualifications, and experience?

A. (Williams) Yes. I have a Bachelor of Arts in political science from Wesleyan University in Connecticut, and a Bachelor of Law from Queens University. I am a member of the Nova Scotia Barristers Society, an inactive member of the Law Society of Alberta, and a past member of the Law Society of the Yukon, as well as the Law Society of the Northwest Territories.

Prior to joining Nova Scotia Power, I worked at the Bennett Jones law firm in Calgary, where I was a partner and represented oil and gas and utility clients in a variety of regulatory settings. I joined Nova Scotia Power in late 2019 as counsel, and have been in my current role as Vice President, Legal and Regulatory since March 2026.

Q. Ms. MacDonald. Ms. MacDonald, you are the Senior Vice President of Technology for Nova Scotia Power. Is that correct?

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

Q. Have you appeared before the Board as a witness in the past?

A. (MacDonald) Yes. I have appeared before this Board on a number of occasions, including past general rate applications, backup/top-up hearings, and Annual Capital Expenditure Plan hearings.

Q. Can you please describe your background, qualifications, and experience.

A. (MacDonald) I am a professional engineer registered in the Province of Nova Scotia, and a graduate of Dalhousie University, with a bachelor’s in electrical engineering. I am also a graduate of Saint Mary's University, Sobeys School of Business Executive MBA Program.

I started my career with Nova Scotia

Power in 2000, taking on increasingly senior roles in the areas of field operations and storm response, work management and field resource allocation, asset management, and IRP system and capital planning. These roles included Director of Planning, Senior Director, T&D Field Operations, Senior Director, Enterprise Asset Management, and Vice President, Transmission, Distribution, and Delivery.

More recently, in my roles as Vice President, Customer Experience and Innovation, followed by Senior Vice President of Customer Strategy and Transformation, I have led teams to refresh the company's customer experience strategies, as well as the development of grid modernization and electrification strategies that depend on customer solutions.

I have also been a co-lead with the facilitation of the transition to the Independent System Operator function in Nova Scotia.

I have most recently moved into my

current role as Senior Vice President of Technology in July of 2026. In this current role, I will work to bring together information technology, operating technology, and grid modernization strategies and teams, with a focus on better serving customers.

Q. Ms. MacDonald, you and the various panel members from Nova Scotia Power had the responsibility for the evidence of Nova Scotia Power; is that correct?

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

[9:20:00] **Q.** And that evidence includes Exhibit N-3, the Cyber Incident Report, Exhibit N-2, N-4, and N-6 to N-12, IRS from the Board, CA, David MacLeod, INQ, NSDOE, and SBA, as well as Exhibit N-17, the rebuttal document filed on August 10. Is that correct?

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

Q. And is Nova Scotia Power's evidence true and accurate to the best of your knowledge?

A. (MacDonald) Yes.

MR. CLARKE: Mr. Chair, we'd now have Ms. MacDonald give the opening statement.

THE CHAIR: Thank you, Mr. Clarke.

OPENING STATEMENT BY NOVA SCOTIA POWER

MS. MacDONALD: Good morning, Mr. Chair, Members of the Board, and stakeholders.

We are here today to discuss the sophisticated criminal cyberattack experienced by Nova Scotia Power in 2025. The attack had a significant impact on our customers, employees, and corporate systems, which in turn impacted public confidence. We acknowledge the work ahead for us to improve our customers' trust and we are committed to earning it through transparency and accountability, including being here today to discuss the attack and our response in more detail.

Everyone at Nova Scotia Power recognizes the concern, frustration, and uncertainty the attack created for current and former customers whose information was part of the breach. This concern is particularly understandable given that the compromised information of certain affected customers included highly sensitive personal data, including Social Insurance

Numbers. Nothing is more important to us than regaining the trust of those we serve, and we understand that trust must be earned through our actions, not our words.

This attack was a serious criminal act. While that fact is important, it does not change our responsibility to our customers. Cybersecurity and privacy governance is not a one-time effort, but an ongoing and ever-evolving commitment. Threats continue to evolve, and our systems, processes, training and expertise must evolve with them. Customers rightly expect us to learn from this incident and to act on those lessons. We accept accountability for the stewardship of the customer information in our care, and we accept responsibility for continuously strengthening our safeguards against evolving threats.

From the moment the attack was discovered, our focus was on protecting and being transparent with our customers, containing the incident, restoring critical systems, supporting affected

individuals, and working openly with regulators and law enforcement. The measures taken were informed by the information available at the time, guided by leading cybersecurity and privacy experts, and directed toward minimizing impact on customers and preventing further compromise.

As the Office of the Privacy Commissioner of Canada recognized, Nova Scotia Power undertook significant remediation efforts and has since committed to additional security, governance, and privacy enhancements to further strengthen our protections going forward.

Our teams worked around the clock to contain and respond to the attack, but this was not an event that could be resolved immediately. Recovery required careful rebuilding of systems, validation of impacted data, implementation of enhanced security controls, and restoration of customer-facing services, while continuing to provide reliable electric service to

Nova Scotians.

Since the attack, our focus has been on restoring systems safely and securely while strengthening our cybersecurity and privacy posture. We are pleased to report that major systems have been restored, and Nova Scotia Power has returned to normal operations across most of the areas of the business.

Nova Scotia Power has also implemented significant enhancements to its cybersecurity and privacy posture, which is detailed in the Company's Rebuttal Evidence.

We do not view this, though, as the conclusion of our work. Rather, it was a defining moment that reinforces the need for continuous vigilance, stronger safeguards and greater resilience. We are committed not only to recovering from this incident, but to improving confidence, learning from what occurred, and emerging as a stronger and more secure organization for our customers, employees, and communities.

One of the central issues in this proceeding is communication with customers. We believe our actions demonstrate a sustained and meaningful effort to keep customers informed through the recovery process. Consistent with PIPEDA's breach notification requirements, Nova Scotia Power issued notifications to affected individuals where the circumstances indicated a risk of significant harm as that information was confirmed. The notices were designed to provide sufficient information to enable customers to understand the nature and potential consequences of the breach, assess its significance to them, and take steps to reduce or mitigate potential harm. The notices also identified available support measures, including credit monitoring, insurance, and identity protection services offered to customers for a term of five years. Our team also established a dedicated cyber incident website, issued ongoing public updates, provided frequently asked questions, offered guidance regarding identity protection by phone, online and in-person

channels, and continued communicating as new information became available.

While there may be differing views about whether more could have been done or done differently, and while we continue to learn from the impacts of the attack, we believe our actions demonstrate a well-coordinated and meaningful effort to keep customers informed throughout the recovery process.

One of the other central issues in this proceeding is the billing issues experienced by some customers. We know that the cyberattack created challenges in billing operations, causing concern and frustration for those customers. We took practical steps to reduce the impact of billing disruptions on customers, including the suspension of late fees and disconnections, recruiting meter readers to obtain readings for customer bills, offering payment plans and interest-free payment arrangements, and providing advance notice before normal collection activities and practices resumed.

Beyond these measures, we offered customers the flexibility to defer payment completely if they had concerns about their estimated bill amount and have honoured this flexibility since the Spring of 2025. These measures were intended to reduce the impact on customers while the Company restored its systems.

We continue to participate fully and openly in the Board's ongoing process. This hearing is an important opportunity for the Board to examine what happened, the actions we have taken, and the work required to protect customers going forward. We know there will be difficult questions, and those questions are appropriate. Our responsibility is to answer them, demonstrate what we have learned, and continue the work required.

Thank you for the opportunity to be here before you today and continue our commitment to transparency with this Board, our stakeholders, and our customers.

MR. CLARKE: Mr. Chair, the panel is

ready for questions.

THE CHAIR: Thank you, Mr. Clarke.

We'll start first with the Consumer Advocate.

CROSS-EXAMINATION BY MR. ROBERTS

Q. Thank you. And as is customary, I'll address my questions to the panel generally and you folks have topics that you'll each respond to, I assume.

I want to start with a general question about the information itself that was gathered in the course of business by Nova Scotia Power. And a good place to do that would be in the Exhibit N-16, which is the redacted version of the incident report, and I'm going to look at page 14 of 46. Thank you. And it's the paragraph beginning at line 10. This is -- in this paragraph, you provide a summary of the different categories of information that were gathered and were subject to, I guess, access by the -- in the attack.

First, you described obviously name, phone number, email address, mailing and service addresses. I guess that's readily understandable as to why you would have that and what purposes it would be put to, but perhaps you could just explain in an introductory

fashion the use of that information?

[9:30:08] **A.** (Williams) Sir, just before, I just want to make sure we have the right reference before we give our ---

Q. It's up on the screen and it's paragraph 3.2, line 10 of the -- of your incident report, the December refile.

A. (Williams) Sorry, is this the correct reference on the screen?

Q. Yeah.

A. (Williams) Okay.

Q. Yeah. And I'm starting at line 12, actually, Nova Scotia Power program participation, you describe the various types of personal information, and the first category, name, phone number, email address, mailing and service addresses.

And just generally, why do you have that?

A. (Lanteigne) Thank you for the

question, Mr. Roberts. I'll answer that. I think just for those general pieces of information that you shared, that's the information that we require to set up an account and provide electrical service to a customer.

Q. Okay. And then the next sentence, Nova Scotia Power program participation information, what is that and why would you have that?

A. (Lanteigne) That information would include if a customer is a part of a particular program. An example of that would be if they're like a member of the time-bearing pricing pilot. So it would be information specific to that customer in those types of situations.

Q. Next, date of birth, why do you include in the information you gather a customer's date of birth?

A. (Lanteigne) The information on date of birth is just another form to establish an account and identify that particular customer.

Q. Okay. Customer account history, and then you have some examples, power consumption service requests, customer payment, billing and credit history and customer correspondence. Why is that information gathered and held?

A. (Lanteigne) That information is really just a record of what a customer has -- I guess has done with Nova Scotia Power. So for example, if there's been a service request, if they've done a renovation, for example, that customer service request history would be part of the customer's file. The payment history, along with the billing history the record of the account activity for the customer.

Q. And then you go on, driver's licence number. Why would you have the customer's driver's licence number included in this information?

A. (Lanteigne) That information, again, would be used to establish the identity of the customer when a customer account is created.

Q. It's not sufficient to have the date of birth as the identifier?

A. (MacLeod) I think from our perspective it just provides the additional confirmation of a customer's identity.

Q. Okay. And then finally, Social Insurance Number?

A. (Lanteigne) Thank you for your patience. Just to clarify, actually, I guess additional information on the driver's licence as well too. So the driver's licence would not be something that's on file for every customer. It would be something that if that identity needs to be verified for that particular customer. So maybe I'll just add to that, if I could, if you're okay with that on this question, and then I can answer the Social Insurance Number question as well.

So from a driver's licence perspective, our current process for identifying a customer is, you know, when a customer is setting up an

account, there's a -- there's a variety of steps that we can take to identify that customer. One of the tools that we do use is the Equifax identity check. It allows us to ask questions of a customer and establish identity. If they're able to pass those questions, that data is not retained, but it allows us to establish the account.

In situations where, you know, if we're not able to verify a customer's identity through that information, it is important for us to understand the customer that we're actually working with, and ID may be required, and that would be the situation where a driver's licence is required.

To continue on the question of Social Insurance Numbers, I think it's important to state that Social Insurance Numbers have not been collected for the purpose of verifying identity and establishing accounts for almost a decade by Nova Scotia Power. When they were collected, that was the purpose as well. It was a source of information that allowed us to establish a unique

identifying record of that customer when they're establishing the account.

Q. Sorry, I just want to go back to your previous comments on the driver's licence. You said that some information is gathered in order to confirm identity but not necessarily retained?

A. (Lanteigne) That's correct. So when we are asking questions to establish an account opening now, the Equifax identity tool that allows you to verify a customer's identity, it does ask questions that would be known to that customer. The information is used to answer the question, and if it confirms the identity of the customer, that would be the end of it. Our team does not retain any of that data in our current practice, and that tool to verify identity, it's a -- you know, a good example of it would be it's similar to if you're establishing identity when you're applying for a product at a bank, for example. It's a commonly used tool in the industry.

Q. The Equifax identity tool, is that in some kind of standard form or a form that your employees apply when they're dealing with customer identity?

A. (Lanteigne) That's correct. So the form is essentially an Equifax tool that the teams use. They're not actually writing down the information. It's a series of questions that need to be answered, and there's choices that are provided. The customer provides the choice. It would be entered in, and then once the identity is confirmed, the account opening would continue. So again, none of that information is actually retained by Nova Scotia Power when we establish accounts.

Q. But the tool itself tells you whether the identity has been confirmed?

A. (Lanteigne) That's correct.

Q. I wonder if we -- I don't know that we've seen that tool in the evidence, and I'm wondering if we could have an undertaking to have it

produced?

A. (Williams) Apologies, Mr. Roberts, the pause was just to confirm what could be produced to demonstrate the tool, and as I understand it, there is product information that we could provide as an undertaking to demonstrate the scope of the tool.

MR. ROBERTS: Okay. I would ask for an undertaking to be ordered. Thank you.

THE CHAIR: Could you just state exactly what you're going to provide, Mr. Williams?

MR. WILLIAMS: I could, sir, but I think Mr. Lanteigne could probably do it better.

THE CHAIR: Okay. Thank you.

MR. WILLIAMS: So I'll turn it to him.

MR. LANTEIGNE: So as mentioned, Equifax provides this service, and they obviously have established relationships with a lot of organizations across Canada. So this is not something that's been designed specifically for Nova Scotia Power. So what we

will do is we will provide information that just demonstrates what the tool does. It will be available from Equifax, but we can provide that as an undertaking, for sure.

THE CHAIR: That'll be Undertaking U-1.

MR. ROBERTS: Thank you.

UNDERTAKING U-1 - To provide information that demonstrates what the Equifax tool does

BY MR. ROBERTS:

Q. And is the driver's licence something that's -- driver's licence number, is that something that's part of the tool or is that an additional source of information if you're having trouble confirming the identity of the customer?

A. (Lanteigne) If -- the tool is successful for most customer applications. If a customer is not able to be identified with the tool, that would be

where there's additional verification steps that are required, so in the current process a copy of the customer's identification and driver's licence is one of those sources, would be -- allow us to establish the identity of the individual setting up the account.

Q. And that information -- sorry, the driver's licence, is that retained by Nova Scotia Power on the customer's file?

A. (Lanteigne) That information -- if you were calling and you were establishing a new account, our current process is that that information is verified and then it is destroyed.

[9:40:00] **Q.** Okay. So again, setting aside for a moment the Social Insurance Number, what among the various categories of information that are described in this paragraph in your incident report is actually maintained and retained in the records of Nova Scotia Power?

A. (Lanteigne) Thanks, Mr. Roberts.

The information that's in this list right now, essentially maybe the best way to answer it is what information is currently not retained.

So the driver's licence number would not be retained and Social Insurance Numbers are not currently something that Nova Scotia Power retains for customers. The exception to that is in the limited situation where it's required for tax reporting purposes.

Q. So everything else would be retained, then?

A. (Lanteigne) That is correct.

If I could just clarify as well, too, the billing and credit history, that would be a record of the Nova Scotia Power billing and credit history. It would not be like a full credit file for the customer. I think it's just an important distinction.

Q. Fair enough.

MEMBER MELANSON: Before we move on from the Equifax matter, I'd just like to -- sorry, Mr.

Roberts, I'd just like to interject.

When you describe the situation where the Equifax tool does not identify the potential client, is that because they can't answer one of the questions or they answer incorrectly one of the questions that's in the tool?

MR. LANTEIGNE: That could be one of the reasons.

Another reason could be, in Canada, there are two, you know, main credit reporting agencies, Equifax and Transunion. And if there is not enough information on the file to establish a credit history for a customer, that could be another reason why it's not able to actually successfully identify the customer.

MEMBER MELANSON: Okay. And just before I forget it on the licence issue, it's the number you're taking down? You're not getting a copy of the actual -- a photocopy of the actual licence?

MR. LANTEIGNE: In our current

process, if a customer is sending us -- so a couple of things.

Again, I cannot say for certain if the driver's licence is one of the questions that Equifax could ask. I do not have that. But if a customer is not able to verify through that process, they are sending us a copy of the licence to verify the identity and then, once we've verified it, we are destroying it.

MEMBER MELANSON: Okay. Because a picture would be -- a picture would be included in what's being sent. The actual licence would show their picture.

MR. LANTEIGNE: That's correct. The customer would take a copy of that and send it to us.

MEMBER MELANSON: Okay. Thank you.

BY MR. ROBERTS:

Q. Now, you go on -- the statement goes on to say:

> For some customers, bank account numbers for preauthorized payment may also have been impacted. This information was provided by those customers.

So first off, I guess, the information that is retained, you described as being retained by Nova Scotia Power, all of that was impacted by the cyberattack. Is that correct?

A. (Williams) Yeah, and this is an important distinction, I think, Mr. Roberts. When we talk about "impacted", I think what we're saying -- what we're really saying is that this information was potentially access by the threat actor, and so I just want to make sure we're clear when we say, "Impacted" what we mean because it's not -- we're not able to definitively determine or say precisely what was taken by the threat actor.

Q. And I agree that's an important point.

And what you're saying is that you have not and presumably will not be able to advise particular customers what among their personal information

held by Nova Scotia Power was actually affected by the attack?

A. (Williams) That's correct. We cannot definitively say what was taken by the threat actor.

Q. And why is that?

A. (Williams) Well, the nature of the systems and what was done is that we can identify the volume of data that was removed from the system and at a high level where it came from within the system, but we are not able to determine precisely what was included with that volume of data.

The example that I've generally used when trying to explain it to people, and I'll try it here, is if you have a bookcase in your home and you've got boxes containing, you know, sensitive documents, books, what have you in the boxes, someone enters your home, moves those boxes around, lifts the top of the boxes, you could tell which of those boxes had been touched, but you

don't know what they've viewed in that and what they've digested in terms of the information that's before them.

So we can tell what's been touched within the system, but we can't -- and we can tell how much has been removed from the system, but we don't know precisely what came out of the system.

Q. So if they took a book, you wouldn't know that.

A. (Williams) Well, it's not -- so my example has limitations, I suppose.

If they looked at the book and tried to memorize what was in the book, we wouldn't know that, but it's not like they're actually removing files. It's more of a copy and paste as opposed to a cut and paste, if you will.

Q. Have you looked at your data systems in order to remedy this issue about knowledge, knowing what individual customer data was actually affected by the attack?

A. (Williams) So I'll offer a response, but I'll offer it with the caveat that we are now getting into some of the more technical aspects of this that are probably best discussed in the next phase of this in terms of -- but my understanding, sir, is that it's not a -- it's not -- has nothing to do with our system or limitations or characteristics of our system. It is just the nature of what was done.

As I said, we know what was touched and we know what was contained in those -- continuing with my example, in those boxes that were touched, but we don't know exactly what was taken. And that's not a function of our system. That's just a function of technology, I suppose.

Q. Now, you'll have reviewed Ms. Ralph's report for the Board -- for Board counsel. And one of the points that she's critical of is what she calls the "personal information inventory" and your inability to do exactly what we're talking about, which is identify

individual customers' information that was affected.

What do you say to that?

A. (Williams) Yeah, and it's a good question. And I think what I would say is just to carry on what the conversation was between you and I.

So our inability to definitively say what was or was not taken from the system has nothing to do with our knowledge of our system.

We know what was in the system, we know where data and information was generally within the system. It's just that, as I said, you can know what's in the boxes in the shelf in your home, but you don't know if someone read that material and took that information with them.

Q. So Ms. Ralph described the -- your personal information inventory system as being "unreasonable" in terms of your inability to do what we're talking about.

What do you say to that conclusion?

A. (Williams) Well, Ms. Ralph's conclusion in that regard, there may be circumstances where her conclusion would -- her conclusion would be reasonable or correct. In this instance, we would disagree because, as I said, we had an understanding of what was in the system and where it was within the system. It's just a matter of we will never be able to tell -- you cannot tell what was actually taken. And it's for those reasons that I've tried to explain in my analogy, which I'm starting to maybe feel was inadequate, but that's the reality of it. So you can tell if someone has picked up a book and accessed it, effectively. What you don't know is if someone read the book and what information they may have taken with them.

So I understand her point, but in this instance, the two things are entirely unrelated.

THE CHAIR: Mr. Williams, just to get an idea of -- you say you know the volume of data that was taken, I think it was 13 terabytes, if memory serves, but

what is the volume of data that actually would have been held by Nova Scotia Power at the time? Like, what percentage of data would that have been?

MR. WILLIAMS: I'd have to take an undertaking on that, sir, if you'd like. I'm happy to, but it's not something I should probably guess at.

THE CHAIR: Okay. No, and we're focused, I guess, in particular on the IT side of things, not the OT side of things?

MR. WILLIAMS: That's correct.

THE CHAIR: Yeah.

MR. WILLIAMS: Well, entirely focused on the IT side of things, not the OT side of things.

[9:50:00] **THE CHAIR:** Yes. Yes. Okay. So that will be an undertaking to provide the volume of data held in the information technology systems by Nova Scotia Power at the time of the cyberattack. U-2.

UNDERTAKING U-2 - To provide the volume of data held in the

information technology systems by Nova Scotia Power at the time of the cyberattack

THE CHAIR: Sorry, Mr. Roberts.

BY MR. ROBERTS:

Q. I want to come back to the paragraph that we were talking from a few moments ago. And the sentence after you referenced Social Insurance Numbers, the sentence:

> For some customers, bank account[s] (...pre-authorized payment) may also have been impacted..."

Can you tell us what banking information was held by Nova Scotia Power? What customer banking information?

A. (Lanteigne) Yes. So if a customer had set up pre-authorized payments for their Nova Scotia Power account and we had that information, it would include the banking number, the transit number, and the actual account number. The information that would be

required for pre-authorized withdrawal to be taken for a payment on an account.

Q. And have you -- is there -- is it easy to describe what that -- what someone could do with that information? In other words, could someone gain access to a bank account as a result of having that information?

A. (Lanteigne) I think, obviously, having that information stolen by the criminal who attacked Nova Scotia Power, it's obviously not something that is ideal. With that information alone, you know, it's just information that could potentially help someone gain access to an account. It doesn't definitively mean that just that information will allow someone to take a withdrawal or gain access to a customer's account.

Q. It could happen, but are you aware of other factors that would prevent it from happening?

A. (Lanteigne) I think from my

perspective, again, you know, protecting that information, monitoring that information is important, but that information alone, you know, the banks obviously have other safeguards and protocols in place to verify identities of customers before transactions are occurring on accounts. So, you know, it's important to monitor your accounts, and that's guidance that we provided to customers. It's important to, you know, make sure that you're being diligent from that perspective, but the information alone would assume, if you were just accessing an account with just that information, it would assume that the banks don't have safeguards in place, which they do, to protect their customers.

Q. Any other banking information, other than the type that would provide that kind of access, any other banking information held by Nova Scotia Power?

A. (Lanteigne) No, beyond, like, a bank account number that I described a moment ago, the

only other way that customers would pay with banking specific information would be through credit cards. Customers can do that through the MyAccount portal using our vendor KUBRA. That information was not affected and is not retained specifically by Nova Scotia Power.

Q. If, as a customer, I found myself at some point in arrears in my payments to Nova Scotia Power for my bill, is there other information that you would obtain from that customer -- from that particular customer, in those circumstances?

A. (Lanteigne) No. I mean if a customer is in arrears, you know, in a typical time, we're obviously increasing our engagement with that customer to help them find a solution to the outstanding balance, but there would be no additional information that is received from customers.

Q. Okay. Now, the list that we reviewed in the paragraph from the incident report begins with the statement that included the following

information. So that suggests that there may be other information that's not contained with -- described within that paragraph or other categories of information. Can you tell us whether or not there are other categories of information beyond what we've been reviewing?

A. (Williams) Yeah, Mr. Roberts, the included language is probably more so to the point that not all of these pieces of information would be applicable to each customer, but this would be a comprehensive list of the types of information that was potentially exposed.

Q. You described it as a confident -- comprehensive list. I want to refer -- you can go if you wish, but in your rebuttal evidence, you also describe a category of information. And I'll just quote it here:

> Demographic and household information, such as the number of individuals per household and your household heat source[s]

That's at page 24 of 65 of Exhibit 17. And I'm wondering if you could describe that information and why you have that.

A. (Lanteigne) Thank you for the question. So just looking at what you're referring to specifically, we are talking about the privacy policy for Nova Scotia Power. And what this would include is information that -- like, a good example, I think, to provide is My Energy Insights. So the tool that allows customers to see their appliance usage and their interval usage. Within that information, customers do have the ability to -- you know, to complete a survey, which allows a customer to tell us what their household demographic actually looks like. And that is relevant information to help the My Energy Insights tool provide more accurate information to a customer. You know, if a home -- you could have two identical homes. If you have just a single person living in one and you have a family of five living in another, the energy use is obviously going to be different. So that helps inform the information.

So in those cases, if the customer elects to provide that information in the My Energy

Insights survey, we would have that information to help that tool provide insights to that customer.

Q. And was that information among the categories of information that were subject to the attack?

A. (Lanteigne) No, it was not.

Q. Now, reviewing these different headings of information, can you tell us how long it's retained and what the length of retention is based upon?

A. (Williams) So Mr. Roberts, we're back to the original paragraph? Are we talking about the list?

Q. Yes.

A. (Williams) Yeah. So for the most part, what we're looking at with this list is the information that would be included in Nova Scotia Power's Customer Information System, so the CIS. And so as we've discussed in our evidence, as I think we've discussed in previous regulatory proceedings, the CIS is a legacy

system. It's been in service for approximately 30 years and has been something that has been considered for replacement and the path to replace it has been one we've been on for a number of years now.

As a result of that, and as we've discussed in our evidence, the majority of this information is retained in CIS without the ability to remove it. There is no automation feature within CIS because of its vintage to remove that type of information, and furthermore, the manual deletion of that volume of information has -- comes with significant risk of impacting the system in a significantly adverse way.

So what has been done is, as I say, continue on the path to develop a CIS that has the functionality to remove that type of information, but also in relation to SINs, where we could, on a limited basis because of the nature of that information, we have identified that and we have not removed it -- not removed the data line from the system, but we've zeroed out those

numbers within the system.

[10:00:02] So in acknowledgement of the sensitivity of that and that there is no need to retain that information that we do have in relation to those SINs, that work was undertaken, it says in the evidence, beginning in 2018, and carried out in more fulsome manner in 2024. And then we're in the process of confirming removal throughout our systems currently.

But I think it needs to be clear that the CIS presents a limiting factor within our systems that the majority of customer information that would reside on that system is retained within that system, but the new CIS that we're developing we'll bring forward to the Board hopefully some time later this year will have as part of it the ability to identify and remove information like this on an automated basis.

VICE CHAIR DEVEAU; I'm sorry, Mr. -- pardon me. Well ---

MR. WILLIAMS: Mr. Deveau, just before

you -- I just want to make one more point.

VICE CHAIR DEVEAU: Okay, yeah.

MR. WILLIAMS: That Ms. MacDonald has just reminded me to make absolutely clear that the CIS itself was not compromised and that it was a cut of information from the CIS into the Azure Data Lake that was the source of this issue, for the most part.

VICE CHAIR DEVEAU: Right.

MR. WILLIAMS: So that's been a source of confusion in relation to the CIS in past proceedings, and I just want to make clear that the CIS itself was not compromised, in large part because of its vintage.

VICE CHAIR DEVEAU: Right. And sorry, I was -- I was thinking of Mr. Williams, but I was looking at Mr. Roberts. Sorry for the confusion.

So my question was that exactly. So you said that this information here that Mr. Roberts has referred you to was contained in the CIS, but I just wanted to confirm, as you explained in your rebuttal, that

it was actually not accessed from CIS by the threat actor. It was accessed from the staging area in the Azure platform for use in the My Energy Insights platform; correct?

So it was accessed from the staging area in Azure.

MR. WILLIAMS: That's correct. You were ahead of me even making that clarification.

VICE CHAIR DEVEAU: Right. And just previously, you indicated that the demographic and household info that was in My Energy Insights, that was not accessed either because it was in the -- it was in that platform, not in the staging area. Is that -- that's correct?

That's why it wasn't accessed, or that was not one of the types of info that was accessed because it was not in the staging area?

MR. WILLIAMS: Yes, that's our understanding.

VICE CHAIR DEVEAU: Okay. Thank you.

Sorry about that, Mr. Roberts.

MR. ROBERTS: Thank you.

MEMBER MELANSON: Could I just -- before we move off from the CIS, why -- is there anything inherent about the vintage of the CIS that makes it more difficult to access via the existing?

And I know I'm getting into technical a little bit here, but I'm just trying to piece it together.

MR. WILLIAMS: So yeah, I'm really hesitant to get into it too much, Mr. Melanson.

It is -- yeah. I think it's a little bit like asking -- you know, if I were to ask my kid to operate a VCR, it's a little bit like that. Obviously, I am incredibly oversimplifying it, but it is the vintage of the system as compared to the technology and the sophistication of the technology that was used. It just doesn't match up.

THE CHAIR: I had some follow-up ones on this topic as well, Mr. Roberts, but I'm content to let -- if you're going to continue on this path, let you go first and maybe before you move on to something else, I might jump in if you haven't covered it.

MR. ROBERTS: That's fine.

BY MR. ROBERTS:

Q. And I was just going to ask a follow-up to Vice Chair Deveau's question.

If you could explain in ways that perhaps someone less tech savvy like myself could understand, how did they get into the personal information if it wasn't directly into the CIS?

A. (Williams) So again, Mr. Roberts, I don't think you have to worry about the level of technicality that I'm going to come at you with here, but effectively what it is, is what Mr. Deveau described, which is that there was -- so within the CIS, as I've discussed, that's where the information resides within our

systems.

So if you think that as the source of the information, there was a cut of that information taken in 2021 and, as it moved over to the Data Lake, it moved through the Data Lake to be processed and then eventually used within the My Energy Insights project.

There was that cut that was -- that remains in the staging area of the Data Lake, and the Data Lake was compromised. And that's where the threat actor gained access to.

Q. And when you say the "Data Lake" that's -- you're describing the personal information of your customers?

A. (Williams) Well, now you're -- so the Data Lake is maybe -- one moment. I'm going to see if there's a better person to respond to what is a Data Lake on this panel than myself.

A. (MacLeod) The Data Lake does house data. It's conducive for big data, so when our AMI

deployment went live, that was a lot of data to consume. And really, when we say the Azure platform, it's really a platform that hosts the data repository where we can put large amounts of data, like AMI data, and organize it, do analytics on it, prepare it for uses like My Energy Insights.

So for My Energy Insights specifically, it requires some customer data and then their usage data that comes from AMI. So the AMI data is delivered to the Data Lake, the customer data is delivered from the CIS to the Data Lake, and that's on the Azure platform, and that's where it's organized and formatted for use for a third-party purpose, for instance, like My Energy Insights.

Q. And where did the intrusion take place, then, in that linkage you're describing?

A. (MacLeod) The threat actor was -- gained access to the Azure platform.

THE CHAIR: Okay. And I had a couple

of follow-ups in the area as well, Mr. Williams, really relating to your description of the interaction between the Customer Information System and the cut, as you called it, of data that went into the Data Lake.

So in terms of the Customer Information System first, you said it's a legacy system, it's 30 years old, and you couldn't have really pulled personal information out of it, although you did describe going down a pathway of starting to remove Social Insurance Numbers back around 2019'ish, '18-19.

Do I infer from that that you've really got 30 years of customer personal information in that Customer Information System? That's what we're talking about?

MR. WILLIAMS: Yes, sir.

THE CHAIR: And the cut that went into the Data Lake, was that a copy of the entire 30 years of personal information?

MR. WILLIAMS: That's correct, sir,

yes.

THE CHAIR: Thank you.

BY MR. ROBERTS:

Q. And I apologize again if this sounds like a simplistic question, but was any of the data -- personal information that you gathered from your customers retained in such a way that there would not be access to it from the internet?

A. (Williams) I'm just pausing, sir, on the -- you're probably getting outside my comfort zone and anyone up here's comfort zone, in terms of talking about access points. And not to avoid the question at all; it's a perfectly reasonable question. I just think to get into that -- such a discussion, we're probably better off having it as part of the cybersecurity portion of this process. Just to be clear, though, none of our systems are -- none of these systems we were talking about are directly linked to the internet. They're all intra, within the company.

Q. With some access points, obviously? External access points?

A. (Williams) There are access points. Our system has access points. Again, we're getting outside my comfort zone, in terms of access and how this happened, and how -- what the entry would have been.

But just to be clear, none of what we've talked about thus far, Azure, the Data Lake, as well as CIS, are directly linked to the internet, as we would all understand it.

[10:10:00] **Q.** Okay. Thank you. And the -- we've been talking about customer information, and I assume that it would also -- that what we've been describing would also apply to information of former customers?

A. (Williams) Yes, to the extent that we're going back to the question that the Chair had just asked, that there would have been former customer

information included within that category, yes.

Q. And you -- the -- you have, at this stage at least, an inability to excise that information, apart from the specific example you gave of the Social Insurance Number?

A. (Williams) That's right. For the same reason that there's no automated function, and to delete wholesale items out of the Data Lake, it is our understanding that -- and I want to be careful here. I'm not suggesting that it could not be done, but the risk that is being communicated to us of taking that on is a significant one, and given how integral the CIS is to the services we provide customers, it's not a risk that we feel is an appropriate one. And when I say risk, we're talking about what's been communicated as catastrophic failure of the CIS, if we were to undertake this. The risk is of that nature.

THE CHAIR: Can I just -- sorry again, Mr. Roberts.

Just you said just a second ago, and I think you misspoke, Mr. Williams, that the risk of wholesale deletion out of the Data Lake, I think you were talking about the CIS?

MR. WILLIAMS: Thank you, sir. Yes, I was talking about CIS. Thank you.

BY MR. ROBERTS:

Q. In terms of the retention of customer data, I'm going to quote from a response to a Board IR. It's IR-9(b), Exhibit N-10. If you want to go to it, please do. It's response to (b). And I'm just going to quote, not really referring to the facsimile build, but I'll give you the quote, and you can see if you can deal with it, or if you want to find the actual reference.

A. (Williams) Sorry, sir, which IR? Can you just ---

Q. It's IR-9(b) from Exhibit N-10, as I have it.

A. (Williams) Is this from the May IR responses?

Q. Yes, yes. Sorry. So I think it's -- it's page 4 of 4 of response to IR-9.

A. (Williams) I'm there, sir.

Q. Okay. And there's a brief statement at line 15. Again, a question of retention of data:

> Certain customer data was retained beyond the time frames contemplated by the Company's internal record retention standards.

And I want to ask you, what customer information are we talking about and how did the retention exceed your own standards?

A. (Williams) So I think with that statement, what we're referring to is the information we just discussed, which was the information contained in the Data Lake. So as I said in relation to CIS, there were limitations within CIS for that information that resided within that system. Once that information had been cut

over to the Data Lake, there was, as the Chair corrected me, there was the ability to remove data from the Data Lake. In fact, there were mechanisms in place, automated mechanisms in place, to remove data. So with that statement, what we are really getting at is the information that was included in the Data Lake, it was intended to be subject to removal mechanisms. In fact, within the Data Lake, within individual work streams, there was -- there were automations that were scanning for information on a 14- and 90-day cycles and removing that information. But for obviously very unfortunate reasons, when this information was included in the Data Lake, it was not made subject to that automated process, and that was an oversight.

Q. And in terms of the actual cyberattack, if it had been made subject to the limitations that you described, it would not have been there for the threat actor?

A. (Williams) It would not have been

there.

Q. And have you determined why those limitations were not in place, or at least did not result in the elimination of that data?

A. (Williams) We know that those -- the cycle and the removal of information was in place in other areas of the Data Lake. Obviously when you're setting up these workstreams, the automation -- there's a manual component to any automation when you initially set it up, and so we don't definitely know, just because of the passage of time, exactly what happened or why it was not. But as I've said, the automation was in place and was operational in other areas of the Data Lake, but it was not for this particular set of data.

Q. I want to ask you some questions about Social Insurance Numbers. You've referred to them a couple of times. First off, you -- or Nova Scotia Power stopped collecting Social Insurance Numbers as a routine form of customer identification in 2018?

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

Q. And why did you do that?

A. (Williams) I think, Mr. Roberts, and I think we've communicated this in some of the materials we've provided, but it was -- again, we're going back almost a decade to this, so my understanding is that it was related to the evolution of the privacy environment and as what was understood to be reasonable in any given circumstances. Like we said, we collected the Social Insurance Numbers obviously for the tax reporting purposes, which we still do, but also there was a period of time prior to 2018 where we were collecting them for identification purposes. I think as industry and possibly the public and society's understanding of privacy and the sensitivity of it, and the evolving nature of technology, there was, around thereabouts, 2018, an understanding that Social Insurance Numbers ought not to be collected anymore, that there are other and better ways of obtaining the information. And so the decision was made to cease

collecting those.

I'll add, and we speak to this in our evidence, that -- and this is just informal discussions, so I'm not prepared to put names on the record, but we do understand from our other -- from other industry participants that it was a practise that was generally applied within industry during that relevant period.

Q. And you would agree with the concerns expressed about Social Insurance Numbers, that one of the issues that relate to them is the fact that they're essentially permanent; that they can't be changed or deleted in any easy manner?

A. So yes. I mean, with the easy manner being the qualifier. My understanding is that they can be -- you can get a new Social Insurance Number, but I certainly would not dispute the fact that it is a sensitive personal identifier that is not easily replaced.

Q. Okay. And when you made this decision in 2018 to stop collecting them, you didn't purge

your system at that time, did you?

[10:20:00] **A.** (Williams) There was no wholesale purging. There was a process that was undertaken to -- and our customer service representatives were instructed to remove the SINs or zero them out upon -- in capturing them within the system. There was, over that period of time, beginning 2018-2019 through to 2024, discussions about how best to address that type of information within CIS, and eventually the decision was made to take the action that was taken in 2024, which was a wholesale removal of the SINs by searching for nine-digit numbers within the system and zeroing them out.

So there was a purge that took place in 2024, which is obviously prior to this attack, But as we've discussed, the cut that included SINs was made in 2021. So there's that intermediary action that resulted in the circumstances that we have here today.

Q. And again, you'll be aware that Ms. Ralph, on behalf of Board counsel, was quite critical

of, I think she used the word *ad hoc*, the *ad hoc* approach between 2018 and 2024 in terms of removal, and waiting six years, essentially, to take a proactive step to remove the SINs. What do you say to that?

A. (Williams) Yes. And I certainly understand your point. I wouldn't characterize it as *ad hoc*. There was a specific directive made to remove them as they were encountered, and there were ongoing discussions about the best manner in which to address Social Insurance Numbers within the system, and data in general within the system. And it was 2024 when that action was eventually taken in relation to the Social Insurance Numbers.

Q. And as a result of that, there were still Social Insurance Numbers in the system connected to customers in March of '25, when the attack occurred.

A. (Williams) So I just want to be clear on that. There were not -- there were not Social

Insurance Numbers as they previously had existed because those had been removed in 2024. So again, CIS was not impacted. So what was in CIS was not part of this discussion.

It is only because the cut occurred in 2021, when the Social Insurance Numbers, other than those that had been removed as they were encountered, the Social Insurance Numbers remained in 2021 when that cut occurred. But as of April 2025, the vast majority of Social Insurance Numbers had been removed from the system, with the caveat that once we had gone through the scanning of our systems to remove SINs there were one-offs.

And again, we're getting into the technical nature of CIS that I'm not really comfortable with, but there were some SINs found in historical records within CIS, but the list of SINs, as you would envision it, had been removed prior to the attack.

Q. So I'll just try put it simply: Had the purge been complete in March of '25, or were there

still Social Insurance Numbers -- customer Social Insurance Numbers in the system that would have been accessed, or potentially accessed?

A. (Williams) So I just want to make sure we're (inaudible due to audio quality) each other. When you say that -- so the purge happened in 2024, we're referring to it as the purge.

Q. And was completed.

A. (Williams) And was completed, yes.

Q. Okay.

A. (Williams) Yes. So the Social Insurance Numbers -- the wholesale removal of Social Insurance Numbers from CIS, was completed in 2024, but again, CIS was not impacted by the attack.

Q. And there were Social Insurance Numbers in the Data Lake, if I can use that word ---

A. (Williams) Because ---

Q. --- (inaudible due to speaking

over each other) ---

A. (Williams) Yes.

Q. --- that were impacted.

A. (Williams) Yes, because of the cut that had occurred in 2021.

Q. Do you know how many?

A. (Williams) I don't. I don't have that number, no, sir.

Q. Is it -- is it something that you can obtain?

A. (Williams) I can't definitively say if it's something we can obtain. I can certainly undertake to make the necessary enquiries, and if we can, to provide it. But I don't know that it's possible.

Q. Thank you.

THE CHAIR: So the undertaking is to enquire how many Social Insurance Numbers may have been resident in the Data Lake at the time of the cyberattack?

MR. WILLIAMS: And I think -- and if

we do have that number to provide it, yes sir.

THE CHAIR: And -- okay. So that will be Undertaking U-3.

UNDERTAKING U-3 - To enquire how many Social Insurance Numbers may have been resident in the Data Lake at the time of the cyberattack, provide that number if available, and how many were expunged in 2024

THE CHAIR: I assume in answering that, probably look at how many were expunged in 2024 from the CIS itself? Because I assume you weren't adding new ones. That would give you a ballpark. If you're able to determine that as well.

MR. WILLIAMS: Well, just to be clear, the number -- yes. So the number should be the same because ---

THE CHAIR: Except for those residual

ones that you didn't pick up initially in the purge in 2024.

MR. WILLIAMS: Yes, correct. Those may have been -- yes, I suppose there could be ---

THE CHAIR: Ballpark. It'll be -- it will be in the ballpark.

MR. WILLIAMS: It would be very similar, yes.

MEMBER MELANSON: So really -- just to follow up on Mr. Roberts' questions. Mr. Roberts was asking about the April 2025, the purge that happened before then. But really the issue is if the purge had happened before 2021, when the information was transferred or the cut was transferred to the Data Lake, if it had been done by then there would have been no Social Insurance Numbers that would have been accessed?

MR. WILLIAMS: That's right, Mr. Melanson. So in order to have avoided the 2021 cut residing in the Data Lake, the purge would have needed to

have -- in order to avoid that cut having Social Insurance Numbers in it, the purge would have needed to occur prior to 2021.

VICE CHAIR DEVEAU: And sorry, probably easier to do it now than later.

So if I'm -- if I understand correctly, obviously MyEnergy Insights is a newer platform, and there would be customers who have joined or who -- customers who have become new customers after July of 2021. They would have used MyEnergy Insights. So am I right that at -- in order to accommodate those customers joining after 2021, that information would have been transferred from CIS to the Data Lake for use in the MyEnergy Insights platform, but those cuts would have been purged. Is that -- from the Data Lake? The automation tool worked on those cuts, but not on the July 2021 cut.

MR. WILLIAMS: You have that correct, sir. As I was speaking to earlier, that we do know that the automation was working in other areas of the Data

Lake, and those cuts were subject to it. That's why it's isolated to this 2021 cut over.

VICE CHAIR DEVEAU: So when those subsequent cuts were made, it wouldn't -- it likely wouldn't have just included the new customers, it would have actually -- all the customer data from all the customers, including the -- including all the -- not just new customers, but all the customers would have been transferred to the Data Lake and the automation tool would have worked; they would have been -- they would have been erased.

(SHORT PAUSE)

MR. WILLIAMS: Sorry, sir. I just wanted to confirm my understanding, which was that it would have -- from -- on a continuous basis between the 2021 and 2025, it was incremental information that was moving. It was ---

VICE CHAIR DEVEAU: Incremental?

MR. WILLIAMS: It was not a full cut

each and every time.

VICE CHAIR DEVEAU: Okay. So it's just so you could recognize -- if you wanted new customers, it could isolate new customers.

MR. WILLIAMS: You could move the incremental data over, yes.

[10:29:52] **VICE CHAIR DEVEAU:** And after it's used by Insights, that's when the automation tool -- does it go from -- actually, from the staging area into the My Energy Insights platform, the information?

(SHORT PAUSE)

THE CHAIR: You're being very patient with us, Mr. Roberts. We appreciate it.

MR. MacLEOD: The way the information is delivered to My Energy Insights, it is delivered from CIS to the staging area. At that point for the specific purpose of My Energy Insights, it's taken from staging area to a preparation area where it's turned into a data set very specific to My Energy Insights. At that ---

VICE CHAIR DEVEAU: Within Azure or within My Energy Insights?

MR. MacLEOD: Within Azure.

VICE CHAIR DEVEAU: Okay.

MR. MacLEOD: And then from that preparation area where it's ready to go to My Energy Insights, that's where it's delivered from that prep area to My Energy Insights.

So it's not directly from the staging area. There's one more step in the middle that's in the Azure Data Lake and, from there, that's where it goes to My Energy Insights.

VICE CHAIR DEVEAU: So is it moved to that preparation area or copied to that preparation area?

MR. MacLEOD: It is copied to that preparation area.

VICE CHAIR DEVEAU: So there -- in the -- so there's a copy in the staging area, there's a copy in the preparation area.

MR. MacLEOD: That's right.

VICE CHAIR DEVEAU: And that would have been the case in -- for the July 2021 data.

MR. MacLEOD: Correct.

VICE CHAIR DEVEAU: So in -- the cut that was taken, was it a cut from the staging area and the preparation area, or just the staging area?

MR. WILLIAMS: I'd just like to be clear on that, Mr. Deveau. The automation to remove data was operational in the preparation area.

VICE CHAIR DEVEAU: Okay.

MR. WILLIAMS: So this is really isolated to the one area within.

VICE CHAIR DEVEAU: Okay. Thank you.

BY MR. ROBERTS:

Q. With that, I'm going to move on to another subject, that's the notice to customers that was provided at various points in the proceeding.

And just reviewing briefly, the attack

itself, you understand, was initiated in, was it March 25th, or what -- a date in March?

A. (Lanteigne) March 19th.

Q. March 19th.

A. (Lanteigne) Yes, sir.

Q. And you found out about it on April 25th?

A. (Lanteigne) That is correct.

Q. And the first notice to customers was given on April 28th?

A. (Williams) That was when we first made public statements about it. Yes, sir.

Q. Right. Not specific notice, but a public statement about the attack.

And you gave specific notices to customers beginning on May the 13th?

A. (Lanteigne) That's correct.

Q. Okay. And there were, as I understand the information, approximately 277,000

customers at that time who received direct notice that there had been a potential compromise of their personal information?

A. (Lanteigne) That is correct.

Q. And you -- on June the 25th, you advised former customers that their personal information had been affected as well?

A. (Williams) Yes.

Mr. Roberts, I think it might be helpful, sir, if we just refer to the evidence put forward by Nova Scotia Power, and beginning on page 44 of 65. So ---

Q. This is your rebuttal, are you talking about?

A. (Williams) That's right. Yes, sir.

It just -- and I don't mean to take you off track at all, but it does provide a good chronology of the communications that were made, not just

the direct communications that were in direct communications to customers, but also ---

Q. Sure.

A. (Williams) --- the press releases that were issued by the company as well.

Q. That's Exhibit 17, and page -- you're saying page 44?

A. (Williams) Beginning on page 44. Yes, sir.

Q. Okay. All right.

And we see the bullet points there. And my first question relates to the time between April -- or sorry, May 13th, when information was given to the 277,000 customers and June the 25th, when information was provided regarding former customers.

And first of all, was -- the information given to former customers, was that direct or was it indirect, given the nature of communication with former customers?

A. (Lanteigne) So to clarify, May 13th was direct communication. It was a letter that was issued to those customers. And that was based on the information that we had available at the time as the complex investigation into the sophisticated attack on Nova Scotia Power was underway and about a couple weeks old.

When we got to June the 25th, even though the investigation was by no means complete, Nova Scotia Power had the information, and, out of an abundance of caution, realized that potentially other active customers and former customers could have been affected by the attack, so we made the decision to provide all current and former customers with access to My True Identity for five years. And customers at that point in time would have received an indirect notification -- current and former customers, it was an indirect notification on June the 25th.

Q. Okay. Indirect notification of

their access to credit monitoring? Is that what you're saying, among other ---

A. (Lanteigne) Yeah, it was -- it was that they could have been impacted and it was the, you know, similar messages to what was in the letter what they can do in light of that, including access to My True Identity.

Q. And one of the points that Ms. Ralph made in her report was the time between May the 13th, June the 25th, she found that interval to be unreasonable. What do you say to that?

A. (Williams) Just one moment, Mr. Roberts. I'm just going to find the relevant page.

So sir, the best reference is probably where we were, so beginning at that page and following through that section. I would also note that Ms. Valdetero also addresses this in her evidence, although I'll let her speak to her evidence.

But I think what is important to

understand and what, with all due respect to Ms. Ralph, is there needs to be an understanding of the context in which we were dealing with at the time, and so that's not just responding to the incident and working within the confines that the incident provided to us, but also the work that is required to make notification of this magnitude and of this significance to this many customers.

So appreciate Ms. Ralph's view, but our view would be much different in that we were very timely with our notifications, and the timelines were certainly appropriate and reasonable, given what we were dealing with and what the magnitude of the task required.

And so happy to kind of read through some of the rebuttal evidence that we've provided, and Ms. Valdetero can speak to her evidence later in this proceeding, but I think there's a fair bit on the record between the two pieces of evidence that address the point Ms. Ralph has raised.

And again, difficult for Ms. Ralph to

provide a view without having the full context, which again, in fairness to her, she likely did not at the time of her opinion.

Q. There's another interval that's of note, and that's between June the 25th and the date in October when you advised another 97,000 customers that their information -- this is in addition to the original 277,000, another 97,000 customers that their personal information had been affected.

How do you account for the period of time between June and October, and was that reasonable?

A. (Williams) Yes. So I believe we address that beginning on page 49 of our evidence that we've been referring to, and Ms. Valdetero addresses it, I believe, beginning on page 9 of her evidence. So again, I'll let her speak to her evidence, but we believe it was reasonable. And again, we believe it was reasonable given the context and the circumstances. There needs to be an understanding of how resource-intensive and time consuming

an endeavour it is to understand and digest the type of information that could have been impacted, and then to identify and provide an appropriate notice to customers. [10:40:25] One of the reasons we did notify like we did at the end of June was the recognition that there was the potential, not yet to have been confirmed, that additional customers had been impacted. And so in an abundance of caution, we went out at the end of June and made the notification we did and extended the offer for the TransUnion service to all those customers, and then continued the work to further verify precisely who had potentially been impacted, and then notified those customers, as you said, at the end of October.

Q. And so what was it about those 97,000 customers that would not have allowed you to give them notice in the -- with the original group in May?

A. (Williams) So what it relates to is the time needed to review all of the files that were potentially touched -- or weren't touched, but potentially

taken. And so there was, in May, a file that we referred to as -- already that was apparent on its face, and we identified customers through those, but as we continued to work through the data and the files that were in the Data Lake and elsewhere, it was identified that those further customers had been -- had had information that was potentially exposed.

Q. And the nature of that notice in October was direct notice to individual customers?

A. (Williams) That's correct. On October 31st, it was letters directly to those customers.

Q. I want to talk about another subject you alluded to.

MR. ROBERTS: Unless -- I can see the Chair ---

THE CHAIR: No, just if you're going to transition to a new topic, it might be an opportune time to take our midmorning break.

MR. ROBERTS: Yeah, absolutely.

THE CHAIR: Okay. Appreciate it, Mr. Roberts.

So it's almost quarter to now, so we'll come back at 11:00 o'clock.

--- Upon recessing at 10:42 a.m.

--- Upon resuming at 11:00 a.m.

THE CHAIR: Okay. Mr. Roberts?

MR. ROBERTS: Thank you.

GLEN MacLEOD, Resumed:

CHRIS LANTEIGNE, Resumed:

LIA MacDONALD, Resumed:

BLAKE WILLIAMS, Resumed:

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

Q. I want to just go back to one point that was made before the break when Nova Scotia Power was discussing the additional notice to the 97,000 customers in October, and I just want to be clear that I heard you correctly. The explanation for coming upon those customers was essentially based on your work through

the Data Lake and elsewhere, and I wondered about that word "elsewhere". What are you referring to there?

A. (Williams) In relation to the 97,000 it's the Data Lake, but we were assessing at the same time what else was potentially impacted or accessed within the company. So it was the entire process, but the 97,000 come from the information that was in the Data Lake.

And I would maybe just ask Ms. MacDonald to provide a little context and clarity about that work and why it was so complex during that period, if that's okay?

Q. Sure.

A. (MacDonald) Yeah, so just -- we were conferring on the break about the conversation earlier about the cut, the 2021 snapshot that is in question. And just to sort of clarify, what we're talking about there is not a list per se that would be readily sortable and easy to sort of discern what's in or not in

this list. It's not a list. It would have been a cut of the entirety of the various layers and file trees and inherent program of CIS and the related technical details that would be involved in something of that nature.

So just to sort of provide context, this cut that we speak of is in no way a list. And so beginning in May through June in the various notification timeframes in question here, we would have had our internal as well as external expert consultants advising us and performing the work to review the layers of files and file trees in question to look for and confirm with precision or not where we would have instances where a list with direct notification was able to be determined and where we would need to continue to query and forensically analyze with the expertise of other programmers and consultants what we were dealing with with this cut.

And so the reason that there are various timeframes that would then inform the

communications -- communications would essentially happen immediately when we had confirmation technically about what was being deciphered from the files in order to produce a list, but the cut we're talking about is not in and of itself a list.

And so I think that's important in the context of it. Now that we look back, after we've analyzed and had the benefit of that work over multiple months, the way we can sum it up in a few words, it implies perhaps that it's simpler or a list that could have been queried in May and in June, and then why October? Well, it's because in parallel, as we understood things about these files in question, we continued to, in parallel, analyze both this cut itself and all the other aspects of our network as we were rebuilding and containing and ensuring that we understood what had happened with the hack.

And I think Mr. Williams might want to also elaborate on some of this before we move on to the

other topics, Mr. Roberts.

A. (Williams) I hope that was helpful, Mr. Roberts. We're coming to the realization maybe there was the assumption that this is just an Excel list, and well, why can't you read that quickly and get these notices out. And it goes back to the discussion I think we were having about Ms. Ralph's evidence. It's important to understand that context. In fairness to her, she, I don't think, had that context.

But it's also, and you'll see in the evidence, you know, it's not even work that we could have done internally. We're talking about in-depth forensic analysis, and we were required to -- we hired both KPMG and Deloitte to undertake the work. It was too much for even one of those to handle at the time, so we had to outsource it to -- both to try to get that done at a pace that we felt was acceptable.

Q. Okay. And I may be the only one in the room who needs to ask this question, but what is a

"cut"?

A. (Williams) I doubt you're the only one, sir, but it is literally as it sounds. It is effectively -- it's not a -- when we say, "Cut" it's more as I said before, it's a copy and paste, effectively. So if you were to do -- if you had -- just as you would with a Word document, is my understanding -- I'm just I'm again oversimplifying things, but for the purpose of this discussion, I'm confident that we're in the ballpark. So it really is just copying the data into the Data Lake for use there.

Q. It's a copy of a mass of data?

A. (Williams) That's correct.

Q. All right. Thank you.

THE CHAIR: And just, Ms. MacDonald, in terms of the work identifying customers, I'm just trying to understand even at a high level, using the same file, this copy, the July 21st, 2021 copy of the CIS data, you were immediately able to identify 277,000 customers

from that. Say it took some analysis to then identify a further 97,000 customers. It's not clear how you were able to do it in the first instance and what was different about those additional 97,000 that you weren't able to do it until October?

MS. MacDONALD: No, thank you, Mr. Chair. And I understand -- I understand the reason for the question. First of all, kind of as we've been explaining about the cut or the copy of the database itself -- and it's not one file, it's many files, file trees, layers of code per se. And because of the nature of CIS and how the fields work, many of which are free-form fields, which is a term that means, you know, the user can use different fields as they see fit. Back in '97 when that would have been deployed, that might have been a more typical or modern way of using a database, and of course, as we know, as time has gone on, databases and computer systems are more sophisticated and have less leeway in terms of how a user can input information or

data, so to speak.

So all that taken together, in addition to the more clear or perhaps more obvious places that employees and consultants would have initially looked for where might SINs be, there are other parts of the system in the file trees and places that are not as clearly searchable that we came to understand needed to also be queried and forensically analyzed in order to rule in or rule out whether there were SINs or other problematic data elsewhere in the various layers of what we were calling a file or a cut or a copy, but it is in fact not one static place but the millions and millions of potential fields and combinations of how the several years or decades of data would have come to have existed over those years.

So the querying of it for the first set would have perhaps been more straightforward and then the further ongoing ruling in or ruling out of where else could there be sensitive data required time and varying

degrees of both manual and complex consultant-driven analysis on our behalf.

THE CHAIR: And just to clarify, in your answer at one point, you focus specifically on Social Insurance Numbers. That really wasn't -- I didn't ask specifically about that. Was that to suggest that the Social Insurance Number issue had something to do with these further 97,000 customers that were identified in October?

MS. MacDONALD: No, not necessarily. It was just sort of anchoring in on the one sort of more obvious or interesting point in front of us with all of this, but it's really about any of that personal information. I'll look to my colleagues on the panel, if anyone needs to elaborate or clarify?

THE CHAIR: Thank you.

Sorry, Mr. Roberts.

BY MR. ROBERTS:

Q. I want to move on then and talk

about the subject of estimating -- or estimated bills. And just to put this in the perspective of work you were doing, you began estimating in June of ’25, issuing estimated bills, I should say?

A. (Lanteigne) Yes, that is correct. And if you would like me to elaborate, I can kind of explain what happened between April 25th and June to get to that point.

[11:10:02] **Q.** Sure.

A. (Lanteigne) I think what’s important to note, and again, we can expand on this, but I’ll just kind of start by saying, you know, billing had been effectively paused from April 25th to June 4th. That was not a decision on Nova Scotia Power’s part to intentionally pause billing. When we started resuming billing in early June, that was the first time that we were able to issue bills for the amount of bill cycles that occur in the run of a day. So as we worked to ensure that our teams had the ability to issue the bills and that

certain systems were in place for customers to support them, including MyAccount, so any customer receiving their bill via email could actually sign in and see the bill, and also ingesting payments so that we could show the payments that were made to accounts. Early June was the first period of time where we were able to issue bills to customers. At that point in time, we were estimating bills, you're correct, that went out.

Q. And the percentage of estimated bills that you were issuing, or really a number, to be fair, increased substantially in July?

A. (Lanteigne) That is correct. I think what's interesting about -- again, in June, essentially the bills that were going out the door were estimates. There were some limited exceptions to that. For -- essentially what we ended up having to do is we had to issue bills for the periods that they were missed. And then -- so the period of June was really kind of catching up so we could return to a normal billing cycle for our

customers.

In the first few days of June, while bills that were -- new bills that were being issued in June were based on estimates, there were a few instances where there were meter readings that were available for customers in the days leading up until April 25th, when we lost access to our systems. And some of those first bills in June actually did have reads on them, so that would affect the read rate in the month of June.

Q. Okay. And can you tell us, in terms of the estimated bills, how were they estimated? What process did you go through to estimate a bill?

A. (Lanteigne) Absolutely. So when Nova Scotia Power would -- estimating bills is a normal course of business for Nova Scotia Power and for any utility. You know, every year we do have a performance standard. That means that we estimate less than 2 percent of bills for our customers. When we have to estimate a bill, prior to April the 25th, for the about six years

prior to the attack, we would have leveraged our AMI technology to have a more precise estimate occurring for customers.

When we lost the ability to communicate with our meters on April the 25th, we also lost that kind of primary estimation logic, if you will. So what we had to revert to was the Customer Information System estimation logic, which has been used since the Customer Information System was installed, and also continues to be used in limited circumstances. For example, we do have opt-out customers. If there is a situation where we have to estimate their bills, that would be -- so we were using our Customer Information System estimation routine to estimate bills for customers when we resumed in June.

Q. So is that -- are you saying that that was based upon past experience, that -- the estimate that you issued then?

A. (Lanteigne) Yeah, so the estimate

itself would have been based on average daily usage at the premise that would have occurred in the same season from the year before.

Q. Okay. And this, we're talking about, I guess, early summer. So you're looking back early summer the year before?

A. (Lanteigne) It's essentially -- this is where I know the concerns had come up as we worked through this process. If you -- for example, if you received a bill on June the 15th, it would not look at your June 15th bill of the year before and actually apply the exact same amount. It would look at the average daily usage from the same season to apply an average daily calculation for the bills.

So what ends up happening in those circumstances is that, you know, for the most part, if nothing has changed for a customer, they're in the exact same premise, over a period of time, the estimation that would come through on their bills would be very close.

However, in individual moments, it could have been slightly under or slightly over, or in some cases, we do know that we've had customers who would have experienced potential larger variances. Those were typically in cases where we didn't have that good history for the customer. In other words, they might have changed premise. It might have been a new premise that they were in. Or they could have had a substantial change in the energy usage in their home. They may have installed heat pumps, for example.

Q. There were, you'll agree then, bills issued for more power than was actually consumed by the customer in the time period -- the relevant time period?

A. (Lanteigne) I think from my perspective, it's important to note, and we've been very clear and transparent about this, you know, an estimate is an estimate. So the Customer Information System would have, you know, made the determination on what bill to

issue for customers. We do know that in many cases, it was close. There were some variances that occurred. We saw, you know -- I would think that it was a little bit more on the underestimation side than the overestimation side. But it is very difficult to go back and ascribe actual usage to the time that it was used because you're looking at two different periods of time. And what I mean by that is if we did an estimate in -- on August the 18th, and then the next true read for the customer occurred on October the 18th, you'd be looking at two different periods of time. So it is very difficult to go back and determine exactly what was used in the period of time.

Q. I saw a figure in the material, and I can go to it if you wish, but approximately 24,000 customers received credits as a result of overbilling?

A. (Lanteigne) If we could go to that material, that would be great, if that's okay.

Q. Sure. Does that number ring a bell to you?

A. (Lanteigne) I'm -- the 24,000 does not ring a bell right off the top of my head, so I wouldn't mind if we actually found the material.

MR. ROBERTS: Okay. Hang on then. I'll go try to find it in my notes. If you -- this is Exhibit N-10, and it's Nova Scotia Power's Response to Board IR-23, and 23(b).

That's right. Thank you. And just go to the response, I think. Yes.

BY MR. ROBERTS:

Q. So you -- this is your evidence in response to the IR:

> 23,989 residential bills had a return of estimate bill (a 'true up' bill) where the new bill amount was a credit.

Now, am I reading that correctly? That those 24,000 bills would have been too high and that's why the person ended up with a credit?

A. (Lanteigne) Yes. So -- and apologies that the 23,989 didn't register as 24 in my

head. I appreciate you finding the evidence for me. But that would have meant that when the estimate was completed, when the next bill came in, there would have been a credit for customers.

I think what's important to note is that further on in the response to this is that we do notice that other factors are at play. So a credit is one element of things, but many of these customers actually had carried a credit in the past. So it didn't actually result in a new credit on the account. Some customers actually choose to carry a credit balance on their account. So I think that's an important issue to note.

The other piece about this in particular is that this specific example and this commentary was a result of the meeting that we had on November the 25th with the Committee for Natural Resources. That's what kind of generated the response to MLA Taggart. And we were specifically looking and commenting on a period of a few weeks in early November, from November 1st

to 20th.

So the way, just to elaborate if I could on the way the Customer Service Information estimates bills for customers. As mentioned it is -- it looks at seasons, but the legacy system, legacy estimation routine that we were leveraging, it really only considers whether the season was warm or cold.

So as we transitioned into November, the colder estimate had come through for the customer, and that did result in some bills being higher at the -- in the first few weeks of November. So we're specifically commenting on that period.

There's a couple of things that Nova Scotia Power did that I think are just important to elaborate at this point.

So the first is, really since the start of this incident, all together recognizing that we were having to estimate bills, we took the approach to think of our customers and make sure that everybody knew

we were not charging late fees/interest on overdue amounts, we were not disconnecting any customers who could not pay their bills. As we worked into November, we -- when we saw this issue, we actually did make some slight adjustments to the estimation routine after November 20th, when we heard this feedback from our customers.

[11:20:19] We also, at that point in time, we actually launched an online forum where customers who did have concerns could submit a photo of their meter read, and we would make those adjustments for customers in real time. And we even called some of the customers that we identified as, you know, potentially having those high estimates in the first weeks of November, to offer them that opportunity to send in a photo of their read, and we would make those adjustments.

So again, those approaches to ensure customers knew they didn't have to pay the estimate if they weren't comfortable, options for us to achieve the true read, those were the tactics that we put in place to

help mitigate that specific period of time which was part of this response.

Q. Okay. So as I heard you, first off, you say that not every one of the 24,000 residential customers' residential bills resulted -- was the result of overcharging on an estimate. Is that what you're saying?

A. (Lanteigne) That is correct, yes.

Q. But a substantial portion of them would have been, correct?

A. (Lanteigne) I think from our perspective, some of them would have been overestimated, yes. And this analysis as well does not consider the whole impact of the customers' experience. You know, the customers as well, like I mentioned, some of them may have been having a credit on their account, and some of those customers as well, you know, did not have to pay the amount that was outstanding too.

So -- but when we looked back and we tried to assess the estimate in hindsight, we did notice

that some of those estimates had been high, yes.

Q. But the problem that brought you to the legislature, and the problem that you addressed in this IR was customers being upset because of the -- of overbilling due to the estimates?

A. (Lanteigne) I think -- if I could clarify that because I actually -- I do agree that was part of it, but one of the larger pieces that we've seen from our customers is really the other side of that issue. So even in the month of November, which was not a peak month in terms of customer complaints that we actually had, there's really been -- and as we worked through the winter, there's really been three drivers that we've seen that's been driving a lot of the escalations that Nova Scotia Power has been receiving.

The first is that if a customer had been underestimated, and they actually had their true read come in, that true read amount, the large amount that was owing, that is what's caused concerns. And that's why

even though, you know, we've been keeping an eye on the customers' concerns about billing throughout this whole incident, the concerns that we heard from customers really peaked when the meter reconnection occurred at the end of December, and the true read rate increased dramatically in January, February, and March.

Additionally, during those periods of time where the peak escalations occurred, underpayment was also a driver. So if that underestimate with the true read resulted in a large balance, and the customer had been underpaying, that could have obviously grown the balance further.

Last, but not least, Nova Scotia Power is a winter peaking utility, so seasonal usage could be the third factor that could contribute to those results.

And again, I think that's been the driver of the vast majority of escalations and serious concerns that we've had from customers. It's what we've heard from customers in the community sessions that we've

hosted across the province, and we've done 11 of them in total, and being in there and talking to those customers directly, those are the concerns that they're having. It's really that true read experience that's coming back.

So I talked a little bit about how we weren't charging interest, we weren't disconnecting, but the other side of that is how to help customers with the balance. And we are ensuring that customers are aware that they can reach out to us, engage with us. We'll help them book the 24 months interest rate on any repayment of an amount because of a situation where they were owing arrears if they were underestimated, underpaid, or seasonal usage had caused an increase on the amount owing.

Q. Right. So again, if I can just cut through what you've said. You -- two primary problems. One of them was that you were underbilling customers, and when they ended up being assigned a proper billing method, if I could put it that way, they had a big jump in their bill. And the other, of course, was when

you were overbilling customers.

A. (Lanteigne) I think -- you're absolutely right. So if we would have been underestimating or overestimating, again, for many customers those estimates were close, but in those cases where it was under or it was over, that definitely could have caused concerns.

And I apologize for being longwinded, perhaps, but I was just trying elaborate is where we did see the bulk of serious concerns coming from our customers, and it was on that underestimate, underpayment and seasonal usage driving up balances.

Q. So why should a customer now be confident that the bill that they're getting actually reflects their power usage?

A. (Lanteigne) That's a great question, and it's a very important question. So I touched on it a little bit, but you know, if you think about it, for some customers the experience of kind of

having a reconciled bill, if you will, or a trued-up bill, would have started in July when meter readers were first deployed to gain energy usage. That number dramatically increased on December the 23rd, when we were able to issue our first bill using over-the-air data as our AMI smart meters had been reconnected to the system.

It did take until March 31st for that work to be completed, but we saw a significant increase in the true read rate occurring in January, February, and March, and by March 31st, we met that commitment we had made in November to reconnect all meters.

In April, May, June, and July, and August month to date, billing has returned to normal. The read rate on bills is back where it was prior to the cyber incident, which our goal again is less than 2 percent, as I touched on earlier. So it's not that customers have just received one bill, customers have now received multiple bills where those amounts have been based on a true read. So the bills are, again, updated and accurate.

Just to clarify, Mr. Roberts, if I misspoke. I just meant to say less than 2 percent of bills estimated is the standard that we aim for, and that's what we're achieving now.

Q. And during the height of this problem, you were up over 70 percent?

A. (Lanteigne) That is correct. In the first couple of months we were in that neighbourhood. And roughly speaking, and I know it's all listed, the specific numbers are in here, but from July to December, on any typical day, approximately half of the bills would have been estimated for customers. So it was, again, December 23rd was the key milestone that started the increase to get back to a normal rate of estimation.

Q. And if there were approximately half of the customers were being billed estimated bills, what read were you doing for the other customers?

A. For any customer, I guess for all of our customers, our approach, as we -- we talked about a

lot in June, how when we restarted billing, we did leverage estimates. We continue to leverage estimates, but we also -- we added a significant amount of meter readers.

So those -- the decision on as we were getting billing back and then adding meter readers, those two items were happening at about the same time in May, but we had to recruit, train, and safely onboard meter readers that were deployed in early July. So the meter readers began to -- that's what allowed us to begin to see an increase in our return, if you will, of true read rates in the month of July.

Q. Given the concerns you've acknowledged on the part of customers, both who were underbilled or overbilled, have -- has Nova Scotia Power reflected on what they might do in the future if there's an interruption to your billing system somehow?

A. (Lanteigne) Sorry, Mr. Roberts, would you mind repeating the question?

Q. Given the level of public concern that you've acknowledged, and not only here but elsewhere, on the part of customers who were underbilled or overbilled during the period you're estimating the bills, have you reflected on whether or not there would be another approach that you could take in future if your billing system was disrupted in the way that it was in this matter?

A. (Lanteigne) And I appreciate that. I think what I would -- what I want to say at first is, like, really two things to start with, and the first is that it's definitely not lost on Nova Scotia Power that, you know, having to estimate bills for a prolonged period of time has been a concern for our customers. So I believe we've acknowledged that, and I think it's worth acknowledging that again.

That said, I think that the approach that we took to issue bills to customers, I think we -- like, when we look back and we review that, I do feel that

we took the right steps and we made the right decisions to issue bills to our customers. I'm not saying it's perfect. I don't want that to be the impression I'm giving, but in hindsight, I do think that the approach that we took with the tools, the systems, the resources that we had, I think that they were the right decisions. [11:30:09] The one thing I will say, though, in terms of lessons learned on this particular topic and how to avoid prolonged periods of estimation, I think one of the things that we've done, you know, is, as we've restored and rebuilt our AMI systems and infrastructure, you know, we've had an eye on ensuring that there's more, I don't know what the right word would be, but perhaps robust redundancies in place to avoid a prolonged outage like this, because having to estimate bills, if we have to do it for a few weeks, that a lot different experience, obviously, than if we're having to estimate half of our bills for a period of eight months.

So in terms of that kind of approach

of trying to bring back the AMI systems with a bit more kind of robust business continuity protocols in place, if I could perhaps pass it over to Mr. MacLeod just to elaborate on that for a minute, because I think it is important.

A. (MacLeod) It is. And the rebuild of AMI, we've leveraged our vendor partners, so we're now in the cloud, effectively. So in the cloud, there's the ability to have -- to set up those architecture redundancies and more resiliency. So not to say a vendor might not be subject to a cyber event, but the ability to have that resolved in days or weeks, versus the number of months that we saw when we were hosting all this equipment at our data centre where the cyberattack occurred, we've drastically cut down that timeframe. So the ability to have the more robust estimation routines should be better at hand in the future.

Q. One of the -- you mentioned it briefly, Mr. Lanteigne, and the consultant for the

Consumer Advocate made some suggestions about the photo meter, the -- as an approach, receiving and using those in the course of creating a bill. Is that something you've looked at?

A. (Lanteigne) Yeah, like that feedback, we've reviewed that, obviously. And we actually -- we talked, as an organization, about photo reads, I think, as this incident unfolded. So I just wanted to add a couple of pieces for it that I think are really relevant to note.

So first and foremost, you know, our ability to kind of stand up the online form submission and then for the team members behind the scenes to process that information, it would have been -- it really would have been virtually impossible for us to do that in the immediate aftermath of the incident when we were focused on restoration.

As well, in terms of our BCP plans that we put in place, our efforts were to really, you

know, focus on the meter readers and focus on estimating bills. Those are the two tactics that we used.

I should add, though, that throughout the months leading up to November when we first put the form on our website, we did reactively take photo reads to help resolve disputes and provide clarity for those customers. We would do it reactively; we were able to handle that.

Listening to kind of the feedback, and you alluded to it as well with some of the concerns that came up in November, that's why we made the decision to actually put the form on our website. We had the ability at that time to process the requests that were coming in and we also, based on customer feedback, based on what we're hearing, based on the time that we had to be estimating bills, it made sense at that point in time to put the form online.

And the other thing that I would add, and I'm just kind of confirming, you know, again, always

open to feedback on our approach to doing things, but in the month of December, where this form was online, we were making customers really aware of it, we estimated 157,000 bills in the month of December. There was only about 500 submissions through this form. And we even heard feedback from customers and other stakeholders that, "It's not my job to read the meter. It's your job."

So while I -- again, you know, I think all feedback of this incident is welcome, I think that the approach we took to focus on estimation and meter readers, and then leverage the photo read when we recognized the length of estimation had taken some time was a good approach to have taken.

Q. All right. I want to briefly talk about another topic, and that's training. And here I'm going to go to Exhibit N-6, IR-1, and page 2 of 3. This is IR Responses to the Consumer Advocate.

And in this response, you -- and we see it there, you have provided a table showing the

failure rate among employees in their monthly phishing tests in the 12 months leading up to the attack, right?

A. (Lanteigne) That is correct, yes.

Q. Okay. And just to be clear, phishing is a way of gaining illicit entry into your system; correct?

A. (Lanteigne) That is correct, yes.

Q. And as it turns out, the actual attack was a phishing exercise?

A. (Lanteigne) Yeah, that is correct.

Q. Okay. So in the 12 months leading up to the attack, the failure rate in your phishing testing ranged between a low of 0.2 percent and a high of 14.3 percent, right?

A. (Lanteigne) That is correct, yeah.

Q. And to what do you attribute the range in the failure rates month to month?

A. (Lanteigne) Thank you. Just quickly talking about that, I think for me, like, the range of failure rates that you actually see across the board, it illustrates the fact that the training is -- you know, it does, at points in time, have some increased degrees of difficulty, which is what the intent of the training actually is. These training exercises are designed to -- we all participate in them at Nova Scotia Power. These training exercises are designed to try and really, if you will, trick the employee into clicking on a link that's in the email. And they'll often even look at, you know, kind of emotional or things that can really increase your level of urgency with the email. So it can be made to look like it is coming from your leader's name. It could be made to look like something significant is happening. I believe that there's one where we talked about how holiday schedules were going to be adjusted for employees. So there's items in there that really try to trick employees.

And I actually think, like reviewing this, that's it's a testament to the program. If every single month this program yielded a zero result, I would argue that the training and the exercises that's being delivered to our employees is not doing a good job of testing them.

I mean, if I could elaborate, I can talk on what we actually do if someone fails.

Q. Well, I ---

A. (Lanteigne) Yeah. Or you can ask on that.

Q. Yeah. I'll come to that in a moment, but just looking at these monthly totals, I appreciate what you're saying in terms of the variability in the actual testing, but in the month of November '24, more than 1 in 10, 14.3 percent of the employees failed the test. And so my question would be, what did you do about that? What -- how did you respond to that seemingly significant failure rate?

A. (Lanteigne) I can start with that and then I can pass it over to Mr. Williams to add as well.

So if an employee, you know, looking at the -- well, maybe I'll start at the high levels, if you will. So if there is a situation in the organization where we have experienced a higher failure rate, there is updates that are provided to the senior management and cascaded down to the management of the organization just to emphasize the urgency.

So that happens at a broad base, but at an individual level, if an individual actually fails a phishing exercise, they are automatically enrolled into mandatory training, additional training. We all do quarterly cybersecurity training, but they're enrolled in additional training as a result of the failure of that exercise.

Their leader is also notified of the failure, and the organization also tracks repeated

failures. And if an employee fails multiple times, you know, obviously the severity of any discussions that is -- are had with that employee would increase.

And maybe I'll pass it on to Mr. Williams just to elaborate a little bit on that, if I could.

[11:40:04] **A.** (Williams) So I think Mr. Lanteigne's kind of outlined in a general sense, Mr. Roberts, what is done. And you know, I'll add in a general sense is that we do now have a financial component attached to phishing testing, and if there are two failures, then there is financial consequences for our employees. So I think that's an important aspect to this.

In relation to the numbers we're looking at here, you get a high level, the sophistication of the phishing testing is elaborate. And I remember, I'm aware of exactly what it was in November of 2024. I'm not going to describe it on the public record for, I think, obvious reasons, but it was something that kind of ticked

all the boxes. When you do this type of cybersecurity training you're trained to identify certain triggers, if you will, within these types of emails, and it was effective, obviously, at triggering all of those.

In response to this, in addition to kind of the general approach that Mr. Lanteigne has outlined, this was a subject -- we have quarterly senior leaders meetings within Nova Scotia Power, and those are at the director level and above, and these results were specifically identified and discussed as a priority within one of those meetings.

So it is something that was -- is always at the forefront, but was responded to directly with direct messaging, as well as the general response that Mr. Lanteigne has responded or provided to you.

Q. And 14.3 percent is obviously a significant number, but the table shows us as well that in January and February of '25, the two months immediately preceding the phishing attack, your failure rates were

6.4 percent and 3.3 percent. Are those numbers concerning?

A. (Williams) I would suggest, sir, that anything above zero is concerning, given what we know can happen. But as Mr. Lanteigne has pointed out, if we had zeroes on these tests, then we'd probably have a problem with our testing. So while they're concerning, it's not as if they occurred in isolation and nothing was done about them. There is very concerted efforts, and there always has been, to respond to these and ensure that anyone who is falling victim to this testing is followed up with specifically, individually with additional training and their direct report is also made aware of it. So it's a discussion that those employees would also have with their direct report.

Q. And...

A. (Williams) Yeah, Ms. MacDonald is -- and apologies, sir, but Ms. MacDonald has just reminded me that exactly what happened in relation to this attack

is not specifically a phishing attempt. There was a phishing aspect to it, but there was effectively another step in the process that resulted in this, it wasn't just a simple phishing test.

So I don't-- I'm not suggesting this is the place to get into that further. I think that's for the next proceeding, but I think it's just a point of clarification. As important as the discussion is that we're having, there's another element to it that led to where we are today.

Q. Okay. And I take it that it's not something you wish to discuss now, what those -- what that other element was?

A. (Williams) I don't think it would be helpful for me to get into it, sir. The technical aspects of it are not something I'm 100 percent comfortable with. But again, not to avoid the question at all, I think it's perfectly an appropriate question to have answered in -- with a different witness, perhaps.

Not up here; I mean at the next proceeding.

Q. I'm in the hands of the Board on this. I mean, I would expect that you might be able to characterize, if not answer in any technical details, at least characterize what that additional element was, other than the phishing exercise.

A. (Williams) Yes. So my understanding is that it was a phishing exercise that then directed an individual to a website, which then was also compromised. So it's not that I see it as something confidential that I'm not prepared to speak to, I just -- more than what I just said, I can't really elaborate on.

Q. All right. Apart from the penalty consequences, if I can describe them, that may be applied to individuals who fail phishing training, are you doing anything different in terms of your training of your staff to be aware of and avoid these kind of intrusions and attacks than you did before March of '25?

A. (Williams) I think -- so for the

most part, I think what we're doing in response, a lot of it is on the cybersecurity side.

In terms of training, the training is -- the training, as it was prior to the attack, was, as you see, monthly; it continues to be monthly.

I think the one thing that is significantly different now than before, and this is probably something that could not have happened but for an attack like this, is a very focused and complete understanding of how significant this issue is and how important this issue is. And so from a cultural perspective, there has been a significant enhancement, I would say. There was always an appreciation of how important this was, but I don't think anyone can truly appreciate how important it is and how impactful it is until you've gone through something like this company has gone through over the last year to 18 months.

And so from a cultural perspective, there is a massive shift, and part of that you see -- and

I'll give you an example, sir.

We have a -- in the -- on the Regulatory team, there's a Teams chat for the team. It is certainly weekly, if not more often, where there are screenshots of emails put in that team chat and discussions about it as to whether this is a phishing test, whether this a legit email, that type of thing.

So that's the type of cultural shift that has arisen as a result of this, and that I think is more important than anything we could do in terms of the training. It's really self-training, where we have our monthly training, but in addition to that, our employees are working together, collaborating, and ensuring that this doesn't happen again.

Q. I just have one more small issue I wanted to deal with, and it's a -- I sent Mr. Norwood a document this morning, and I gave a copy to my friend, Ms. Power. It relates to claims made by -- that were repeated in the rebuttal evidence claims originally made

by the expert retained by Nova Scotia Power.

MR. ROBERTS: And if we could go first to Exhibit 17 of the rebuttal evidence, page 34.

Sorry, Mr. Norwood, I sent you off -- and yes, you have it right there.

BY MR. ROBERTS:

Q. This is part of the rebuttal evidence, and it relates to the question of the amount -- the period of time under which people would have access to credit checks, essentially, or credit protection. And Ms. Valdetero's statement, which is at line 8, says:

> I am unaware of any regulatory settlement, consent order, or adjudicative decision -- in Canada, the United States, the [U.K.], or Australia -- that has required an organization to offer or explore credit monitoring beyond five [years] as a condition of resolving...breach notification regulatory proceeding.

[11:49:52] And this morning, I sent Mr. Norwood a copy of a settlement, a court-endorsed and ordered settlement out of the State of Georgia regarding Equifax,

which had a serious data breach in 2019 -- or 2017. The court order was issued in 2019. And the summary from the Federal Trade Commissioner, which you see at the beginning, notes, among other things that the result of the settlement was a 10-year credit monitoring, four years plus an additional six, if the person wished to avail themselves of that, plus certain other benefits, if I can put it that way, to the individuals.

And I just -- I take it that when Nova Scotia Power adopted and repeated the statement of Ms. Valdetero in that reference I just brought you to, that you were not aware of this settlement?

MR. CLARKE: Mr. Chair, I appreciate the question. We have a hard copy of the material that Mr. Roberts provided. Nobody on this panel has seen this. So I'd like the opportunity to give this hard copy to the panel and five or 10 minutes so they can look at it and reflect on it before answering any questions, ---

THE CHAIR: Fair enough.

MR. CLARKE: --- since they haven't seen it before.

MR. ROBERTS: I did provide it to my friend this morning, but I take him at his word that he hasn't -- the panel members haven't seen it. But it is what it is.

I also want to point out that we didn't excerpt the entire decision. The decision itself is a couple hundred pages long. So we just have the initial portion of the decision.

THE CHAIR: Is your question just whether they were aware of this particular settlement?

MR. ROBERTS: That's correct. And I think we just got the answer.

THE CHAIR: Yeah. So Mr. Clarke, if that's the limit of the question, without getting into the details of the settlement, do we still need a break to have them review the document?

MR. CLARKE: Well, I guess I'd turn to

the panel itself, and if they're comfortable, I'm going to defer to them. If they're not comfortable and they'd see it, then I'd request we come back again.

THE CHAIR: Okay.

MR. WILLIAMS: Sorry; what precisely am I responding to at this point, sir?

THE CHAIR: I think it's just whether you were aware of a settlement involving Equifax that had a credit monitoring term that was 10 years?

MR. WILLIAMS: I can confirm that no-one on this panel has seen that document or was aware of that settlement prior to a moment ago.

MR. ROBERTS: Okay. Thank you. Those are my questions.

THE CHAIR: Did you intend to have that marked?

MR. ROBERTS: Yes, I'm sorry. Thank you for reminding me. I would ask for it to be marked as an exhibit.

THE CHAIR: Mr. Clarke?

MR. CLARKE: No issues.

THE CHAIR: So that would be Exhibit N-22.

--- EXHIBIT NO. N-22:

Equifax data breach settlement

THE CHAIR: Thank you, Mr. Roberts.

Small Business Advocate? And Ms. MacAdam, no restrictions on you at all in terms of time or anything, but just if you are still going between 12:30 and 1:00 and find a convenient place to break for a lunchbreak, that would be appreciated.

MS. MacADAM: Thank you. Some of my questions have already been covered, so I may be able to finish by then.

CROSS-EXAMINATION BY MS. MacADAM

Q. So I'll start -- I just wanted to follow up on the request for Undertaking 3, with respect to the amount of SIN numbers. And I'm wondering, would the number of SIN numbers that were potentially accessed be equivalent to the amount of letters that reference the SIN numbers potentially being accessed?

A. (Williams) They would for current customers, but letters were not sent to former customers, and the vast majority of customers where we had SINs for would have been the former customers, given the fact that we ceased collecting them in 2018.

Q. Okay. Are you able to provide the number of letters that were sent out that referenced the SINs possibly being accessed?

A. (Williams) Just give me one moment on that, Ms. MacAdam.

Q. Sure.

A. (Williams) Yes, so just to be

clear, so there was two separate letters sent out when we notified. One would have included the potential for SIN to have been exposed, the other would not. So in terms of the count on the letters that would have included the SIN as potentially, in the initial 277,000 it would have been, I'm going to say, approximately 154, just because I've got it written down here and I can't read my own writing. One hundred and fifty-four thousand (154,000). And then the same for the second, which is -- the second notification was 97,000 in total. And of those, approximately 74,000.

Q. Thank you.

A. (Williams) You're welcome.

Q. So I want to start, in much of your discussions and in the correspondence, there's a reference to customers, but then we've spent a lot of time specifically talking about residential customers. And so when we're talking about the breach with respect to customers, that does include residential and small business customers; is that correct?

A. (Williams) Sorry; could you just ask that one more time?

Q. Sure. Perhaps I'll rephrase it. When you were talking about 277,000 letters that were sent out, were they sent out to just residential customers, or were there any small businesses that were contacted that way?

A. (Williams) Apologies; the letters would have been sent to residential customers because they were notifying of the exposure of personal information, so the information that Nova Scotia Power would have had in relation to small business commercial customers would not have fallen within that category. That is not to say that there wasn't an appreciation for how the breach may also impact small businesses, and so again, that was part of the thought process in developing the robust communications process that was developed and rolled out, including the October -- or sorry; the June notification that all customers, current and former, could have

potentially been impacted.

So the letters, again, specific to those who would have had their personal information impacted, but certainly the communications process, as it was as a whole, was certainly recognizing that other customers were potentially impacted as well.

Q. And so within that CIS cut, there would have been information about small business customers?

A. (Williams) Yes, there would have been the contact information for those customers, yes.

Q. And I know my -- you spoke to my friend about the information that you obtained from residential customers. What is the information you obtain for small business customers?

A. (Lanteigne) So for small -- like a business customer that's setting up an account with us, obviously the business name would be something that's unique, a contact on the business that can be engaged to,

you know, work with the business. But then there's -- there are some similarities, the business address is obviously important to have as well.

So it really would be the same principle, the -- you know, the information required to establish and bill a business for their account. We may require the HST number for the business, just so we have that information on record as well.

[12:00:01] **Q.** What about bank account information?

A. (Lanteigne) It would depend if a customer has actually established preauthorized withdrawals for their payments through Nova Scotia Power.

Q. And you referenced a contact for the business. What information from that person would you obtain?

A. (Lanteigne) My understanding is it typically would just be name, phone number so we had a way to reach out, and we knew who was authorized to

actually conduct business with us on behalf of that business.

Q. And so if someone called in to talk about the business account, would there be any verification process with respect to who was actually giving that information about the business?

A. (Lanteigne) There would be, yes, but I'm not -- I don't have the specific procedure in front of me on exactly the verification process for a commercial customer.

Q. Would you be able to provide that?

A. (Lanteigne) We could undertake that, yeah. Yeah.

MS. MacADAM: If I could have that as an undertaking.

THE CHAIR: So you're looking specifically for the verification process for confirming the identity of small business customers?

MS. MacADAM: Yes, and the representative who's speaking on behalf of the small business when they contact NSP.

THE CHAIR: And you can provide that, Mr. Lanteigne?

MR. LANTEIGNE: Yes, we can take that, yes.

THE CHAIR: So Undertaking U-4.

UNDERTAKING U-4 - To provide the verification process for confirming the identity of small business customers and the representative who is speaking on behalf of the small business when they contact NSP

BY MS. MacADAM:

Q. And why -- while I recognize there's a difference between the personal information you talk about with residential customers and the information

you talk about for small business, you'd agree with me that some of the information you just described is potentially confidential, such as bank account information, if they've signed up for that, and contact information for the individual representing the business?

A. (Lanteigne) I would agree that the bank account information would be confidential, yes.

Q. And is -- so are small businesses able to obtain the credit monitoring that was offered to the other customers?

A. (Lanteigne) My understanding is that that credit monitoring is actually only offered to individuals by TransUnion, and also Equifax.

Q. So if we could pull up the rebuttal evidence, Exhibit N-17, page 5 of 100. On line 5, it says:

> On May 13, 2025, NS Power sent direct notification via letter mail to approximately 277,000 current customers...

Then on line 21 of that same page, starting at line 19, it says:

> Based on the customer complaints included in this record, most directly notified customers received their notification letters, dated May 10, 2025, via Canada Post on or about May 13, 2025.

And I'm just wondering, when were the letters actually sent if customers were saying that they received them on May 13th?

A. (Williams) So just to confirm, I think in -- the letters were, I believe, dated May 10th, but they were sent on May 13th.

Q. Okay. So I guess my question is, if they were sent on May 13th, how -- I guess the comment about "most directly notified customers received their notification letters" on or about May 13th. They wouldn't have received them the same day they were sent?

A. (Williams) I'd agree with you, Ms. MacAdam. They would have received them -- I'm not sure if there's a circumstance where they could have

received them on the 13th if they were sent on the 13th, but it would been shortly thereafter.

Q. Shortly thereafter.

A. (Williams) Yeah.

Q. Thank you. And then if we stay in that document, go to page 32, lines 9 to 12. This talks about -- this is in response to Recommendation 7 from InterGroup. And you talk about the codes. Starting on line 9, you say:

> NS Power has purchased a select number of additional codes for customers who contact the customer care centre wishing to enroll.

When you talk about a select number, does that mean once those codes have been used you aren't able to obtain anymore?

A. (Lanteigne) No. Essentially, all of the codes that were provided to customers through the direct and indirect notifications last year expired on December the 31st. Nova Scotia Power has taken the approach where if any residential customer, any person I

guess, calls in, and they might have missed the deadline or they want credit monitoring, we have made the decision that we've been granting that for our customers. We're just trying to do the right thing if someone legitimately missed out on the opportunity to sign up.

So that's really what that's speaking to. It's just that our approach has been to, even though all the codes have been expired since the end of last year, if someone calls and they have concerns, we're actually providing them with the codes that they can sign up.

Q. Okay.

A. (Williams) And just to be clear, when we're talking about the code being expired, they expire if they haven't been used.

A. (Lanteigne) That's right.

A. (Williams) So obviously if they've been used, they ---

A. (Lanteigne) Yeah.

A. (Williams) --- continue to be active.

A. (Lanteigne) That's right.

Q. And that means that if someone were to call up today and express concern and ask for a new code because they hadn't already signed up as of yet, they would be able to do that.

A. (Lanteigne) That is correct, yeah.

Q. Further on that same page, you refer to a lookup tool at line 19:

> Further, it is NS Power's understanding that these enrollment figures do not capture utilization through the lookup tool which accounted for a significant number of additional access code redemptions.

What is the lookup tool?

A. (Lanteigne) When we issued the indirect notification and the offer to all active and former customers on June the 25th, that they could receive a code to sign up for the five years complimentary

TransUnion myTrueIdentity service, essentially the way that that was done is with a -- you would come to Nova Scotia Power's website, you'd be able to search for your name in that information, and if the name came up with a match you'd be able to receive a code.

So the term, "lookup tool", would describe that functionality for customers to receive a code via the indirect notification.

Q. And so why wouldn't you be able to capture how many of those codes were issued through the lookup tool?

A. (Lanteigne) We don't have -- the codes that we receive from TransUnion, and we do comment in the evidence about the, you know, the total amount of signups, but it's not broken out between the different methods that a customer signs up, if it was codes from the letter, if it was codes from the indirect notification. We just know the total amounts. And then obviously, you know, the commentary about the sign up from the first

notification in May, there's some certainty of it because that was the only notification method that had been in place at that point in time, with the exception -- all throughout this, I mentioned earlier, how we've -- we do have like a small reserve of codes if someone has -- wants one now. But even from the beginning of this incident, if a customer had called us and they didn't get a letter, and they said, "I still want a code", we're doing the right thing for that customer and issuing them a code.

So we wouldn't be able to differentiate that either, but that would have been a smaller uptake than the direct letter that came through in May.

Q. Okay. So this is more about not being able to specifically identify what the uptake was for that look-up tool, but the actual uptake of those codes through the look-up tool is included in the overall -- in your overall understanding of how many look-up -- how many codes were utilized?

A. (Lanteigne) That's my understanding based on the information that's been provided by TransUnion. It's important to note we do not have any direct insight into that because the customer is signing up with TransUnion's myTrueIdentity service. So we actually -- Nova Scotia Power doesn't really have anything to do with that process itself, but based on the information that TransUnion has provided, that is our understanding, yes.

[12:10:00] **Q.** So if we go in the same document to page 18, starting at line 12, you have a discussion about the December 2024 privacy audit of Data Lake.

In INQ's evidence, which I can take you to, if you like, it refers to periodically audit internal access to PI to ensure that access to PI is only done for legitimate business needs.

And I'm wondering, when you're talking about this December 2024 privacy audit of Data Lake, was that doing what INQ was recommending in their evidence?

A. (Williams) Can we maybe just flip to the evidence? I would just prefer to have that in front of me.

Q. Absolutely. It's Exhibit N-14, page 9 of 29, paragraph 31.

A. (Williams) So I think this audit would in part be similar to what she's suggesting. I don't think it's completely what she's suggesting, and obviously she carries on to acknowledge that none of this arose as a result of internal access, and so not really determinative of any point as it relates to the attack and what happened thereafter. But this audit, we are providing a response to one of the IRs just to ensure that the record is as complete as possible. So yes, I think in part it is being responsive to the issues she's raised.

Q. Okay. And the audit of the Data Lake, would that have included -- I know she was referring specifically to access was only done for the purpose of legitimate business needs, but was there an audit done of

whether the individuals who have access are required to have access? I know -- I believe in one of the other matters before the Board recently, there was a discussion of ensuring that only those who legitimately need access to certain items needs to be reviewed on a regular basis.

I'm just wondering if this December 2024 audit would have included that issue?

MR. CLARKE: Mr. Chair, I'll defer to Mr. Williams on this. I do have some concern with respect to the confidentiality of the audit. I have no concern with the question, but the confidentiality issue with respect to the audit. So just remind Mr. Williams of that, and he can make a decision on whether he wants to answer at this point.

THE CHAIR: Thank you, Mr. Clarke.

MR. WILLIAMS: I appreciate the reminder. If I can just take a moment, I'm going to see if I can thread the needle here, Ms. MacAdam, and give you a response despite the confidential nature.

Ms. MacAdam, do you mind just repeating the question, and I think I'm in a position to ---

BY MS. MacADAM:

Q. Sure. I want to know whether the December 2024 audit of Data Lake included within it determining whether the individuals who had access legitimately required that access for the purposes of carrying out their work, or was there anybody who no longer needed access to it?

A. (Williams) Yes, thank you. So I think I'm comfortable responding on the public record that, yes, it addressed the issue you're raising.

Q. Thank you.

If we go to page 23 of N-17, so same document, on line 17 you talk about completing:

> ...a review of all the Company's privacy policies currently under review by a reputable and independent external security assessment firm approved by the OPC.

Is that LevelBlue that you're referring to?

A. (Williams) That's correct. So we have already had Gartner, who's an external consultant, review those policies, and the reference in this paragraph, though, is -- would be to LevelBlue and the process that they're undertaking as part of the OPC commitments.

Q. And if I understand from later on in this document, that's to be completed or estimated to be completed in October of 2026?

A. (Williams) That's right. I believe it's the end of October is the date in the letter.

Q. Yeah. And so if we go to page 59 at line 7, you say:

> NS Power is to inform the OPC in writing whether LevelBlue has made recommendations, which recommendations it accepted, and the reasons why any recommendations were not accepted.

Are you able to provide that document

that you're providing to OPC to the Board and intervenors?

A. (Williams) What you're referring to is whatever communication we provide to the OPC on or before the end of October?

Q. Specifically, when you talk in this paragraph about informing the OPC, yes, if a copy was able to be provided or notification if it's publicized on the OPC website, notification that it's been publicized?

A. (Williams) So I will say certainly with the caveat that I don't know yet what will be in that and whether there would be confidentiality restrictions around it, but otherwise, yes, absolutely.

Q. And as part of that -- I appreciate that it's talking about which recommendations are accepted. For those that are being accepted, would there be a timeline for the completion of those recommendations within that report, do you expect?

A. (Williams) I would -- I'm hesitant to say that without knowing what the

recommendations would be. It would not be -- I would suggest it would not be unreasonable for there to be timelines associated with certain recommendations, but again, without knowing what the recommendations are, hard for me to say definitely.

Q. Thank you.

A. (Williams) Maybe I'll just say, Ms. MacAdam, that regardless of whether there's timelines associated, I can assure you that Nova Scotia Power will implement those in a timely manner.

Q. Thank you.

In INQ's evidence, there's some discussion about a concern with the PI inventory, and I just want to understand. I appreciate that you're saying that you cannot identify what personal information may have been accessed, but I just want to confirm that if an individual contacts NSP and wants to know what information is contained in there file that could have been accessed, they would be able to determine -- they would be able to

confirm all the information that could have been accessed?

A. (Lanteigne) I think if a customer was to call us today and they want to know what information is available on file; we are able to help them understand that. I think some of the, you know, concerns that came from customers as we worked through this incident is that -- and as we talked about earlier, you know, our customer service associates would have access to what's currently on file for a customer. They would not necessarily have the information that had been stolen by the criminal when the cyberattack actually occurred. So our ability to actually confirm exactly what was taken is not there in all cases, and that's why our teams that have been supporting customers have been advising to follow the guidance that's been provided in the notifications to customers.

Q. Okay.

MEMBER MELANSON: Before we move on from that, if the information that was taken from the

Lake, the Data Lake, was in the CIS system that has been in existence for 30 years, but you still have access to this, do you not have access to the Customer Information System now?

MR. LANTEIGNE: Yeah, and thank you for the question. I think what I was -- and apologies if I wasn't clear. What I was trying to say is we can tell the customer what's on file for them now, but we would not necessarily be able to confirm what was on file in July of 2021.

MEMBER MELANSON: Why not? Don't you have the same information that was on file? Hasn't it been cumulative?

[12:20:03] **MR. LANTEIGNE:** The information that's in the Customer Information System would just be what's currently there. So for example, if -- I actually don't want to pick one, but if something had changed, that current record is what would be showing, not the previous record. Yeah.

MS. MacADAM: If we go to page 40 of this document?

BY MS. MacADAM:

Q. On line 11 it says:

> NS Power has been tracking and reporting costs associated with the cyber security restoration effort.

Can you just confirm where you have been reporting them?

A. (Williams) So there is -- in terms of where we're reporting them, I know there's current IRs in the regulated financial statement filing that are specific to that question. I wouldn't be able to provide you an answer, and rather than provide an undertaking, I would -- that question will be answered in the Regulated Financial Statement process with an IR that is currently outstanding.

Q. Okay. And you say -- so continuing on, it says:

A substantial portion of these costs is

covered through the Company's insurance policies, with any remainder being expensed by NS Power.

What do you mean by "Being expensed?

A. (Williams) Yeah, it might be helpful, Ms. MacAdam, to refer to the CA's IR-6, where there is -- I guess it's confidential, so foiled again. There is a breakdown -- for your information, I suppose, I'll just direct you to that. Maybe not on the record. There is a breakdown of what those numbers are.

But to get to the point of your question, in terms of what it means to be expensed, those are expensed in the year that they're incurred. So whether it was '25 or '26, those are expensed and written off as such. So they would not be costs that are being deferred in any way and carried forward to a future period for collection from customers. They're being expensed at the expense of the utility and its shareholder in the year that they're incurred.

MS. MacADAM: Okay. So if we go to

page 46?

BY MS. MacADAM:

Q. At line 8 you, you refer to sending proactive notices to Cape Breton media outlets, but on line 1 for June 25th, you say, "Via substitute notice on its website, in the media, on social media…" What was in those proactive notices to Cape Breton media outlets on June 30th that was different than the June 25th notice to the media?

A. (Lanteigne) The June 25th, we would have had media advisories on what's listed on line 1 through 6, as you mentioned, but for the other ones that were specific to regional areas, Nova Scotia Power was conducting community sessions across the province and informing -- really it was just reiterating some of those key points from the June 25th update, but also advising customers of the local sessions that were actually occurring. We did over 30 of those sessions in June and July to help our customers who required support signing up

for TransUnion's myTrueIdentity service. So that would have been the specifics of why they were regional, because if they were happening in those areas at that time, we wanted to make sure that the word was out to those customers.

Q. And would that explain why there's gaps between those notices?

A. (Lanteigne) That's correct. Again, I think the June 25th notices would have been all encompassing, getting out to all media about that update when we offered the five years of myTrueIdentity service to all current and former customers, and then the localized ones, the time between them just would have been the timing between when sessions were being held.

Q. Okay. Thank you. And then you were speaking with my friend earlier about the phishing failure rate from March 24th -- 2024 to March 2025. Are you able to provide an update for the period of April 2025 to date?

A. (Williams) We can provide that.

MS. MacADAM: If I could have that as an undertaking?

THE CHAIR: It'll be Undertaking U-5.

UNDERTAKING U-5 - To provide an updated phishing failure rate for the period of April 2025 to date

MR. MAHODY: Mr. Chair, I'm sorry to interrupt, but on the undertaking list, Ms. MacAdam, a short time ago, had been referring to a filing that may be made with the OPC. And I -- it was unclear to me whether or not that would, given the time with which it's to be filed, whether that would appropriately form an undertaking or not, but as we move forward with numbering, I just wanted to capture that issue.

THE CHAIR: Yeah, I think that will occur after this process, so it's probably not an appropriate undertaking for the process. But thank you for raising that.

MR. MAHODY: Fair enough. Thank you.

MR. WILLIAMS: Mr. Chair, we'll -- I agree. Not an undertaking, but it is a commitment that Nova Scotia Power has made.

MS. MacADAM: And actually, I didn't take you to where the phishing description was, and I should have, because I have another question about that section.

So if we were to go to Exhibit N-6, IR-1, page 2 of 3?

BY MS. MacADAM:

Q. At the very top, (e):

> Please provide a summary of the number and types of cyber incidents NSPI recorded in the last 5 years? What improvements have been made to systems and practices as a result of these events.

I don't see -- if we scroll down, I don't see a response to that question.

A. (Williams) I don't either, Ms. MacAdam.

MS. MacADAM: Could I ask for that response as an undertaking?

THE CHAIR: Could you just repeat the request, Ms. MacAdam?

MS. MacADAM: Sure. Provide a response to CA IR-1(e).

MR. WILLIAMS: Mr. Chair, I would -- it certainly was not intentional not to respond to this question, but now that it's come to my attention, I do think that if we're going to provide a response to this, I would prefer to provide it in the context of 12273, rather than this proceeding, just given the subject matter and the nature of it.

THE CHAIR: Ms. MacAdam?

MS. MacADAM: I don't have difficulty with that. I'm not quite sure how we can keep track of that, but perhaps in the correspondence, you can indicate that that is responding to that question, just so that we can assure that it does get addressed.

MR. WILLIAMS: That's maybe a good suggestion, Mr. Chair. We could take it as an undertaking that we'll make the commitment, as part of the response to the undertaking, if that's agreeable to all.

MS. MacADAM: It's fine with me.

THE CHAIR: Okay. So that will be U-6, to confirm that that IR will be addressed in the other matter.

UNDERTAKING U-6 - To confirm that CA IR-1(e) will be addressed in Proceeding M12273

MS. MacADAM: If we go to Exhibit N-10, which is the Board IR's, at page 81?

BY MS. MacADAM:

Q. This is a question about:

> ...any memos, assessments, reports or email messages prepared by NS Power or on its behalf about its initial pause to customer billing after the cyber attack and its resumption of billing, including any discussions about the methods, processes [and] procedures it would use to estimate customer bills...

I won't continue on with the rest of the question.

My only question is, with respect to the response, is you say:

> To the extent potentially responsive documents exist, most of them are subject to privilege.

I'm just wondering, what type of privilege is being claimed?

A. (Williams) So I think, broadly speaking, what would be being referred to would be solicitor/client privilege.

[12:30:02] **Q.** Okay. And later on in that paragraph, I just want to confirm, you make a lot of references to IRs, and I appreciate with two matters, they get a little confusing. I believe when you refer to NSEB IR-12, filed September 5th, 2025, NSEB IRs 13 to 16 filed December 23rd, those are the IR responses contained in M12273?

A. (Williams) I believe both

packages have been included on the record in this proceeding as well though. And I agree, it is somewhat confusing, but I am fairly confident that both the September and the December IR responses are included on the record in 12600.

Q. Okay. But I guess the IRs were initially issued under M12273. I just want to differentiate between when you talk about the IRs 01 to 07 and 22 to 24, those are the ones that we're talking about in this actual document?

A. (Williams) You may have lost me here. So you're asking is NSEB IR-1 to 7 and 22 to 24, are they related to 12600 or 12273? Is that the question?

Q. Sorry, and I just want to differentiate between -- because when we talk about IR-12, and IRs 13 to 16, those are not the IR-12 and 16 in this document?

A. (Williams) Yes, I'd have to go back and look at them, but just reading this, I would read

it as the dates that were referenced, with 12 and 13 to 16 were specific to ensure that we're clear that those related to the prior rounds of IRs, whereas the latter versions, and we could probably just check even to see if there is 24 in the initial round, but I don't think there is. But I'm quite confident that NSEB IR-1 to 7 and 22 to 24 is referring to the May round of IRs.

Q. Okay.

A. (Williams) But I don't have ---

Q. So this document we're looking at?

A. (Williams) I believe so, but that's subject to check. I can take the time to dig it up if you'd like, but that's what I would read that as saying.

MS. MacADAM: No, that's -- I'm satisfied with that.

I only have a few more, so I think if I could just finish up?

If we go to Exhibit N-11, which is the SBA IRs, IR-19, which is on page 34?

BY MS. MacADAM:

Q. And in this question, it's talking about backups. And you provide some information about some backups that you did have. Did you have a policy about backups prior to the incident?

A. (Williams) I apologize, Ms. MacAdam, but that's likely a question that's better left for 12273. It is a cybersecurity-related question and I don't believe there's anyone up here that could provide an informed answer.

Q. Okay. On line 21, you say, "…except for certain backups from an earlier currency…" What do you mean by an earlier currency?

MR. CLARKE: Can we just scroll down the page, please?

MR. WILLIAMS: So again, I'll provide the same caution, Ms. MacAdam, but my understanding of

what an earlier currency backup would be is if you've -- and I'm just making up dates, so if you had saved something as of the end of 2025, the earlier currency would have been that backup as of the end of 2024. So separate backup, but from a later -- or earlier date, I suppose.

BY MS. MacADAM:

Q. With my friend, there was a discussion about the issue with estimated bills for residential customers, specifically with either estimated bills that were overbilling or underbilling. Were there similar issues with respect to small businesses?

A. (Lanteigne) Yes, the same principles would apply when estimating bills for a small business. So the energy that would have been consumed for a period of time, you know, we would be looking back at the previous seasonal usage and taking the average daily consumption during that same period of time. So it could result in a business having a situation where the energy

that was actually consumed in the premise would have been over or underestimated. And when we were able to obtain meter readings, the actual energy consumed would have been -- it would have been reconciled and trued up.

Q. And you mentioned that with respect to residential customers, I believe you indicated that it was the underbilling that was the more significant concern when the bills were trued up and there was a large amount. Was that similar or different with respect to small businesses?

A. (Lanteigne) I think the one difference that occurred for some of the commercial customers, business customers, small business customers, was that some of those customers are actually on a demand rate. So the -- you know, again, energy usage, the meters, even when they weren't connected, they continued to function as they should, recording energy, but Nova Scotia Power's ability to reset the demand on a monthly basis, that was also something that we were not able to

do. And when we actually looked at those -- when we looked back at those accounts, essentially what would happen was there would be periods of time where the peak demand would have existed over a period of, you know, several months, a couple months, it could have been just based on the time between the true readings on the bills. So for those customers, you know, it just added a different variability, where a customer could have had -- you know, their energy consumption might have been a little under or a little over when bills were being issued, and then the demand as well was not able to be reset.

So that's really just the other element for -- that affected many commercial customers.

Q. So if the demand wasn't able to be reset, how would you have determined it when you trued it up for that -- for the demand for that period of time?

A. (Lanteigne) Yeah, so our approach in just working with those customers is that we have

actually gone back and we've leveraged historical demand for the business. So again, in this case, pretty much all of these customers are billed monthly. So we've gone back and looked at historical demand for the same period of time from the previous year. I do think, you know, from our perspective, it's just allowed us to go back and ensure that we're, you know, probably billing the customers. So we get the rate energy usage, recognizing if the demand for a particular month wasn't able to attributed, it would be estimated for that period of time, but we would -- you know, we made adjustments based on what we saw in the history of that customer's file.

Q. And so is it fair to say for those customers with demand, their ultimate bill will never be exactly what it was because you have to make estimates with respect to those demands based on previous years?

A. (Lanteigne) That is correct. And our approach as we've been adjusting these is, you know,

we do understand that some of these commercial customers could have effectively been overbilled. We've also seen instances where the demand was applied and a minimum demand was applied for multiple months. So as we've reviewed those customers, we've made adjustments. We have not -- you know, any adjustments have been in the customer's favour. We haven't actually made any adjustments that would be trying to recover money from this issue, just recognizing the situation that occurred.

MS. MacADAM: Thank you. Those are my questions.

THE CHAIR: Thank you, Ms. MacAdam.

So we're at 20 to 1:00. We'll break for an hour for lunch, come back at 20 to 2:00.

As usual, caution to the panel, you remain under oath, so you can talk amongst yourselves, but not with anyone else about the testimony here today.

So we'll resume in an hour. Thanks.

--- Upon recessing at 12:39 p.m.

--- Upon resuming at 1:42 p.m.

THE CHAIR: Okay. Welcome back, everybody.

I think we were up to cross-examination on behalf of Mr. MacLeod.

GLEN MacLEOD, Resumed:

CHRIS LANTEIGNE, Resumed:

LIA MacDONALD, Resumed:

BLAKE WILLIAMS, Resumed:

CROSS-EXAMINATION BY MS. AKCAKIRYAN

Q. Hello. In terms of estimated billing practices, you had mentioned to my friend that Nova Scotia Power used historical averages of power utilization to estimate customers' bills.

How did Nova Scotia Power estimate customers' bills when they lacked data pertaining to customers' previous year's usage or historical data, say, for an individual who moved into a new residence?

A. (Lanteigne) In cases where there was no data to actually form an estimate, we would have sought to obtain a meter read. As I had mentioned earlier, we had -- we also hired meter readers to be out reading meters.

Q. Okay. And I just want to circle

back on the meter photo functionality on Nova Scotia Power's website. Approximately how many customers utilized this service?

A. (Lanteigne) In total, we received -- I think we processed just under 2,000 submissions to that forum. There was an additional approximate 1,000 submissions that were not processed because they were actually situations where the customer did have a true read on their account, so there was no adjustment that was required to the account.

Q. Okay. Thank you.

And in terms of those adjustments, how did Nova Scotia Power notify customers of any usage adjustments that were made following the evaluation of that submitted photo?

A. (Lanteigne) An immediate adjustment would have been made to a customer's bill for them.

Q. Okay, perfect. Thank you.

And Nova Scotia Power acknowledged in its rebuttal evidence that privacy incidents may carry residual risks.

A. (Williams) I believe that was acknowledged in the rebuttal, yes.

Q. Okay. And Nova Scotia Power also acknowledges that future misuse of the compromised information cannot be categorically ruled out.

A. (Williams) I think it would be probably helpful to go to the portions of the evidence you're referring to.

Q. Okay, perfect.

I believe it's page 34, line 24 of Exhibit N-17.

A. (Williams) If you want to restate the question, I suppose, but I think the words speak for themselves or what is stated there is obvious.

Q. Okay. Thank you.

So Nova Scotia Power nevertheless

opposes Mr. Mollard's recommendation to examine longer-term monitoring options and report those options to the Board.

A. (Williams) Again, I think the position's been outlined in the written evidence.

Q. Okay.

CROSS-EXAMINATION BY MR. MacLEOD

Q. (MacLeod) So my interest here is on the aggregation of data. We've been asking questions about, you know, the SIN data and the driver's licence, et cetera, but I'm more about aggregation, okay? And the reason I say that is because there's a lot of very valuable information that was possibly lost, all right, and that includes your name, your address, banking data, contact information, and your customer account, what you did within that account.

So my ---

MR. CLARKE: Excuse me.

Mr. Chair, I just would caution this gentleman that he's here to ask questions but he's not here to give evidence.

THE CHAIR: I think you just cut him off when he was saying "My question is".

MR. MacLEOD: It's all good. Right.

BY MR. MacLEOD:

Q. So my question is, did you spend any time or does NSP spend any time with the RCMP finding out what happens if that data would have been compromised prior to the -- prior to the breach? In the form of PD or something like that.

You mentioned earlier about quarterly-- yeah, quarterly level of -- sorry; quarterly senior level training for your senior management.

A. (Williams) Senior leadership.

Q. Yeah, sorry.

A. (Williams) No, that's okay.

So the question is, had we ever consulted with the RCMP to further understand the ramifications of such a breach?

Q. Yes.

A. (Williams) So apologies, Mr. MacLeod. Just taking the time to confer to make sure my understanding is consistent.

Not aware of any instances where we

would have consulted with the RCMP, but obviously, as is on the record, and happy to discuss further, we do have retainer arrangements and regularly consult with external parties, whether they be experts in privacy, cybersecurity, all of those matters. We have -- we have consultants that we engage with to better understand the environment in which we're operating within.

Q. Okay. So if you had something like an exercise with your senior management, did you ever tabletop it, or...?

[1:49:57] **A.** (Williams) So we have done tabletop exercises. In terms of the specifics of that, I'm hesitant to get into it in this portion of the process, especially on the public record. But yes, we do carry out tabletop exercises.

Q. Okay. Those tabletop exercises, do they understand -- sorry; do you -- did practise happen, what happens after an event or is it just, you know, trying to prevent an event?

A. (Williams) So in short, yes. I mean, we have, as you've seen on the record, specific procedures in place in terms of how we respond to these types of incidents. And obviously, a significant matter of evidence on the record here details what that response was.

Q. Right. So if I asked you, like, what would happen if somebody's address and name and that kind of stuff is, you know, exploited, you'd be able to tell me what happens to that person? Like, do you have a deep understanding of what goes on?

A. (Williams) You know, so what you're asking is specific to individuals, I suppose. So certainly we have an understanding of what information is sensitive, what information has the potential to be harmful and the reasons as to why it is sensitive and why it could be harmful for individuals.

You know, what the specific ramifications could be for any particular individual is

obviously specific to them.

Q. That's not necessarily true, but okay.

Is the information that -- for an account, is that siloed or is that collected together within an account just generally? I'm not looking for -- I'm not a technophile.

A. (Lanteigne) Yeah, the information that's available for a customer in our Customer Information System would be grouped by the customer, so the individual on the account and their address and their phone number, for example, would be grouped together, you know, as -- I don't want to get into the technical elements of the system but, you know, it would be a one customer file, if you will.

Q. Okay. So with one customer file, that means that sufficient aggregate data to do some mosaic intelligence. So have you guys ever been briefed on mosaic intelligence and what it actually does?

A. (Williams) I can say myself, personally, I have never been briefed on mosaic intelligence, no.

Q. Okay. Thank you very much.

MR. MacLEOD: Thank you.

THE CHAIR: Thank you.

Industrial Group?

(SHORT PAUSE)

CROSS-EXAMINATION BY MS. RUDDERHAM

Q. Good afternoon. My name is Brianne Rudderham, and I'll be asking questions on behalf of the Industrial Group. I'll refer the question out to the panel, and I'll allow amongst yourselves to decide who's best to answer the questions.

I'll do my best to try not to repeat any of the questions that were asked earlier, but I might fall off on some.

So to start, would you agree that NSPI's public assurance to date has been that none of the restoration costs associated with the cybersecurity attack would be recovered from customers?

A. (Williams) Yes.

Q. And in saying no restoration costs will be recovered, I want to know specifically whether NSPI's assuring the Board and the public that it's not going to charge customers for any costs flowing from the cyberattack, or is that just limited to the costs

associated with restoring function?

A. (Williams) Do you have a specific cost in mind, Ms. Rudderham?

Q. Well, can we go -- you'd agree with me that there's both direct and indirect or downstream costs associated with the cyberattack?

A. (Williams) For the purposes of the discussion, I'm happy to say yes. Again, I'm not clear on what costs specifically you're referring to.

Q. Direct costs would be like the forensic investigations, remediations, restoring of the physical function or credit monitoring costs. Correct?

A. (Williams) Correct.

Q. Indirect costs could be, like, the cost of redeploying your employees to different functions, the overtime associated with certain things on having the available staff, project delays related to capital costs or operating inefficiencies; fair?

A. (Williams) Well, a lot of --

you've listed a lot of things there, so whether I would be prepared to agree that they're all indirect costs of ---

Q. I'm trying to understand -- let's start over.

I'm trying to understand what you're assuring the public of when you say that no restoration costs are going to be recovered from customers.

A. (Williams) Well, the company has been restoring itself since the incident occurred in April of 2025, so there would be costs arising as a result of that restoration in 2025 and 2026, still ongoing through this year. And I think what we've committed to is that any costs arising within that period would not be to the cost to customers, and I think that's evident given the place we are in within the regulatory environment, within the regulatory calendar.

So to expand on that, in 2025 rates would have been set in 2022 for 2024. They were not updated in 2025, so those rates were the same rates that

were in place in 2024 and had been approved in 2022. So there are obviously no costs from the cyber incidents in rates in 2025.

In 2026, the rates were just approved in the most recent General Rate Application, and as I believe everybody or most of the people in this room would be aware, there were no costs associated with the cyberattack in those rates that were approved by the Board for 2026.

So I think we can say definitively that there are no costs associated with the cyberattack that are in customer rates. There were none in 2025 and there are none in 2026.

Q. Okay. So to summarize, fair to -- so you -- the assurance is that if costs would have -- sorry; would not have occurred but for the cyberattack, then it's not going to be recovered by customers.

A. (Williams) Sorry. If costs were to be incurred but for the cyberattack. I'm not

following.

Q. Would not have been occurred but for the cyberattack, it's not going to be recovered but from customers.

A. (Williams) I'm still not following, but I'm comfortable saying it is definitely proven that there are no costs being incurred by customers that arise from the cyberattack.

Q. Okay. You're saying it's definitively proven. And as I understand, you're saying that's because rates were set in 2022 or in the GRA recently.

A. (Williams) Correct.

Q. That's your -- so you don't agree that there might be incremental costs associated with certain aspects of that GRA or those rates associated with the cybersecurity attack?

A. (Williams) I don't know how there could be.

I mean, if you want to provide me with a scenario, I'm happy to have the discussion.

Q. We can get into it a little bit later. But I guess what I want to understand is what's the significance of using the phrase "Restoration costs" rather than "Any costs".

A. (Williams) Well, I think the significance is what we've just discussed, that we're talking about the cost to restore to bring the company back to where it was, and ---

Q. But is it ---

A. --- those costs are being incurred -- were incurred in '25 are being incurred in '26.

Q. So NS Power, it's not an assurance that they're not going to be seeking any costs arising from the cybersecurity costs, it's just the restoration costs?

A. (Williams) Well, if you have a --

again, if you have a specific cost in mind ---

Q. Right.

A. (Williams) --- or a type of cost, I'm having to have the discussion. But I'm not entirely clear on what you mean.

[2:00:00] **Q.** How about the incremental costs of delaying a project, a capital project?

A. (Williams) So hypothetically if there were, and so those costs would be incurred in a future -- or be before this Board in a future capital application, then I think that it would be before the Board at that time to determine whether there any of those costs were prudent or imprudent.

Q. Okay. So if I understand you correctly, where NSPI is drawing the line as to what's going to be not recovered from ratepayers associated with the cybersecurity attack is anything above and beyond what is currently embedded in rates?

A. (Williams) Well, no. I think as

I just said, it would be anything in the future would be up to this Board to make a determination as to whether it was prudent or imprudent.

Q. Okay. So that's not -- the assurance doesn't go that far, then. The assurance is "We're going to leave that up to the Board," but anything in the current rate timeline, nothing above what rates are currently set at?

A. (Williams) Well, I think that what we've stated, I think very clearly, is that the costs related to the restoration, which were incurred in '25 and are anticipated to continue to be incurred in '26, will be to the account of the utility, and ultimately the shareholder.

Q. Can you tell me, then, what are the cost categories under the restoration costs associated with the cybersecurity attack?

A. (Williams) Well, those are included in the response to CA IR-6 that we mentioned

earlier that's confidential.

Q. Okay. I'll come back to that, then.

All right. So when my friend, Ms. MacAdam, was asking questions about the rebuttal, the rebuttal says that NS Power is tracking and reporting costs associated with the cybersecurity restoration effort. Correct?

A. (Williams) She asked me those questions, correct.

Q. Yeah. And I believe what your response was, is those costs are being reported in the regulated financial statements, and then also are included in the response to CA IR-6. Fair summary of your evidence?

A. (Williams) Well, I think a more specific summary would be that I said that there's questions currently within that process, the regulated financial statement process, that have been asked by way

of IRs, that would provide the information that I believe Ms. MacAdam was looking for.

Q. Okay.

MS. RUDDERHAM: Mr. Norwood, if you don't mind pulling up one of the exhibits that I just sent you on the break. It's from Matter M12835, which is the 2025 Annual Financial Statements of NS Power. And I'm looking specifically at Exhibit N-1.

BY MS. RUDDERHAM:

Q. Mr. Williams, I assume you're comfortable with or you're familiar with the financial statements that have been filed?

A. (Williams) Well, that's not my background, Ms. Rudderham. I think as you know ---

Q. Is there anybody on the panel who can speak to ---

A. (Williams) This document from a different proceeding? No, I don't believe so.

Q. Okay. If you don't mind going to

Attachment 2, which is at PDF page 23.

You agree with me that these regulated financial statements, they're public documents; correct?

A. (Williams) Correct.

Q. And I'm referring you to a note that's associated with the financial statement, and I'm looking specifically at the heading, "Cybersecurity Incident"; do you see that there?

A. (Williams) I do.

Q. And in it, the last paragraph there says, in the last two sentences, it says:

> The Company maintains cyber insurance coverage and is working with the insurer on the claims process. In Q4 2025, the Company recognized [1 million], after-tax, in costs related to the Cybersecurity Incident. For the year ended December 31[st], 2025, the Company recognized [7 million] in after-tax costs related to the Cybersecurity Incident. (As read)

You see that there?

A. (Williams) I see it, yes.

Q. Are you not familiar with any of

these figures?

A. (Williams) You're asking me if I'm familiar with the figures that you just read to me, or...?

Q. Yeah. I'm -- do you have any knowledge of any of these reporting on the costs associated with the cybersecurity incident?

A. (Williams) So I'm familiar with what I just read, if that's the question.

Q. Okay. Can you tell me what that $7 million, what are the -- what costs is that? What's associated with that?

A. (Williams) I don't know what the breakdown would be. As I said, there is a breakdown included in response to CA IR-6.

Q. Okay. So this $7 million figure for 2025, are you saying that that should be the same figure that would be included in the CA IR-6?

A. (Williams) No, I'm not saying

that it's necessarily going to match up. And that's, I guess, why I cautioned you when we first began this discussion about this document, that there's no-one up here prepared to speak to this document from a different proceeding.

Q. Okay. Can you clarify for me why this figure here is public but the figure in the CA IR-6 is not?

A. (Williams) Yeah. I mean, there's a more detailed breakdown and there's forecasts included in the document that's included as in response to IR-6. So I think the detailed breakdown you could possibly get, but certainly the forecast would be what would generate the confidential treatment, from my perspective.

Q. So would a breakdown of the total costs incurred associated with the cybersecurity incident be able to be reported publicly ---

A. (Williams) Well, my understanding is ---

Q. --- for 2025 and 2026?

A. (Williams) --- that's partially what's being requested in this proceeding.

Q. So why can't it be part of this proceeding that we're currently talking about, the accountability associated with the cybersecurity?

A. (Williams) Ms. Rudderham, I never said it couldn't.

Q. Can it?

A. (Williams) I don't know. Are you asking? I -- it's on the record it's being treated as confidential because there's a forecast included in it. If you have a specific ask, you could make it.

Q. Can the actuals from 2025 be made public in this proceeding for costs associated with the cybersecurity incident, along with the specified cost categories?

MR. WILLIAMS: So Mr. Chair, I'm certainly happy to commit to making the enquiry as to what

and cannot -- what can and cannot be made public and provide the details that Ms. Rudderham has requested. And if not on the public record, then we could provide them confidentially.

THE CHAIR: Ms. Rudderham?

BY MS. RUDDERHAM:

Q. For the request, the actuals are here in this publicly. Are you saying that the 2025 breakdown of cost categories is considered confidential? I'm just trying to understand what your qualification is for your response to the undertaking.

A. (Williams) Well, my qualification is what my qualification was when we started this discussion, that it's not my area. And so I'd need to ask other people to confirm that, and I don't want to speak to them.

Q. Okay. So why don't I make the undertaking to be the actuals from 2025 for the costs associated with the cybersecurity incident, including cost

categories, and while we're here, can we get an updated forecast for the 2026 as well?

A. (Williams) So I can confirm that if we're going to get into forecasts, then we're talking about our confidential treatment on that.

Q. Presumably, you can redact certain aspects that might be confidential.

A. (Williams) Are we -- are you talking about the 2025 numbers being unredacted?

Q. Yes.

A. (Williams) Yes, subject to the same caveat, that I will need to confirm that internally that there's no issues with providing the 2025 on a public basis.

THE CHAIR: Okay. So that will be Undertaking U-7.

UNDERTAKING U-7 - To provide the actuals from 2025 for the costs associated with the cybersecurity

incident, including cost categories, as well as an updated forecast for 2026

BY MS. RUDDERHAM:

Q. And apologies to -- while we're on this undertaking, are there forecasted costs also for 2027? Sorry; 2027 and beyond. I don't know where that would ---

A. (Williams) I don't know the answer to that question. We can certainly endeavour to include that as part of the undertaking. I would -- obviously, the same discussion that we had previously applies to 2027 as well, and that -- those rates were set as part of the last General Rate Application and any costs in 2027 would also not be included in rates.

[2:10:11] **Q.** Yeah, but I'm just looking for the breakdown of what costs are associated with the cybersecurity attack, whether or not they're recovered in rates or not. It's just the breakdown of the costs

associated with that.

A. (Williams) No, I understand.

Q. Okay. And so my friend, Ms. MacAdam, was asking about what does it mean when it says "Expensed by NSPI" or what does "Expensed by NSPI" mean. I'm not 100 percent clear on what the response was to that. Is it that it's absorbed by shareholders because the rates have not changed? I'm just trying -- or is it taken from another aspect of the budget?

A. (Williams) when we're expensing something, it's an expense we're incurring in that present period, and unless it's included in customer rates, it would be the expense of the utility, and ultimately its shareholder.

Q. So is it fair to say that some of those funds could come from another area of the budget that would have been allocated for something different?

A. (Williams) No, I don't believe it would be fair, because the funds that were allocated for

that something different would be needed for that something different.

Q. Presumably there's been some functions that were not operational during the period of the recovery after the cybersecurity incident; correct?

A. (Williams) That's not a presumption I would make.

Q. So you're saying all avenues of the business were still operational after the cybersecurity incident?

A. (Williams) Yes, I would be of the view that those functions were being fulfilled, yes.

Q. So the TVP rates were being fulfilled?

A. (Williams) The TVP rates were on hold for 2026.

Q. Presumably there was a budget for that?

A. (Williams) Not a specific

operating budget. It's one of many responsibilities that the relevant teams would have within their portfolio and it's just like any other matter that arises or falls away during any given period. That's just responsibilities, effort, resources shift accordingly. It's no different than many different scenarios within the company, some of which would be, you know, industry-specific tariffs or riders that come up in the normal course. So those are -- that's work and that's resources that are not included in a revenue requirement forecast or budget, but it's part of the responsibilities of the team that are included in that budget.

Q. Okay. The evidence does confirm -- NSPI has confirmed that they had redeployed employees from one area to another area to respond to the cybersecurity incident; correct?

A. (Williams) Yes, but in their areas of the business. So again, it's the same discussion I just had, where you're triaging within your area, so

you're dedicating your time and resources to whatever is the task before you, whatever is needed at the time. That's how any business works. You don't have employees that are designated to one project and that's it. They have a general responsibility, and as I said, as work becomes more demanding or maybe falls off in any given area, you recalibrate and refocus your efforts.

Q. Okay. So are you willing to agree that something that would have been budgeted, those employees or whatever those tasks were, would have shifted because of the cybersecurity attack; correct?

A. (Williams) No, not correct.

Q. Okay. You'd agree that NSPI did incur almost $2 million more of overtime expenses in its operating budget?

A. (Williams) Do you have a reference for that? I don't have that in front of me, but I'm prepared to take it subject to check, to keep the discussion going.

Q. It's Exhibit N-8. It's the responses to IRs from the Department. IR-6. And the figures are 1.735 million in customer care overtime and 207,000 in billing overtime. And I just rounded that up to about two million.

MR. CLARKE: Sorry; could we see that, please?

THE CHAIR: Exhibit N-8, Rob.

MR. NORWOOD: What page is it? Sorry.

MS. RUDDERHAM: I don't have the page number, but I have the IR number on the side. It's bookmarked. It should have IR-6. Is it there? Right there. That's right.

BY MS. RUDDERHAM:

Q. It's starting at line 13 there. I can give you a moment to familiarize yourself with that.

A. (Williams) Yes, and the last sentence there would be the crux of what you and I were discussing.

Q. It's absorbed in the rates currently; correct? Or in the rates that were previously set?

A. (Williams) I'm not sure I understand what you mean by "Absorbed in the rates".

Q. Where's the $2 million coming from?

A. (Williams) So that's, again, to the expense of the utility and the shareholder.

Q. Okay. So it cuts into profits, is that what I'm understanding you to say? Or is it taken from another area of the budget?

A. (Williams) Ultimately it would reduce what is provided back to the shareholder as a cost of capital. I wouldn't term it as profit, but the cost of capital.

Q. Okay. And I know you've said there's no cost to the ratepayers, or it's not charged to customers because it's in rates. That's the position;

correct?

A. (Williams) It's not a cost to customers because it is not in rates.

Q. Yeah, and the reason for that is because once the rates are set, any increased O&M cost can't be recovered after the fact; correct?

A. (Williams) Not absent a specific mechanism to defer and later recover those costs.

Q. But NSPI has the ability to adapt to the environment? They can move funds from one budget to another budget, depending on what the circumstance is in any given year; correct?

A. (Williams) I'm not sure I am prepared to agree to that. I don't understand the premise of the question, I suppose. To move funds between years? No.

Q. Not between years. I'm talking about budgets; you have budgets for a reason and things change; correct?

A. (Williams) They do, yes.

Q. You have to adapt to those changes; correct?

A. (Williams) I would agree.

Q. And that could involve moving money from one area, or refocusing, or redeploying, as the terminology has come up? Is that fair?

A. (Williams) Yeah, I guess the hesitation is with the moving money concept.

I mean, you change your budgets and you incur additional costs. The potential for that exists, yes.

Q. Okay. So I wanted to refer to the response to the IR that we've been talking about. That's Exhibit N-6, the response to CA IR-6(a). And that's at PDF page 13, I believe. Yeah.

So the IR's asking to quantify the costs incurred in response to the incident and to provide a forecast of remaining costs NSPI anticipates through to

December 2027.

See that there?

[2:20:11] **MR. CLARKE:** Just hold on one second, please.

Can you scroll down?

MS. RUDDERHAM: I was just reading the question that was before.

MR. CLARKE: Yeah, okay. That's -- just caution that the attachment is confidential.

MS. RUDDERHAM: Yeah.

BY MS. RUDDERHAM:

Q. You see the question?

A. (Williams) I do, yes.

Q. Okay. So then the next page has the response there, and it provides that confidential attachment we've been referring to, and it confirms that at that time, NSPI did not anticipate costs beyond December 31st, 2026; correct?

A. (Williams) This is what the words

on the page say, Ms. Rudderham, yes.

Q. Okay. I'm not going to ask about the confidential figures, and I know you're going to be providing, perhaps, some actuals that are not confidential, but I want to understand what, exactly, is included in that calculation of costs when it says, "In response to the incident"?

A. (Williams) Sorry. The wording "In response to the incident" is found where, exactly?

Q. In the question. That was what was asked. Then a confidential attachment was provided. And I want to understand specifically what that attachment is calculating. What types of costs or what costs are we looking at?

A. (Williams) Well, Ms. Rudderham, we could refer to the attachment, which is confidential. It's self-evident what those costs are.

Q. I'm trying to keep as much as possible on the public record, okay? And I want to

understand, when you're calculating what the costs of this incident cost the company, what are you calculating? What are you looking at?

Are those the costs above and beyond what's currently built into rates or is it costs that are -- like, I'm just trying to understand what you're actually looking at. What are these restoration costs?

A. (Williams) And I appreciate your efforts, and I think what I've said previously remains, which is that there were no costs to respond to the incident included in rates, so everything in response to the incident is over and above what would have been included in rates.

Q. So are you including O&M cost shifts?

Like, if you've redeployed an employee from one area to another area, are you including those costs?

A. (Williams) I think, as we've

discussed, that is not what occurred and that's not what we're talking about here. We're talking about costs over and above what was included in rates.

Q. So you're not capturing, like, productivity losses or anything?

A. (Williams) No.

Q. You're not capturing any incremental costs that might be associated with delaying projects or remobilizing after a project was stopped and then restarted?

A. (Williams) Those would be capital costs.

Q. So are capital costs not included at all in that figure, in that confidential -- I thought it was capital and operating costs.

A. (Williams) So I guess what I'm saying where I suggest that it's capital costs, those would be costs that would be approved by the Board as capital expenses, not costs that are included in this list

that we're talking about.

Q. So I guess I'm just trying to understand what is actually being captured. What are you tracking? What extra costs are you tracking?

MR. CLARKE: Mr. Chair, I'll leave it to you, but I think the witness has been responsive, and I think he's answered the question.

THE CHAIR: Ms. Rudderham?

MS. RUDDERHAM: I don't think he has, Mr. Chair. I'm trying to understand what I'm looking at, and first he said it was anything that came up afterwards, which presumably would include capital costs associated with getting the networking back on, and he said it wasn't capital costs included. I just don't ---

MR. WILLIAMS: I don't think I ever said it wasn't capital costs included. I just want to make sure the record's clear on what's been stated.

MS. RUDDERHAM: He had said - I had asked about the incremental costs and he said, "No, that's

capital". So I had said, "Okay. Well, then, is capital not included or" -- I'm just -- I can't quite understand what I'm looking at, what's actually being tracked, what's actually being recorded.

I just want to understand what I'm looking at when I see the costs of the cybersecurity incident. Where is that line being drawn?

THE CHAIR: So I guess two things.

One, I heard the response being you can look at it, and you can see the costs categories. I'm sensing that that's not cutting it, from your perspective.

I suppose the other thing is, is part of the issue we're having here because it's confidential and we can't really get to it directly or is it something else?

MS. RUDDERHAM: Well, I think that part of the response, the undertaking, is it's not all confidential. Some of it are actuals and it should be on the public record, so it's kind of hard to tiptoe around

because it's reported in one proceeding, not reported here. And I'm just trying to understand for the public record what costs are we looking at here that's made up this expensed amount at the end of 2025, the end of 2026, and potentially 2027.

THE CHAIR: And so why -- so the response that's basically you can look down and you can see what's itemized there and how the categories are described, what in that is lacking, from your perspective?

MS. RUDDERHAM: Well, first it doesn't say whether it's capital or if it's operating, doesn't say where it's coming from, other than it's expensed. So I'm just trying to understand when I'm looking at the impact to the business and the impact to NSPI and the impact to customers, where is this money coming from, I guess, and what's the impact on the business.

MR. CLARKE: And Mr. Chair, I thought he said again and again where the money's coming from. I think he's answered that two, three, four times.

(SHORT PAUSE)

THE CHAIR: Ms. Rudderham, I guess I'm not sure you're going to get anywhere else, in terms of just being referred back to the confidential exhibit. I appreciate your point that there's an undertaking outstanding that may leave these numbers in the public forum, but perhaps what we're left with, though, is if you come back to it in a confidential session and be more specific, that may get us further along, although I appreciate your efforts to try to get as much on the public record as possible.

[2:30:20] **MS. RUDDERHAM:** Maybe I can go about it another way to try and get the cost categories on the public record, where it's tracking, there's evidence that it's -- they're tracking using specific codes similar to, you know, the storm costs. So in the storm cost proceedings, all those categories are included on the record, but they're not included here.

THE CHAIR: Well, you could try and

you could see where you get, but I think the objection that Mr. Clarke has made, and I think it is well made, is that the same question seems to be put to the witness over and over again and we're not getting any further along.

MS. RUDDERHAM: Okay. Sure.

MR. WILLIAMS: Mr. Chair and Ms. Rudderham, if I may, in an attempt to be helpful, I do think the undertaking that's been provided will shed some light on this. And I also -- I know we referred to them before, but the IRs that are outstanding in M12835 are requesting exactly that type of information, and in fact request IR-14 is:

> If any cybersecurity incident costs were recorded in the Regulated Statements, please provide a breakdown by cost, category, account number, financial statement line item... (As read)

It's a detailed breakdown that's being requested there.

THE CHAIR: So in terms of the exhibit that's on the record, I understand there's a concern about

the forecast numbers in particular, and I think you were uncertain about whether the 2025 numbers would be confidential on their own?

MR. WILLIAMS: In general, actuals are essentially for public consumption. I just -- I want to make sure that I'm not overcommitting here. I would anticipate that we would be able to publicly disclose 2025, but anything that is still subject to a forecast of 2026 and beyond, we would need to treat as confidential, because obviously that has a potential to impact ---

THE CHAIR: The reason I was asking is could -- if we were to break for a second and come back with a version of that page that's attached there that just had the 2025 numbers, would she be able to talk about it?

MR. WILLIAMS: I'm happy to undertake the exercise, and we would need to seek confirmation externally off this panel that we could disclose those numbers, that there's not some reason that we're not aware

of. But at the end of the day, sir, it doesn't get us any further than what Ms. Rudderham can read for herself in terms of those line items. We can't break those down further up here on the stand. The information that will be provided in the understanding and that will be provided in the Regulated Financial Statement proceeding I think is more voluminous than what we'd be able to do here on the fly.

THE CHAIR: Her questions, I guess, would at least be able to be a little bit more specific and in a public session.

MR. WILLIAMS: I would agree, but I think the line items that we're speaking to will be in the public realm as a result of the undertaking, would be my assumption.

THE CHAIR: Right, but she's asking questions today.

MR. WILLIAMS: I understand. Like I said, I'm happy to undertake the exercise. I don't know

that it gets us much further.

THE CHAIR: Ms. Rudderham?

BY MS. RUDDERHAM:

Q. I can't remember off the top of my head, but do you know when that response to the IR from the Board on the Regulated Financial Statements would be filed?

A. (Williams) September 3rd.

Q. Okay. Is it able to be done sooner on this record? Just that one response.

THE CHAIR: Sorry; what one response are you asking him for now, Ms. Rudderham?

MS. RUDDERHAM: The -- on the Regulated Financial Statement, the Board asked questions about itemizing the cost of the cybersecurity and it would have been by cost categories, I assume more detailed than what's provided in the confidential response to IR-6, and perhaps that would be sufficient, if it was truly a breakdown of all the cost categories under the Regulated

Financial Statements, and then I can move on. I'm just -- I guess I'm having a hard time understanding where we're delineating between, like, the confidential -- sorry; the full session and when we're going to actually get an opportunity to review the costs associated and whether the costs incurred were in fact reasonable or if they're trackable as being recovered from customers. Perhaps it's for another matter. I just -- I had thought that the costs associated with the cybersecurity incident was a matter for this proceeding.

MR. WILLIAMS: I think as I've heard, so there's -- I wouldn't anticipate there to be any process to determine whether the costs thought to the account of the utility and the shareholder that are not in customer rates are reasonable or not.

THE CHAIR: So on that point, though, Mr. Williams, each year Nova Scotia Power is subject to return overearnings to its customers. So everything you expense, down to the bottom line, potentially impacts that

calculus; correct? In any given year, regardless of what rates are.

MR. WILLIAMS: It has the potential to, yes.

THE CHAIR: Yeah. So for example, if you took all of the cybersecurity costs that were expensed in 2025 and added them back to the financial statements as if they weren't expenses, your return would be different than what it is with them included?

MR. WILLIAMS: It's an exercise that potentially would have merit if you added them back in and at 40 percent equity you were at a 925 percent return, yes, but I don't think we're there, sir.

THE CHAIR: Well, we don't know, because we don't have the numbers.

MR. WILLIAMS: That's why I said, yes.

THE CHAIR: So in terms of the costs and there being only a possibility of possibly impacting shareholders, that's not necessarily the case?

MR. WILLIAMS: You have to get through the first wicket too.

THE CHAIR: Understood.

MR. WILLIAMS: So there's a preliminary question before you embark on that type of exercise.

THE CHAIR: The preliminary question being?

MR. WILLIAMS: That even if you did include all those costs, would you be back to (inaudible due to speaking over each other).

THE CHAIR: You get beyond the upper threshold.

MR. WILLIAMS: Yes.

THE CHAIR: Yes, yes. No, that's understood, but that's a question. It's an open question.

MR. WILLIAMS: Yes, but you do not have to have this discussion before you answer that question. That question would be a preliminary question

before you would need to embark on a more detailed examination of the cost.

If you're not going to be at 925 at 40 regardless, then there's no point in even assessing those costs.

THE CHAIR: How do you know where you are if you don't assess the costs?

MR. WILLIAMS: Well, you'd know what the costs have been that have been incurred and ---

THE CHAIR: Sorry, yes, that's what I was talking about.

MR. WILLIAMS: Yeah.

THE CHAIR: And I think that's what Ms. Rudderham was looking for. And we're going to have the breakdown there, potentially something else coming in the IR response in that other matter, and then an undertaking response in this matter?

MR. WILLIAMS: Yes, I think so. But again, you know, a test of the reasonableness of those

costs is only something you would embark on if you're even in a position to be at 925 and 40. Otherwise they're just to the expense of the utility and the shareholder. There's no potential for it to incur costs on behalf of customers if you're not at that upper threshold.

THE CHAIR: Go ahead.

VICE CHAIR DEVEAU: Yeah, I'm just -- I mean, you could add it back, but you could also be deemed, you know, in some proceeding, imprudent. So you'd have -- you know, there could be directly two different calculations and it would impact -- I mean, I suppose all we're saying is your statement that, you know, it's paid by the utility and ultimately the expense of the shareholder is not absolutely right, depending on -- again, depending on the overearnings and where that falls, where the range is, whether you add them back or they're imprudent. That's going to be a -- potentially it could impact -- because all these -- if they're expenses that are paid by -- they're paid for money earned through

rates.

MR. WILLIAMS: I would disagree on the last point, but I agree with you that the preliminary question would be ---

VICE CHAIR DEVEAU: They're not paid from rates? If they're expensed they're not -- if they're in your Regulated Financial Statements, they're not paid from rates? Where does the money come from, then?

MR. WILLIAMS: Ultimately those are the costs of the shareholder. They're not customer costs.

VICE CHAIR DEVEAU: That are recovered through rates.

MR. WILLIAMS: Well, no. The shareholder would accept a lower return on its investment as a result.

VICE CHAIR DEVEAU: Perhaps, if it's -- depending where it falls on the range, in the range. If it's overearnings it could still be ---

MR. WILLIAMS: So yes, if we're into

the -- again, though, I think there's....

My point, I don't disagree with ---

VICE CHAIR DEVEAU: Right.

MR. WILLIAMS: --- what's been said. My only point is that it's a detailed exercise to assess the reasonableness of costs. We don't need to go there, though, if you're not even in an overearnings position. So if you're not at 925 and 40, even with those costs, then it matters not because the customers are not paying for any of those costs and they have no potential to flow back to customers through the FAM.

[2:40:04] **VICE CHAIR DEVEAU:** Right.

MR. WILLIAMS: So ---

VICE CHAIR DEVEAU: But would they ---

MR. WILLIAMS: --- the only question would be the 925 and 40.

VICE CHAIR DEVEAU: They can't do that analysis right now, though.

MR. WILLIAMS: No.

VICE CHAIR DEVEAU: No.

MR. WILLIAMS: No, not -- I think that's the genesis of the question.

MEMBER MELANSON: There's another aspect to it, which is to the point that Ms. Rudderham was trying to measure I think with her questions, which is there were estimates on everything, projections forward on every cost that Nova Scotia Power generated, including revenue requirement when you do a GRA. None of those costs or almost -- well, I shouldn't say none, but for the part, those estimated costs will not be the actual costs when you have to do your financial statements. There will be costs. Some costs are higher in some categories, some costs are lower, and as long as the costs are generally in that range, you would earn what you're expecting to earn. Would that be a fair assessment of how a GRA works?

MR. WILLIAMS: Well, my view would be that a GRA works in that it's approving an envelope, it's not approving specific cost centres.

MEMBER MELANSON: Right.

MR. WILLIAMS: And so it's approving a prudent cost envelope. And so to go back and look at how those amounts are expended within that envelope would be retroactive.

MEMBER MELANSON: Sure. But when you say that the costs of the cyber incident are absorbed by the shareholder, that is not necessarily the case if you simply reduce costs in another area to make up for that money you've expended in the cyber -- on the cyber incident, the restoration costs of the cyber incident.

MR. WILLIAMS: But again, that's not how the approval is issued. The approval is issued on the envelope. So ---

MEMBER MELANSON: Sure.

MR. WILLIAMS: --- if it's over and above the envelope then they're to the costs of the shareholder.

MEMBER MELANSON: Right. Perhaps

debatable. I'll leave it at that.

MR. MAHODY: Mr. Chair, rather than get my oar in this water while it's too late, I was intending to ask for CA IR-6, Attachment 1, the portion that could be filed non-confidentially, to be filed that way. I'm talking about the categories in the 2025 costs that have been incurred.

I know that's a subject matter of an undertaking, but as a matter of course, panels have been able to -- witness panels have been able to look at certain information and say to the Board, "No, that's no longer confidential. That can now form part of the record." And I think it is worthy of consideration whether or not the process is improved by having that information sooner, like today, as you had suggested, rather than awaiting an undertaking that will come in after the chance to question this panel has expired.

THE CHAIR: Mr. Clarke?

MR. CLARKE: I think I'm going to

defer to the panel with respect to the appropriateness of that request.

THE CHAIR: So I think if ---

MR. CLARKE: Sorry. I should have said that panel.

THE CHAIR: That panel.

(LAUGHTER)

THE CHAIR: That panel can go first, then we'll see ---

MR. CLARKE: That panel.

THE CHAIR: --- where we are.

MR. CLARKE: Yeah, no.

(LAUGHTER)

MR. CLARKE: I can't tell your panel what to do, but I -- I'd like to hear from my panel.

MR. WILLIAMS: And I'm going to apologize. Ms. MacDonald and I were just talking, so I -- I'm not entirely clear how the request from Mr. Mahody differs from the existing one, so...

THE CHAIR: I guess the issue is whether, at least in terms of what we have before us, which is the confidential Attachment 1 to CA IR-6, whether that can be made unconfidential, at least to the extent of the cost categories and the incurred in 2025 column.

MR. WILLIAMS: So I think based on the discussions Ms. MacDonald and I have had, we would be comfortable with the cost categories, even at this point in time. My hesitation on the 2025, even though it is actuals, is the insurance element, and they need to go through insurance process and confirm the impacts or the benefits of insurance. I -- that's my hesitation on this. Otherwise, if it was just actuals I would say actuals we usually disclose without a discussion. But I want to confirm before we would be agreeing to disclose the 2025 amounts, that there is, in fact, no concerns internally.

THE CHAIR: Okay. And I think that's covered by your previous undertaking. But for purposes of our discussion today, we can at least refer openly to the

cost categories?

MR. WILLIAMS: Yes, sir.

BY MS. RUDDERHAM:

Q. Apologies for that whole, I guess, tangent.

So let's start with the first category that's included in the attachment. I'll just read it in, so you don't have to show it.

First category on there is "Containment and investigation." Can you explain to me what is included in that category of costs?

A. (Williams) So at a high level, that would be the costs in relation to the immediate response, so consultant-related costs for the most part. And then investigation I think speaks for itself. What flows from the containment and as we respond to the incident, getting a better understanding of it. And so those would be costs, as I said, consultant-related, legal counsel in the context of counsel specific to the response

and the impacts of the attack.

Q. So costs from, like, all those lawyers, I think you said, KPMG, LevelBlue, those types of costs is what you're describing, or...?

A. (Williams) Mandiant's, others, yes.

Q. Okay. The second category there, it just says "Customer"; what's included in that cost, "Customer"?

A. (MacDonald) That would include the projects and the restoration activities listed under the customer pillar in the monthly cyber reports. So things like "Restoring my account," the AMI heading system, and activities such as those.

Q. Okay. Then it says, "Cybersecurity"; what is included under that cost category?

A. (MacDonald) So that would include the initial remediation efforts to reestablish barriers

and other processes that were needed in the immediate aftermath in order to get back to where we were, where we needed to be to run the business to go forward.

Q. So is that separate and apart from "Containment and investigation"? I had thought that that was just referred to as the consulting costs in the immediate aftermath investigation and ---

A. (MacDonald) In some ways all of it is related. So we would have established these categories, and then no costs would be duplicated. So if something was more related to getting up and running with cyber requirements to go forward, that would be that category. If something was in the immediate, quote/unquote, "Containment" to understand what had happened, and how and why, and how to prevent further occurrence specifically related to the incident, then that would have been in the first category.

Q. So this one's the rebuild, the other one is identify and understand?

A. (MacDonald) Yes, you could think of it like that.

Q. Okay. So then the "ERP restoration," I assume that that has to do with restoring that specific function of the business. Is that right?

A. (MacDonald) Yes.

Q. Okay. Presumably -- you said there's no overlap, but presumably, there would have been investigation and containment efforts in relation to the ERP ---

A. (MacDonald) Right. So this is ---

Q. --- program as well?

A. (MacDonald) There's no duplication or overlap of costs, they're categorized separately and distinctly. But of course all of these categories would have interrelated components.

Q. Okay. And then "Technology enablement"; what does that involve?

A. (MacDonald) So that would involve reinstatement of certain network data centre backup recovery components. And again, what I'm looking at would be the labels in the monthly cybersecurity follow up reporting where we list with the Gantt chart the progress along with the remediation activities.

Q. Then you have "Restoration program office"?

A. (MacDonald) So that's the project management oversight that we've described in those monthly reports of the response itself.

Q. And then you have "Other"; what's included in "Other"?

A. (MacDonald) I don't have that at my fingertip, but we can undertake it. I think it would relate to the existing undertakings, to the extent we can provide more in either of those two.

[2:50:15] **Q.** I don't believe we have an undertaking that actually breaks down the costs more

granularly. And if you're willing to provide that as an undertaking for costs for 2025, forecasted and actuals for 2026 and onward, that would be -- are you able to do that?

A. (MacDonald) So I think with the same sort of qualifier, subject to check, that Mr. Williams described a moment ago, if there is a reason why either the 2025 or forecast 2026 details cannot be provided, we will have to indicate that in the undertaking. But if there isn't, then we will provide as much of it as we can.

Q. The categories wouldn't have to be confidential.

A. (MacDonald) I think the categories we're already talking about and then ---

Q. I'm talking about the more granular ones. Like, if you were to provide a more granular -- you're referring to the amounts being potentially confidential, but I'm wondering if these amounts can be broken down even further so we can

understand what's being included in what.

A. (MacDonald) And that's what I'm saying we need to take away and confirm whether we can or can't do that. If we can, we will do it. If we can't, we will indicate so.

Q. Okay.

MS. RUDDERHAM: Can we get that as an undertaking, Mr. Chair?

THE CHAIR: So a more granular breakdown of the table in Attachment 1, CA IR-6?

MS. RUDDERHAM: Yes. Thank you, Mr. Chair.

THE CHAIR: Undertaking U-8.

UNDERTAKING U-8 - To provide a more granular breakdown of the table in Attachment 1, CA IR-6

BY MS. RUDDERHAM:

Q. In terms of the response to the CA IR, there was an indication that there would not be any

costs beyond December 2026 -- sorry; December 31st. 2026.

Is that still NSPI's position?

A. (Williams) That's our understanding kind of further to the discussion we had previously that no-one on this panel has any information to the contrary.

Q. Okay. And you're aware that -- you've been referring to the monthly updates. There was a monthly update filed from the related matter last week; correct?

A. (Williams) That's correct.

Q. And I don't think we need to necessarily bring it up, but it's fair to say that there's several work streams that remain incomplete and there is, in fact, target dates that extend into the fall of 2026 or even early 2027?

MR. CLARKE: Could we bring that up, please?

MS. RUDDERHAM: Mr. Norwood, I had

sent that to you. It is not an exhibit in this matter, but I had sent you the document itself anyways.

It's the August 2026 11th monthly update.

If you don't mind scrolling down. I was looking at the table.

BY MS. RUDDERHAM:

Q. If you need a moment to familiarize yourself with this, I ---

A. (Williams) No, we're good.

Q. Okay. So I had asked for -- to confirm that some of the dates are extending to fall 2026 or even early 2027 there.

A. (Williams) No, not there.

Q. Okay.

MS. RUDDERHAM: Let's scroll to page -- could you scroll down just there, Mr. Norwood?

It's the one that refers to the Joint Use Agreement.

I apologize. It's pretty small here.

There it is, right there.

BY MS. RUDDERHAM:

Q. So you see the third row down, the very end, it says Q2 2027. Do you see that there?

A. (Williams) I do.

Q. So do you disagree that that says -- suggests that full restoration activities will continue into Q2 2027?

A. (Williams) I do.

Q. So then what does that mean?

A. (Williams) That's a regulatory schedule.

Q. Okay. So it says, "Forecast restoration of normal activities updated August 11, 2026" is the heading there. And here it says, "Q1 2026 to Q2 2027." Can you explain that to me, then? Why is it going into 2027?

A. (Williams) I'd have to look at

the previous update, but if we want to scroll back up, the table we were referring to is the Gantt chart that was on the screen initially. That's the restoration timeline.

Q. Okay. So then what is this table for?

A. (Williams) Those are regulatory proceedings.

Q. Okay.

MS. RUDDERHAM: Scroll down. Scroll down there.

BY MS. RUDDERHAM:

Q. So when you say, then, "Regulatory proceedings" that go into 2027, are you just saying that that's when it's going to be complete and it's not when it's -- it's not impacted by the cybersecurity incident?

A. (Williams) I can't recall the specifics around that joint use proceeding, but yes, the costs we've been talking about and the schedules we've

been talking about are -- relate to the Gantt chart.

The table you've referred to is -- as I've said, it's regulatory proceedings and timelines related to those proceedings.

Q. It doesn't relate to the restoration timelines, restoring the function of those items that are noted?

A. (Williams) The timelines that are described in that Excel table relate to timelines of the regulatory proceedings and intervals within those regulatory proceedings. The costs and the timeline of restoration associated with those costs, again, is the Gantt chart that is on the screen currently.

Q. Okay. And separately from that, NSPI's committed to five years of credit monitoring through Transunion; correct?

A. (Williams) That's correct.

Q. In terms of the costs of that, are those all up-front costs or do they carry over to the

end of that five-year period?

A. (Williams) Those are all up front.

Q. Okay. And I think I understood the evidence that someone could request to be a part of that after the fact. Have those costs already been incurred or would those be additional costs?

A. (Lanteigne) Those costs are already incurred.

Q. Was it like a lump-sum fee?

I'm just trying to understand how the costs are already anticipated if new people sign up.

A. (Lanteigne) Essentially, it's similar to when we actually secured codes for Transunion. We would secure a block of codes and then we would actually deplete the block if customers request them.

The amount that we keep in reserve is extremely small.

Q. Okay.

A. (Lanteigne) There's not a lot of requests coming in. So we are, like, talking right now that there might be $100 of codes held in reserve.

Q. Okay. And I believe, Mr. Williams, you acknowledged or the evidence has acknowledged that there is risk of future malicious use of exfiltrated data. That can't necessarily be ruled out. That's fair. That's what you had indicated earlier.

A. (Williams) I think I'd agreed to the words that are on the page. I don't know if those exact words were used.

Q. Okay. Would you agree that that could create the possibility of additional financial obligations beyond 2027?

A. (Williams) I don't think I'm in a position to agree or disagree or really even have that discussion right now.

Q. Okay. Correct there's currently a class action by customers against NSPI arising from the

incident; is that correct?

A. (Williams) Sorry. I missed the question.

Q. There's currently a class action that's been advanced by a group of customers against NSPI in relation to the incident; correct?

A. (Williams) Correct.

Q. Has NSPI identified how those costs of either defending or resolving that claim would be treated for rate-making purposes?

A. (Williams) No, not at this time. To the extent that they were ever to be included in a forecast revenue requirement, we would make that determination at that time.

Q. So it's not insured?

A. (Williams) That's part of the discussion.

Q. Okay. Will NSPI commit that any costs associated with defending or settling or paying

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

A. (Williams) Nova Scotia Power is prepared to commit to it - it already has - in that customers will not pay for the cost of restoring the utility as a result of the cyberattack.

Q. Would these be considered restoration costs?

[3:00:30] **A.** (Williams) So I think whether or not those costs would be included in a revenue requirement in the future and subject to payment by customers would be a determination we would make if we had to make it. At this point, it's not costs that are in rates, and we would not anticipate incurring costs during a relevant period where we would need to have the discussion.

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

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

Q. Okay. I'm asking specifically about this class action. You had said, "We already committed to not doing restoration costs." I said, "Is this considered a restoration cost?" I don't believe you answered the question. Is this considered a restoration cost or are you going to commit that none of these costs associated with this action will be recovered from ratepayers?

A. (Williams) So, yes, what I'm trying to explain to you, Ms. Rudderham, is that the distinction you're trying to draw is immaterial because those costs are not going to be incurred in a period where we're coming before this Board with a revenue requirement application. So if they're incurred in '26 -- '25, '26,

’27, then it’s immaterial.

Q. But they could be incurred later, correct?

A. (Williams) And that would be a discussion that we would have as part of that proceeding, if we were to seek recovery of them.

Q. Okay. So I was asking whether you were going to commit if any time in the future. I understand then your answer is no?

A. (Williams) My answer is as I’ve provided twice already, that we’ve made the commitment we’re prepared to make.

Q. Okay. Now, sort of related to the insurance that we’re kind of talking about, I wanted to follow up on one of the recommendations from InterGroup, the consultant for the Consumer Advocate.

MS. RUDDERHAM: Perhaps it will be easier to pull it up. Mr. Norwood, if you don’t mind pulling up Exhibit N-13? This is the evidence of

InterGroup, and I'm looking specifically at PDF page 26. Yeah.

BY MS. RUDDERHAM:

Q. I wanted to ask you about the last two paragraphs on the page there, so in relation to recommendation 13. So InterGroup notes, it says:

> ...the magnitude of this claim may have future implications on NSP's ability to access cybersecurity...

I assume it's supposed to say cybersecurity insurance.

> ...in the future including higher premiums, stricter underwriting terms and increased deductibles. In InterGroup's view, customers should not be made to bear any increased premiums that may arise as a result of NS Power's insurance claim.

Do you see that there?

A. (Williams) I see what's on the screen, yes.

Q. And in the rebuttal to that recommendation, NSPI focuses on why any increased premiums

should not be blanketly excluded without a further improvement. Fair summary of what the rebuttal is responding to?

A. (Williams) Well, I don't want to get into whether your summaries are fair or not, Ms. Rudderham. The rebuttal speaks for itself and it's found on page 40 of 65 at line 20.

Q. Okay. So it remains unclear to me whether the risks that have been identified by InterGroup have actually been realized. So are you able to tell today whether NSPI has any indication that it may have difficulty actually obtaining cybersecurity insurance in the future or will be facing increased premiums or stricter terms?

A. (Williams) I think, again, what InterGroup is discussing and identifying is a potential in the future, and if that potential were to be realized, it would need to be addressed as part of whatever relevant proceeding those costs would be dealt with. That's

consistent with the rebuttal evidence.

Q. Yeah, and I'm asking if any of those concerns have been realized to date or do you have any indication ---

A. (Williams) Not to my knowledge.

Q. Okay. We sort of touched on this, and I'm not abundantly clear, would you agree that delayed capital projects may give rise to increased costs for things like reasons of inflation, remobilization costs, standby charges or extended vendor or consulting costs?

A. (Williams) Just as I would agree that delayed projects could reduce costs for customers, yes.

Q. Sorry, I didn't catch the end. Would reduce costs for customers?

A. (Williams) Delayed investment could reduce costs for customers, yes.

Q. At the time, but in the future --

I'm talking about when the project actually comes online. Would you agree that delaying a project can increase costs of the project, whether it's for reasons of inflation even?

A. (Williams) Just as delays could decrease for a variety of different reasons.

Q. Okay. So it could decrease or increase is what your distinction is here?

A. (Williams) Again, you're talking about hypotheticals, yes.

Q. Okay. Now, in the 2026 ACE Plan proceeding, I believe the evidence -- and you could tell me if I'm wrong -- that approximately 60 projects in 2025 were delayed, deferred or cancelled; fair?

A. (Williams) I don't have that in front of me, Ms. Rudderham.

Q. Subject to check, would you accept that?

A. (Williams) I'm prepared to accept

it subject to check, yes.

Q. Okay. And at least some of those projects in 2025 would have been deferred because of the cyberattack or the activities that came afterwards, decreased staff and things like that?

A. (Williams) That's where you're going to lose me. I don't think we're in a position to have that discussion.

Q. Do you disagree that some of the IT projects would have been delayed during 2025 because of the cyberattack?

A. (Williams) I'm aware of that, yes.

Q. Okay. Are there any other projects aside from the IT projects that would have been delayed or deferred or cancelled because of the cybersecurity attack?

A. (Williams) Again, Ms. Rudderham, I don't have the information in front of me, but I think

it may be helpful for the discussion you and I had about whether delays increase or decrease costs, I'll maybe ask Mr. Lanteigne to provide an example.

A. (Lanteigne) Yeah, so just to elaborate on what Mr. Williams is saying, that you really can't make a statement to cover everything, but you can talk about specifics. So in 2025, we delayed the launch of our Customer Care Modernization Project, which was replacing telephony. When the cyber incident/attack occurred on April 25th, in the week or two after that, we essentially put the full project on a full pause. You know, as the situation evolved and unfolded, probably about -- you know, it was in June, I believe, that we actually stood the project back up. So all of the, you know, resources that have been engaged have been stood down. You know, there's external, obviously, parties, including Amazon, who are helping us launch this project.

We ended up launching the project in March. The initial implementation timeline was supposed

to be June of last year. So despite the fact that that project came in nine months later, we did come in under the budget for that still. So it's an example where the investment had been delayed, it had been pushed out, and it allowed us to actually still come in with a properly managed budget for that initiative.

[3:09:52] **Q.** I appreciate that example, and maybe it's best by undertaking -- I want to know whether NSPI has analyzed and quantified the impact of the delay of any projects as a result of a cybersecurity attack? And I'm specifically referring to the capital project. Has there -- is there anywhere, or has NSPI analyzed what the financial impact has been?

A. (Williams) So again, these are all questions that would be assessed as part of those applications, and so whether there are -- just as there would be in the normal course when projects are delayed or accelerated, the questions would arise as to what impacts that delay or acceleration had on the cost of it and

whether they were prudent. So I'm not prepared to get into a discussion about project costs when there's processes in place that will deal with those.

Q. I appreciate that. I'm looking for it to be in one spot for easy consumption, I suppose, because there's a lot of capital projects, there's a lot of proceedings going on. I just want to know whether it's actually been analyzed and quantified, what the impact of the cybersecurity incident has had on capital projects?

A. (Williams) No, because, you know, its impact or its influence on each project would be specific to that project. There's no general principle or theory that can be applied to capital projects since they're all different, they're at different stages, the attack would have impacted them differently. Accelerations, delays would have different impacts on different projects. So no, we have not done that work, nor would it be beneficial to do it.

Q. I appreciate you're saying it

wouldn't be beneficial, but it's possible it could be done to analyze what the financial impact has been on capital projects from 2025-2026? It's possible?

A. (Williams) Well, it's possible because it's done on each individual project.

Q. Okay.

A. (Williams) But to do them in some aggregated form like you're suggesting and apply overarching principles or theories to it is not practical.

Q. And I'm not trying to apply overarching theories or things like -- I'm just trying to understand where I can look to specifically understand what the financial impact has been, or the cost impacts have been to the deferred capital projects. And what I understand you saying is, it's done on an individual basis and it can be found based on the projects as they come before the Board. Am I correct?

A. (Williams) Those capital filings would come before the Board and they would need to be

approved by the Board, and so any -- to the extent that there is any costs associated with a delay, and that that delay is determined to be imprudent, then those costs would be dealt with by the Board in the normal course.

Q. And on those applications, is there always reporting on, like now that the cyber incident has happened, whether it has been impacted by the cyber incident? Like, in those files before the Board, are you specifically reporting this was impacted by the cybersecurity incident and this is the cost implications of that?

A. (Williams) To the extent that there was a delay in cost implications, yes, those are identified ---

Q. Okay.

A. (Williams) --- and explained in all capital plans, regardless of the reason.

Q. Okay. I'm just trying to -- and I'm not trying to trip you. I'm just trying to understand

where I'm meant to be looking.

A. (Williams) I'm not worried about being tripped.

Q. Okay. A specific project or projects I wanted to ask about was the Dispatch Study Action Plan. Oh, actually, before I move on to that, in the monthly reports, there is a section about capital applications and impacts on the capital applications in that table we were looking at, correct? One of them, it's not the Gantt table, it's the actual table at the end that has listed impacts and it's broken down into various aspects, and one of them is capital.

MR. CLARKE: Can we pull that up, please?

MS. RUDDERHAM: Yeah, just scroll down to the table that we were looking at previously. Yeah, there. That one doesn't have the capital, but -- the capital projects. If you could just scroll? Right there.

BY MS. RUDDERHAM:

Q. It says Capital and ACE Plan. Do you see that there?

A. (Williams) I see it.

Q. And so I assume this is reporting on affected regulatory matters, correct?

A. (Williams) So you're referring to the top line that says capital budgeting and finance data?

Q. No, I'm just trying to orient ourselves as to what's being reported on here. I understand that the things that are reported on in this table are affected regulatory matters and this subsection is Capital and ACE Plan.

A. (Williams) Correct. Yes.

Q. Okay. So I only see there one project, which is the CIS Replacement Project, correct?

A. (Williams) I don't know what you see, but that's what's on the page, yes.

Q. Okay. We had discussed that there were other IT projects that had been delayed, and I

want to know, why is this only reporting on the CIS and none of the other projects?

A. (Williams) Well, I think it's reporting on confirmed or anticipated timelines. So the other projects wouldn't have necessarily fallen into the same category. I think CIS raises to a level of significance that the others perhaps don't.

Q. What about the IAN Project that was -- that's currently before the Board, and the decision, why is that not in here?

A. (Williams) I'm not sure. Is there a reason that you think it should be?

Q. Well, it was -- and I don't know if you were -- I can't recall if you were at the ACE hearing and we had gone over it, and the cost of that project had increased by about $5.5 million as a result of being delayed. Do you recall that?

A. (Williams) These are -- just to clarify, these are regulatory -- impacts to regulatory

schedules, not impacts to project costs.

Q. Okay. So is there any reporting on impacts to regulatory -- this is an affected regulatory matter, so this is your -- you're only reporting on dates, no other impacts?

A. (Williams) This is regulatory processes that have been impacted.

Q. So if it was delayed in filing, that doesn't qualify under that?

A. (Williams) So, correct. Again, these are intended to convey impacts to regulatory processes or schedules. The CIS Project, again, a bit of an outlier and included on here because of its significant relevance and the fact that it would be a substantive application.

Q. So when I'm reading this, this means ---

MR. CLARKE: Excuse me for a second. Mr. Chair, I was just wondering about

the mid-afternoon break and where we are with that?

THE CHAIR: Yeah, you were about to transition ---

MS. RUDDERHAM: I was, but I just wanted to finish this up first.

THE CHAIR: Yeah.

BY MS. RUDDERHAM:

Q. When I'm reading this then, does this -- okay. When I'm reading this then, does this mean that there are no other capital projects whose schedules were impacted by the cybersecurity incident?

A. (Williams) I don't -- I haven't said that, Ms. Rudderham, and that's not what it's been put forward as, so no, I would not encourage you to take that for -- or to take that from this table.

Q. Is there somewhere where NSPI does report on all capital projects that have had impacts to their schedules other than here?

A. (Williams) So there would be

information included in ACE, but I think important to remember, the cyberattack may not be the only variable that has influenced the timing of the applications and that applications are moved forward and moved back as a matter of course on a regular basis.

MEMBER MELANSON: Could I just interject on this particular listing? I'm just trying to remember, because I don't have it in front of me, but there's a whole series of reports, and my understanding was that these are updated so that if a product has been filed it might not have been listed because it's no longer being delayed. Is that potentially the case?

MR. WILLIAMS: They are sequential, sir. I don't -- I can't say for sure without going back and looking at each ---

MEMBER MELANSON: It would be another report ---

MR. WILLIAMS: Any regulatory schedule that has been impacted as a result of the attack has been

included in this table at one time or another at the very least.

[3:20:03] **MEMBER MELANSON:** So if we went back through the various reports they'll be able to tell us some came in and some came out and that -- once they were filed?

MR. WILLIAMS: I'm not -- I can't say for certain that there's -- I think I'm following you, that there are fewer rows in this table than there were in the first, but in any event, anything that was a regulatory schedule that was impacted by the attack, the intention was to have it included in this table.

BY MS. RUDDERHAM:

Q. That was my understanding as well. That was what I was trying to understand, what's being represented in this. This is the -- this is any and all capital projects that are currently being impacted or had previously been impacted but not remedied; is that right?

A. (Williams) I'm losing track a little bit, Ms. Rudderham, about how you're trying to characterize it. I think I've said it a number of times what this table is intended to be.

Q. okay. Then maybe could have the afternoon break.

THE CHAIR: Okay. So we'll come back at twenty to four.

--- Upon recessing at 3:21 p.m.

--- Upon resuming at 3:39 p.m.

GLEN MacLEOD, Resumed:

CHRIS LANTEIGNE, Resumed:

LIA MacDONALD, Resumed:

BLAKE WILLIAMS, Resumed:

THE CHAIR: Okay. Welcome back.

MS. RUDDERHAM: Thanks.

CROSS-EXAMINATION BY MS. RUDDERHAM, (Cont'd):

Q. I want to circle back to thing to clarify my understanding. So NSPI currently tracks

incident-related costs using project codes, similar to how they would track storm-specific costs, correct?

[3:40:00] **A.** (Williams) Yes, certainly certain costs are tracked in that manner.

Q. That project code tracking, are those codes -- do they correlate with the categories, the seven categories we discussed in the CA IR-6 response, or is it the more granular level that I was speaking with Ms. MacDonald about?

A. (MacDonald) Each of those main categories are not, in and of themselves, a code, so there would be more granular categories across some of those other examples that I noted.

Q. So when we get that IR response, will those granular level -- those will match what was tracked in the project codes? Is that -- I'm just trying to understand what is actually being tracked and how.

A. (MacDonald) So I can't confirm that now, but as part of the undertaking, back to what we

explained earlier about if we can provide more granular with that undertaking, we will, and with that, if the way we do that is by sorting on codes where they're available, we'll do it that way. I just can't confirm right now if that's precisely how it will work for all of it.

Q. And the way that works is each individual employee would just track it under that code and that's how it's tracked? Is that how that works?

A. (MacDonald) Usually when there's a project, the project itself would have a code, and then whether it'd be employee costs, or consulting costs, or other costs that would roll into that code, they would all be associated like that.

Q. Okay.

A. (MacDonald) So a code could have several different types of costs, including labour.

Q. Okay. And I understand that that means it's tracked in real time. It's not like an after the fact at the end of the month tracking? It's as it's

being incurred, it's recorded as that project code?

A. (MacDonald) Different costs are incurred or tracked at different timelines in any given month, like whether that be on a payroll timeline or when an invoice is received or accrued for an external cost. So it really depends. It's not any specific schedule within a month, but we track what we can to the timeframe where it was occurred.

Q. Is there a process on a monthly basis where NSPI is tracking the cybersecurity-related costs, or is that just at the end of the year or end of the quarter?

A. (MacDonald) So not my specific area of expertise in terms of the specific financial tracking processes, but in general, we track everything monthly and the cyber costs would be within that as well, as would any other cost.

Q. So I'm going to switch gears. I wanted to ask some questions about the Dispatch Study

Action Plan, which is one of the listed regulatory matters on those monthly updates, correct?

A. (Williams) It's on there, yes.

Q. And I'm correct that under that action plan, it includes two projects, the Economic Dispatch Optimization Solution and the System Dispatch Dashboard that NSPI has been working on? Does that fall under that category, that regulatory category?

A. (Williams) Could you just ask the question one more time?

Q. I'm just trying to orient ourselves. When we're looking at that, we're considering the two system solutions or the two programs under there for dispatch, the Economic Dispatch Optimization Solution and the System Dispatch Dashboard, correct?

A. (Williams) I'll take it subject to check, Ms. Rudderham, yes.

Q. Okay. You're familiar with those programs, though, those projects?

A. (Williams) I'm not familiar with the kind of day to day. I don't know ---

Q. But just in general. I'm not asking about the day to day. I'm just trying to orient ourselves, what we're looking at here when we're looking at, like, the go-live date that's reported on and things like that. We're looking at those projects, the Economic Dispatch Optimization Solution and the System Dispatch Dashboard, correct? I don't think your microphone is on there.

A. (Williams) I understand the line item we're referring to so we can proceed with the discussion. I don't know how much I'm going to be able to give you on this though.

Q. Okay. I'm just looking at the report here. It says the go-live for the EDOS project would have been July 14th, 2026. And then it says, "Transitioning to full operations August 11th." Are you able to tell me what that means?

A. (MacDonald) Sorry, Ms. Rudderham, can you repeat the question again?

Q. So here it's saying, "Project go-live happened July 14th" and then it also, in the last column, says, "Transitioning to full operations on August 11th." I'm just trying to understand what's actually being reported on here. I assume it's two projects, the EDOS, the Economic Dispatch Optimization Solution and the System Dispatch Dashboard, correct?

A. (MacDonald) Subject to check. We were confirming that, but yes, we understand the project you're talking about.

Q. Okay. And so when it says, "Transitioning to full operations," does that mean both projects?

A. (MacDonald) So again, we would need to confirm this, but I think the intent of the comment provided by the employees completing the template would be that the project moved from the project phase

into being used in day-to-day operations, but the target was that it would on or around that date, and that's why it was reported that way.

Q. Okay. And those projects, those programs, are meant for, like, dispatch system optimization, right, like, dispatching in real time?

A. (MacDonald) Yes. And I believe the reason they're tracked here at all is that they are one of several regulatory initiatives that had proceedings associated within this year, so they were due this year and they were being tracked as an appendix to this report.

Q. And they were delayed in relation to the cybersecurity attack, correct?

A. (MacDonald) I don't think that's necessarily the case. I think everything that's tracked here has perhaps some effect on its timeline because of all the other priorities in the business over the last year. And then for completeness, to confirm back onto the record, these projects would have records themselves, but

to sort of track that the progress of the project was happening on or around the timeline that had been committed to in the proceedings themselves, for completeness and transparency, they're also noted here.

Q. Okay. Are you aware if the transition to full operations did in fact occur on August 11th?

A. (MacDonald) We would need to confirm that.

Q. Okay. Are you able to confirm whether this project was delayed as a result of the cybersecurity accident -- or sorry, attack?

A. (MacDonald) We can do that, perhaps, but I think to Mr. Williams' testimony earlier, there are many factors in any given year about why projects or regulatory proceedings may move up or back in their timeframe, or their deadlines, or their deliverables. And obviously this cyberattack and the company's focus for the last year, with everything to do

with it, would have affected, to one degree or another, many things. And so the straight line to draw here about whether or not those projects in particular had an issue because of the attack, other than timeline variations that can happen in any given year for any given reason, I just want to clarify that I'm not necessarily agreeing with the premise of the question, but we can check your question.

Q. Okay. Is NSPI tracking incremental costs associated with the delay if it was caused by the cybersecurity incident, or not?

A. (MacDonald) So I'll pass it back to Mr. Williams, because this is back into the same discussion we were having earlier on a different example. So when these projects would have been filed and approved, and recently reviewed, I believe they were approved within the last number of months. If those questions were relevant, they would have come up in those applications, and I believe we've already addressed them on the record if they were relevant.

But Mr. Williams, maybe I'll ask you if you have any other comment on that.

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

I thought that this question had been asked several times already and answered several times already.

THE CHAIR: I just want to hear what Mr. Williams has to say just to the last point, and take it from there, Mr. Clarke.

MR. CLARKE: Thank you, Mr. Chair.

MR. WILLIAMS: What I was going to add, sir, is -- and I don't know how helpful this will be to you but was to just agree with Ms. -- what Ms. MacDonald had to say.

But I -- like, we have been attempting all afternoon to be, you know, as responsive as possible to these types of questions, and I -- and at some point, I think there needs to be recognition, Ms. Rudderham, that

you're asking questions about things that are not on the issues list in this proceeding. So costs, the finances, none of that's on the issues list in this proceeding.

[3:50:19] So we've attempted to be as responsive as possible, but I think we're probably at the end of what we can say, and that's why I think you continue to cycle back on the same questions.

VICE CHAIR DEVEAU: Just in relation to this list, I'm not sure what the -- what your view is now, but this list arose specifically as a result of an enquiry from the Board in terms of the monthly updates, and was to provide a schedule. And if I remember the letter, I'm just going from memory here, but the letter outlined 15 regulatory matters that Nova Scotia Power had indicated were delayed because of the cyber incident. So that was the genesis of this list.

So I'm not sure what you're reporting on now, but originally this list, the schedule in these updates came about as a result of Nova Scotia Power saying

these matters are being delayed because of the cyber incident. So the Board wanted an update about the delay and where the projection was.

So I'm not sure what your intention is now in terms of there are other factors, you know, resulting in the delay, but the list started because Nova Scotia Power had said -- and I can find the letter if you wish, but again, it was a -- we went through several bullets, several pages of bullets saying this project was delayed because Nova Scotia Power said it was because of the breach, and it was like two or three pages of those bullets. And that's how this list originally started.

MR. WILLIAMS: Yeah, I'd agree, sir. That's ---

VICE CHAIR DEVEAU: Yeah.

MR. WILLIAMS: --- certainly my memory of it, is at the point in time when the attack occurred, and as we were recovering from it, there was a cascading impact on the regulatory process. And so it was to try to

provide the Board with a comprehensive understanding of what the impacts would be to the regulatory schedule of those incidents.

VICE CHAIR DEVEAU: Not -- that's not to your point, Ms. Rudderham, but that was the genesis of the list. It was -- it came directly from the Board's request for this schedule.

MS. RUDDERHAM: That's what my understanding was, and I was confirming, but now I'm unclear that it is anymore. So I'll...

BY MS. RUDDERHAM:

Q. Just to clarify, these programs that are falling under this project, the purpose of them was to improve cost effectiveness or efficiency for system dispatch. Is that right?

A. (Williams) I think we'll just take it subject to check, Ms. Rudderham.

Q. Now, has NSPI looked at whether the delay in implementing this project has resulted in

increased operational costs or implications for NSPI's customers?

A. (Williams) So I think we're just circling back now again on my previous point, which is I think we've attempted to be as responsive as possible to these types of questions, but at the end of the day there are processes -- there will be processes in place to assess whether there are any residual costs that may arise as a result of any delays, whether they're a project or whether a study like this, and the Board has the appropriate mechanisms in place to address that should it arise.

Q. And -- so for this project, that'll all be reported on once it's finally completed? Is that what I'm understanding you saying?

MR. CLARKE: Hold it. This question has been asked several times, and it's been answered several times, Mr. Chair. It's unnecessary to answer this question again.

THE CHAIR: So there's quarterly reports in the other proceeding about the timeline and what's impacted the timeline is, as you're aware, and I guess I am unclear now where we're going.

MS. RUDDERHAM: It doesn't report on costs specifically or costs increase in relation to the delay. So if it's that this particular project is going to have a report at the end once it's done of all the cost implications, then that's fine. I just wasn't sure what was actually being tracked and what's going to be reported on.

THE CHAIR: And I don't know whether that's the end result in that other project. The most recent quarterly update has come in, and I understand there was a further delay, but it looks like it's getting closer, but no indication beyond that.

MS. RUDDERHAM: And, Mr. Chair, I think my frustration is a few months ago, I was sitting here at the ACE Plan, and I asked a bunch of questions in

relation to the cybersecurity, and I was referred, "No, there's specific matters in relation to cybersecurity costs." So I'm here now asking questions about the cybersecurity costs and being referred, "No, these are having to go with the project costs."

So I'm just trying to understand when exactly do I get to ask questions about the cost increase in relation to the cybersecurity incident?

THE CHAIR: Okay. So the question -- sorry, go ahead.

MR. CLARKE: I wasn't here for the ACE, so I want to say that upfront, but I do think the questions have been answered, and I think they've been answered responsibly and transparently and appropriately. I just see that we're repeating the same questions again and again.

THE CHAIR: Answers have been provided. My concern, I guess, would be similar to Ms. Rudderham's, that the issue of the cost implications

of the delay on the project, I think the response was, "There's a separate process there that's dealing with that."

It's not clear to me that that actually is going to occur in that process, and if the panel believes that it is, I think that's what Ms. Rudderham is trying to confirm if that's the intent, that that other process will include an assessment of those costs. And if it's not, I think I am inclined to let her explore that in this proceeding.

MR. CLARKE: My understanding, and better to put it to our panel, but I understood that the answer was that it was going to be checked and a response was going to be given.

THE CHAIR: Maybe. My understanding of the response was there was a separate process that was dealing with those issues. I didn't hear clearly that the costs were going to be explored in those -- in that proceeding.

MR. CLARKE: Well, if there's any ambiguity, I'll defer -- I'll allow the question to be asked.

MR. WILLIAMS: I guess, sir, I -- since we're talking about the specific project, so in this project, the Dispatch Study, my understanding of it is that there is -- it's a follow-up from a previous FAM to the capital application associated with it, that's been approved. So that is what it is.

To the extent that the delay in implementation has resulted in increased fuel costs, for instance, then that would be handled in the FAM.

So when we say there are processes in place that the Board has established and available to it in relation to this, that is precisely what I mean in this instance. And when we talk about other capital costs, obviously those costs are going to be before this Board for approval.

So I do feel like I have been

responsive, and Ms. MacDonald as well, to the questions. And again, these types of questions and the subject matter is not on the issues list in this proceeding, so I think we have been more than fair in responding to these questions.

THE CHAIR: Just to get to the nub of your response, though, in terms of the direct response to Ms. Rudderham's question about where costs might be assessed in that, it would be the FAM audit for the 2025 period?

MR. WILLIAMS: That would be my assumption, sir, yes.

MS. RUDDERHAM: Thank you.

BY MS. RUDDERHAM:

Q. In terms of the delay of the ---

MEMBER MELANSON: Just before we go on. ACE Plan, because I was in the ACE Plan, for the ACE Plan projects -- well, actually, the ACE Plan projects are already filed and let's leave that aside. But for any

future projects, capital projects, whether it be an ACE Plan or for subsequent projects, if there are issues that arise with respect to whether it was delayed by the cyber incident, you are saying that that will be addressed in those proceedings and addressed by IRs, that type of thing. Is that what you're saying?

MR. WILLIAMS: I would anticipate those issues to be dealt with in those capital applications, just as any delay questions would be on any matter if there was a delay, and whether or not that delay was prudent or not, any cost that would flow from that delay would then be a question for the Board as to determine whether they ought to be part of rate base.

MEMBER MELANSON: And for projects that don’t come to the Board before approval that are under $1 million, if there was any cost, then are you saying that those issues would be addressed in AGRA when you’re looking at the imprudence of the costs that might have been incurred?

MR. WILLIAMS: Well, I think we're going even further afield now, I suppose, but that would be my understanding, is that anything that is not pre-approved by the Board is approved as part of rate base in a general rate application.

MEMBER MELANSON: I'm just trying to find out where we're going to get these costs. Thank you.

MR. WILLIAMS: I think you cut in straight to it, sir. Thank you.

BY MS. RUDDERHAM:

Q. I'm just going to follow up on that because perhaps I'm confused again, and I apologize if I am answering -- asking questions, because I am confused by the answers.

[4:00:10] You had indicated, if there's a project that comes up and it's been delayed and then the Board at each one of those applications can determine whether it was imprudent or not, that's what you're saying, is that in each individual application the Board

is going to look at whether that delay or that cost increase because of that delay is imprudent; is that what you're saying? It's assessed individually?

A. (Williams) Yes, I think effectively. I mean, there's nothing that I'm aware of that would result in the Board changing its normal process in terms of how it approves capital filings. This is another element that would be considered to the extent there has been a delay, to the extent that the delay is the result of a cyberattack and to the extent that the delay has resulted in costs that may or may not be imprudent; that's something for the Board to determine as part of that filing just as it would be any delay for any other reason.

Q. So you'd agree with me, though, that the Board can't make an assumption, for example, that the cybersecurity incident was caused by any imprudence when each one of those individual projects come up; correct? They can't assume that you were imprudent by

having the cybersecurity incident; correct?

A. (Williams) Well, absent a determination that the occurrence of the cybersecurity incident was the result of an imprudent act itself, then I would agree with you, yes.

Q. So what I'm trying to understand is where is it being tracked then, all of these projects that are impacted, if in fact there was a later determination, and I'm not saying one way or the other, that there was imprudence in relation to having the cybersecurity incident happen or the aftereffects of it; like where is that being tracked or is it being tracked?

A. (Williams) When you say, "Tracked" what do you -- we're talking about costs that may arise as a result of delay which would be put forward as -- could be put forward as part of an application process if there had been a delay and if there were additional costs or maybe there were reduced costs; those would also be part of it, but I'm not quite sure I'm

following.

Q. So the Board is going to be reviewing the cybersecurity incident, the technical aspects of it in a different proceeding; correct?

A. (Williams) Correct.

Q. And I'm not 100 percent clear whether the Board is considering whether there was prudence -- imprudence or anything like that in that proceeding or in this proceeding, but if there was a finding of imprudence, will the -- when does the Board get to look at the costs caused by those imprudences? I'm trying to understand ---

A. (Williams) In fairness, I think that's a question for the Board.

MR. CLARKE: This has been asked several times and it's been explained in terms of how this would be presented to the Board and what authority the Board would have.

THE CHAIR: So I agree with Mr.

Clarke. I think the responses that we've gotten are it would be subject to the Capital Applications that those particular ---

MS. RUDDERHAM: Okay.

THE CHAIR: --- projects are related. It hasn't come up, but my assumption would be that if it's a project that's currently been approved and is ongoing, if there is an increased cost as a result of that, likely to see in an ATO Application, in which case then it would be reviewed there.

MS. RUDDERHAM: Okay. So it's -- okay, it's based on the ATO threshold then?

THE CHAIR: That point isn't is specifically before us at this point in time, but that would be the trigger, I guess.

MS. RUDDERHAM: Okay. And I feel like I'm just slightly confused. I'm having a hard time following some of the answers and that succinctly described it to me.

BY MS. RUDDERHAM:

Q. In terms of the dispatch, which is for the dispatch project, the delay of that project as a result of the cybersecurity incident, has it affected the transition to the IESO NS at all in taking over the system operations?

A. (MacDonald) No.

Q. Okay. I'm going to switch topics, and we spoke about this a little bit this morning and in your opening statement where NSPI has not applied late charges or penalties to outstanding customer balances since the incident; correct?

A. (Lanteigne) That's correct.

Q. And as a result of that, NSPI has collected less late fee revenue than it had budgeted; correct?

A. (Lanteigne) That's correct.

Q. There's -- the amount of that variance is included in a confidential -- confidentially

in response to an IR. I don't think we need to bring it up, but I'm assuming that's the same thing that's occurring in 2026 as it did in 2025?

A. (Lanteigne) That is correct for 2026 to this point, and we have communicated to our customers. We promised to provide at least two months notice and on July 15th we informed customers that interests on overdue amounts of return on October the 1st.

Q. Okay. And as I understood from the response to the IR, that decrease in the budget revenues was borne by a reduced shareholder return; is that fair? I can pull up the IR ---

A. If we can pull it up, that would be great, yeah.

MS. RUDDERHAM: Yeah, Exhibit N-11, SBA IR-17(b). I don't actually have the pdf number, but I can pull it up for you here in a moment.

MR. NORWOOD: IR-17?

MS. RUDDERHAM: Yeah.

BY MS. RUDDERHAM:

It says:

> Lower revenue for NS Power resulted in lower earnings which caused a reduction in NS Power's regulated return on equity, therefore NS Power bears the financial impact.

Do you see that there?

A. (Lanteigne) I can see it there for sure. Sorry, could you repeat the question about it?

Q. I was just confirming that that's what -- that it was borne by NS Power and I assume that's the same for 2026 as well, or is this related to 2025?

A. (Lanteigne) Yes, it would be the same in 2026.

Q. Okay. Now, I understand that with the estimated bills and the customer disputes and things like that, I'm correct that NSPI has also experienced a higher number of unpaid bills than it would ordinarily expect in 2025 and 2026, correct?

A. (Lanteigne) That is correct. We

do monitor the amount of customers who are in arrears and while, you know, the vast majority of customers are still current on their bills, we have seen an increase in that rate.

Q. Okay. And in the absence of the late fee penalties or charges, and then also the deferred or the delayed payment of the bills, has that had any impact on NS Power's operations or systems or customer services, that decrease in revenue?

A. (Williams) So the short answer would be no, Ms. Rudderham, and I think it's notable that carrying that type of cost does have a corresponding or corelating costs to Nova Scotia Power, so it does increase costs for Nova Scotia Power.

Q. So that increased cost, you're referring to like the carrying cost or the interest on those unpaid bills? Is that what you're referring to?

A. (Williams) Correct.

Q. But not the late fees, because

the late fees are absorbed by NS Power; is that what you're saying, the fewer -- sorry, the late fees resulted at a certain number of less revenue.

A. (Williams) The late fees are not a carrying -- not being carried by the Company.

Q. So are you able to say -- sorry -- what was the carrying cost impact then? Does that -- it just impacts the cost to the Company?

[4:10:00] **A.** (Williams) Apologies, Ms. Rudderham, we don't have that number.

Q. In the assurance that's been given about the restoration costs, that increased carrying costs were not -- for those increased ARs, is NS Power intending on collecting those increased carrying costs from its customers?

A. (Williams) No.

Q. So it's tracking it separately?

A. (Williams) Yeah, again, you're getting into areas -- this is the third time I'm going to

say it. Like, these are questions that are not on the issues list and I'm trying to be as responsive as possible, but I think we've come to the end of this discussion as well.

Q. We can bring up the issues list if you'd like.

A. (Williams) Happy to.

MS. RUDDERHAM: Would you mind bringing up the issues list? I can read out the section I was going to look at. There it is. Can you scroll down to the second page there, Item 11. I'll just read it in.

BY MS. RUDDERHAM:

Q. It says:

> Business and regulatory impacts, including continuing impacts to day-to-day operations, bill payments to third parties, regulatory proceedings...

You agree with me that unpaid AR would have an impact on day-to-day operations and bill payments to third parties?

A. (Williams) No.

Q. You don't think it has any impact on your business or regulatory endeavours, I guess?

A. (Williams) I can confirm for you that it does not fall within what's itemized in Number 11.

Q. Okay. Well, we'll leave that for the Board. I was asking about your assurance about saying they're not going to be -- you're not going to be recovering any cost associated with the restoration costs, and you had said NS Power was not going to be carrying -- or recovering the carrying cost associated with the unpaid AR. And so I had asked are you tracking that? And your response was, "This does not fall under the issues list."

A. (Williams) No, I believe my response was I am not sure. We can't confirm that up here because we've kind of reached the end of what we're able to provide you here. So ---

MS. RUDDERHAM: I see counsel here motioning to ---

MR. CLARKE: I don't think you've got

your microphone on.

MR. WILLIAMS: I do. I'm just -- so again, Ms. Rudderham, we've been at it all afternoon, trying to respond as best we can to your questions, and I'm happy to continue, but I have sensed your frustration at times and I'm trying to avoid that, because it's not that we're not trying to be helpful, it's just that we're somewhat limited in what we can offer you, given the scope of the proceeding.

BY MS. RUDDERHAM:

Q. And I understand that. I'm -- there's an assurance that's in this proceeding that specifically says Nova Scotia Power will not be seeking recovery of any restoration costs from its customers, correct?

MR. CLARKE: Of course it's correct. He's answered that several times.

BY MS. RUDDERHAM:

Q. Okay. So I am asking, those

carrying costs, that's part of that assurance then?

A. (Williams) So that assurance is not necessarily part of this proceeding. That assurance was given well before this proceeding was established. So I'm not -- I guess I'm not clear on what the point is, that because something has been stated here, it's now therefore relevant. So ---

Q. Are you saying it's not relevant?

A. (Williams) What I'm saying is that we have attempted to be as responsive as we can be, and as I said, I'm happy -- more than happy to continue the conversation, but I'm trying to just caution you that this panel is limited by the scope of the proceeding as it was established. And so again, happy to continue the conversation, but I have sensed your frustration at times and I am trying to just manage expectations.

MR. CLARKE: And, Mr. Chair, the witness has indicated, from the panel's point of view, that further questioning on this issue is outside the

issues list. So that is our position with respect to any further question.

(SHORT PAUSE)

THE CHAIR: So the Panel has discussed and we believe that the issues relating to changes in accounts receivable would be a business impact. It is caught within the scope of the issues list and Item 11 and we're going to allow Ms. Rudderham to pursue that line.

MR. CLARKE: Thank you, Mr. Chair.

BY MS. RUDDERHAM:

Q. So as I understand, Mr. Williams, you're not able to, today, confirm how those increased carrying costs are being tracked or what that amount is, so perhaps I could get an undertaking to confirm what it was for 2025 actuals and 2026 to date, and then forecasted forward for however long it would take to get back to normal in terms of accounts receivables?

(SHORT PAUSE)

[4:20:29] **A.** (Williams) So my apologies. We

can certainly -- the hesitation in the discussion with the panel is just it will not be any of us doing that work, and so I don't want to make commitments that can't be fulfilled.

So I would -- I think we're prepared to accept the undertaking, but with the caveat that we will confirm that everything's that's been requested is available and can be done. I would anticipate it is, but I just want to make sure that that's clear.

Q. I think that's fair. And if -- my question was originally is this being tracked separately where it's not being recovered from customers? If the answer is it is in fact not being tracked separately, if that's all that you can provide, that's all that you can provide. It just -- and if it is being tracked separately, what that amount would be.

Is that sufficient? Is that ---

A. (Williams) We can take that.

THE CHAIR: Okay. So just so it's

clear on the record, though, maybe, Mr. Williams, you can restate what you're -- what you think you're agreeing to promise, or what you've promised.

MR. WILLIAMS: I like how you put that back on me, sir. So I think what we have agreed to is to confirm whether or not it is in fact tracked separately, and if it is tracked separately, what that amount is.

THE CHAIR: And that's the -- the "it" is the carrying costs on accounts receivable.

MR. WILLIAMS: Yes.

THE CHAIR: Okay.

That will be Undertaking U-9.

UNDERTAKING U-9 - To confirm if carrying costs on accounts received are tracked separately, and if they are, what that amount is for 2025-2026 until it is forecasted to get back to normal

MS. RUDDERHAM: I'm just going to

quickly look over my notes here, and otherwise I'm probably finished. Just one moment.

BY MS. RUDDERHAM:

Q. I'm just reminded; for the undertaking, U-9, just to confirm that it was for 2025-2026 and forecasted until it's -- and forecasted to get back to normal. Is that -- that's still okay under that undertaking?

A. (Williams) That's fine, sir. Thanks.

Q. Those are all my questions. Thank you, panel, for being so patient.

THE CHAIR: Department of Energy?

MR. KAYTER: No questions from the Department. Thank you.

THE CHAIR: Any -- did I miss anyone before going to Board counsel?

--- (No response)

THE CHAIR: Okay, Mr. Mahody, we do

have a hard cut off at 5 o'clock tonight, so as close as you can get to there. If we go a minute or two over, that's fine. You don't have to finish by then.

MR. MAHODY: With the amount of cross-outs that I have on my notes, Mr. Chair, that should not be a problem.

THE CHAIR: Okay, good. Let's see how it goes.

CROSS-EXAMINATION BY MR. MAHODY

Q. I do appreciate that we're in the non-technical proceeding, but there was a lot of talk this morning about the Data Lake and the cut of data from 2021 that was the subject matter of the exfiltration, the 13 terabytes. Is the panel aware of what I'm talking about?

A. (Williams) Yes.

Q. Okay. Mr. Williams, in addition to the exfiltration of that 13 terabytes, was it the case that there were other system-related impacts that related to the company's inability to access the Data Lake for a period of time?

A. (Williams) So I appreciate the lead-in, sir, being that this is the non-technical. So with that in mind, the only limitations would have been the need to, as part of the response to the attack, to isolate the Data Lake. And then before being able to do anything within the Data Lake to assess and identify what

information had potentially been impacted, was to assure ourselves that the threat -- there was no longer a threat within the Data Lake, that we had -- the attack had concluded, so to speak, and again, I'm speaking in non-technical terms here.

But that would have been initially, and then we would have been able to move on after that initial period. The Data Lake itself was not encrypted as part of the ransomware.

Q. But the -- it wasn't simply the exfiltration of the data; there were the other system impacts that you then had to -- NSP needed to address as part of the reconstruction process.

A. (Williams) Yes, sir. I think you're referring to just everything else that was going on at a simultaneous time?

Q. Yes. So for instance, the exfiltration of date is one thing and has a whole host of very significant customer-related concerns, but in

addition to those concerns, the Company's challenges in accessing systems and the other number of issues that they addressed were related to other actions by the threat actor?

A. (Williams) Yes, absolutely, and that's an excellent point, sir. I mean, I think there needs to be an appreciation, and it goes -- kind of goes back to where we started today, perhaps, about the context of this. And this was an attack that -- it had a crippling effect on the business. So in terms of the front-office systems, the IT systems, there was very little that wasn't impacted, and so just functioning within a corporate environment was a challenge.

Q. I do have just a couple of confirmation questions regarding the collection of the personal information from customers. I don't anticipate that they're controversial, but can you confirm for me that Nova Scotia Power agrees that the personal information that is provided by customers and the data

that's generated as a result of the customers' energy usage is information that Nova Scotia Power has a custodial responsibility as part of the utility/customer relationship?

A. (Williams) So as a lawyer speaking to a lawyer, I haven't researched necessarily what custodial means in the legal context.

Q. How about stewardship? It's in your opening statement. Will you take -- do you have a stewardship responsibility?

A. (Williams) Yes, so accountability. We have accountability. I'm not trying to dodge the question; I'm just trying make sure that we're all on the same page. And I would 100 percent agree that we are accountable for that information.

Q. Okay. And would you also agree that Nova Scotia Power has an obligation to only retain personal information to the extent necessary to provide electricity to customers?

A. (Williams) Yes. Sir, the only hesitation is just on the "needed for electricity". There are many different aspects of the service we provide that is not just the delivery of electricity. So there's -- but it is limited to the services we provide our customers, yes.

Q. And that you're only to retain that personal information to the extent necessary for the service you provide to your customers?

A. (Williams) Yes, I would agree with that, with the addition that what is necessary is contextual, and so that’s where you get into a discussion like CIS, where information may be retained for a period, but it’s a period that is somewhat dictated by the technical limitations of the system itself.

Q. That CIS, Mr. Williams, as I’ve heard you describe it today, the 30-year CIS system, seemed to have technical limitations that included an inability to operate in a manner consistent with the

retention policy of the company. Would you agree with that?

[4:30:08] **A.** (Williams) No, I don't think I would necessarily agree with that. The retention policies of the company, just as with kind of the governing legislation, they acknowledge the contextual nature of this and what is reasonable in the circumstances. So it's not -- they're not absolute in terms of those requirements. I think there's a recognition that context dictates what may be reasonable or necessary in the circumstances.

Q. Well, let me just take that issues with the CIS to the removal of Social Insurance Number information. So beginning in 2018, or in 2018, Nova Scotia Power took the decision to no longer collect SINs and to remove the SINs that it was storing? Is that an accurate summary of the decision relating to Social Insurance Numbers in 2018?

A. (Williams) Yes, I think so. To

-- and again, I would say that to begin the process of removing those SINs, just to be clear, they were not all removed in 2018 or 2019.

Q. Okay. And the method that Nova Scotia Power chose to use in 2018 regarding the removal of SINs was to direct your customer service representatives to delete the SINs when the customer service representatives encountered them; is that correct?

A. (Williams) So initially, that was the measure that was taken. And again, I just want to be clear, when we say delete, it wasn't a deletion as you would think about it in a Microsoft document or something. It was zeroing those out. So the same number of digits, the nine digits remained. It's just you're zeroing out every one of the nine so that you're anonymizing the SIN, effectively. But that would have been the beginning of the process. It wasn't that that decision was made and then there was no further thought to this. It was a continuing discussion about how to best address this

within what is understood and known to be a very fragile environment.

Q. Was the direction to the customer service representatives in 2018 documented?

A. (Williams) Sorry, sir, I was just confirming my understanding, which is that I'm not aware that the documentation still exists. I would have expected there would be documentation of it but given the fact that we're talking about 2018 and we've now gone through this cyberattack where we lost a substantive amount of information, I have not seen and am not aware of a document that is currently presentable.

Q. Okay. Mr. Williams, if you would like the opportunity, I would accept an undertaking for you to go and check to see whether or not documentation of that 2018 direction exists, but if you're in a state where you know that that would not be a productive undertaking, I'll move on.

A. (Williams) So I'm -- it is an

inquiry we have made previously as part of this, and -- but I -- there's no harm, sir, in taking the undertaking, just to make sure it's clear on the record that we have undertaken that search.

MR. MAHODY: So Mr. Chair, that would be an undertaking to search, and produce if found, directions in 2018 to customer service representatives regarding the deletion of Social Insurance Numbers.

THE CHAIR: Thank you. It's Undertaking U-10.

UNDERTAKING U-10 - To search for, and produce if found, directions in 2018 to customer service representatives regarding the deletion of Social Insurance Numbers

BY MR. MAHODY:

Q. And Mr. Williams, I think you just mentioned this, but as I understand it, that 2018

process was -- the CSRs would then, when they encountered a SIN number, nine-digit number, they would then zero out that number? That was the mechanism by which the Social Insurance Number was eliminated from your system? Have I got that right?

A. (Williams) Yes, sir.

Q. Now, between that process when it started in 2018, and up until 2024, just before you commenced a new way of addressing SINs, so during that period, does Nova Scotia Power know how many SINs were removed from its system?

A. (Williams) No, sir. There would not be any way to determine a precises number.

Q. Just a comment on precision. Is there an estimate that the company would have any available to it, Mr. Williams, before I move on to 2024?

A. (Williams) That's fair. I didn't mean to qualify the response. We don't have a way to provide a number.

Q. Okay. Now, if I could take you forward to 2024? And I think it was -- the evidence had established it was perhaps May of 2024 that the decision was made that a new process to address Nova Scotia Power's possession of Social Insurance Numbers was undertaken. And was that process that began to be instituted beginning in May of 2024, was that process documented?

A. (Williams) It is my understanding that there would be documentation of that, sir, and we can ---

MR. MAHODY: Okay. If I could get an undertaking for the 2024 SIN elimination program?

THE CHAIR: Undertaking U-11.

UNDERTAKING NO. U-11 - To provide the 2024 SIN elimination program; to advise how many SIN numbers were purged from NS Power's system

BY MR. MAHODY:

Q. And I think I heard you correctly today, Mr. Williams, that that 2024 program to delete Social Insurance Numbers was implemented and completed in 2024, during that year?

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

Q. And during that period in 2024, beginning in May, does the company -- is the company able to indicate how many Social Insurance Numbers were purged from its system?

A. (Williams) We would have to check on that. Certainly we could add that to the previous undertaking, if helpful.

MR. MAHODY: That would be fine to add it to the undertaking, if we could, Mr. Chair.

THE CHAIR: Add it to Undertaking U-3, I believe it was. Oh, sorry; the previous one you just gave?

MR. MAHODY: Yes.

THE CHAIR: Sorry; there was a similar

one at U-3. So we'll add it to U-11 then.

MR. MAHODY: I'll add it to yours, Mr. Chair. I'm fine either way. Okay. Thank you.

BY MR. MAHODY:

Q. The process engaged by Nova Scotia Power between May and December of 2024 to purge Social Insurance Numbers, what, if anything, in that process would have prevented Nova Scotia Power from using that same purging process in 2018, 2019, 2020, or 2021?

A. (Williams) I'm not aware, sir, that there is any difference in the technology that would have been used to do it. My understanding of it, based on the discussions we've had internally, is that it really was a progression of a level of comfort with undertaking the work. Again, it all goes back to the sensitivity of the system and balancing what is the risk versus what work do we want to do in there and accomplish. And so the decision was made, on a progressive basis, to undertake this work to address the SINs within CIS, and the comfort

level was obtained to proceed with that work, and it was done, as you've indicated in 2024.

But I'm not aware of, as I said, any difference in technology. So to your question had the same level of comfort existed in 2020, 2019, any other year, my understanding is that it could have occurred, it was just, as I said, the progression of understanding what those risks and making sure everyone was comfortable with balancing them.

Q. But having determined in 2018 that Social Insurance Numbers were not needed to serve utility customers, except in very limited circumstances, on what basis does Nova Scotia Power say that it acted prudently when having -- by retaining hundreds of thousands of SINs on its system for years after 2018?

[4:40:17] **A.** (Williams) No, and it's a good question. I think the prudency comes into where the reasonable actions come into it, where the decision was made, and it was recognized that there were SINs on the

system that needed to be removed, and there was discussions on an ongoing basis to remove them, and that that progressed and that was done, and even on in the interim, until there was a final level of comfort and a final decision made on removal of those on a more wholesale basis, they were being removed as they were encountered by customer service representatives. So I think, again, it's a contextual discussion, and so were it a more modern system where this could have just been automated or the removal could have occurred without the risk of kind of a cascading negative effect within the system, then it's a decision that likely would have been made earlier and an action that would have been taken earlier, but as I said, it's a -- it remains a fragile system, and so there were a number of discussions, is my understanding, that were occurring through that period of time that eventually resulted in a comfort level where the work was undertaken in 2024. So I think the prudency comes in which is what I said, all reasonable actions were

taken in the interim to limit the risk, while at the same time recognizing potential impacts to the system itself were action taken too hastily.

Q. But the fragile system was able to withstand the purge in 2024, and Nova Scotia Power has not identified any other structural barriers to having implemented that same fix in any 2018 through 2021?

A. (Williams) Sorry; I think it's similar to the response I gave you, but I just wanted to reconfirm. So no, sir, I'm not aware -- we're not aware of any structural barriers that would have been different in a preceding -- I shouldn't say -- in the interim period between 2018 and 2024. Again, it was -- work was being undertaken to remove them, and then the discussion progressed to a point where the risks were balanced; the risks of retaining them versus the risk to the system if they were to be removed.

Q. The Social Insurance Number decision, as this background that we've just been over,

that goes back to 2018 and the change of course that the company began to embark on, or the decision was made at that point, what about the other personal information? And I appreciate that the Equifax tool now has eliminated the need to retain it, but all of the driver's licence information, bank information that the company continued to possess, why was there no decision taken to go and attempt to remove that data, the way there was about the other -- the personal information associated with the Social Insurance Numbers?

A. (Williams) So again, sir, it's a good question. It's one that I certainly asked as we moved through this. And so, I'm going to refer back to Ms. MacDonald's description of the system and how complex it really is.

When you're talking about SINs, you're talking about very specific information or data points that are all nine digits. It's easy to search them; it's easy to zero them out. The search functions within CIS

are limited, again, because of their -- because of the vintage of it. So as a starting point, it would be difficult to search on an automated basis to find all that data and remove it like you can with the SINs, because of that nine-digit characteristic. The more important point, I think, is when we talk about CIS and we talk about the data within it, when you start poking data holes within it, that's where you start to create the greater risk for the system and unintended consequences within the system. So when you start to look at removing a larger number or a larger amount of data, which would be what you would eventually get to when you're talking about additional personal information within the system, the risk increases exponentially.

And so that's why, you know, to refer back to the initial discussion about getting comfortable with removing the SINs, and we were able to get there, again, my understanding, because of the ability to search for those nine digits and simply zero them out on a

consistent basis throughout the system, every number has nine digits, you just put nine zeros in its place. So it was something that could easily be automated and retain the same data points within it. The exercise that would be required to remove more personal data, from a search perspective, would not be functional. And even if you could do it, you would be risking making significant changes within the system that then would expose you to the significant risk we talked about.

Q. And that's what I was trying to get at about the antiquated nature of the CIS system and its misalignment with your information retention policies. It strikes me that you had the CIS tool that did not allow you to perform the -- for instance, the destruction of personal data that was no longer needed to provide service to customers, the CIS tool did not provide you with the ability to do that?

A. (Williams) So I would agree. The CIS tool does not allow us to do a number of different

things because of the nature of it, but I think that's been part of the discussion in the regulatory forum for a number of years, identifying that that is an antiquated system that needs to be replaced. That comes, obviously, at not an insignificant cost. And so this gets into the discussion perhaps that we were having with Ms. Rudderham as well, about when you make those types of investments and what is in the best interest of customers, and there's a number of different factors or variables that need to be balanced when you're making those types of decisions.

To go back to your point about whether or not it was in compliance with our internal policies, again, I don't believe it was inconsistent with the policies, because those policies would acknowledge that it is contextual and what is reasonable, what is necessary in the circumstances, needs to take into account what is possible in the circumstances.

Q. Just on the notification to customers. So in -- first off, from a timing perspective,

the direct notification in May, was it not the case that the mailout of the 277,000 letters began on May 13th, but that there was a process to get those all in the mail and out the door? They didn't all go in the mail on one day; did they?

A. (Lanteigne) You are correct that we couldn't drop all 277,000 into a mailbox at one time, but that process to get them into the mail and to shoot it to customers would have all occurred within an approximate one-day period of May 13th, like within that 24 hours.

And I think what's interesting to note as well too, is that the mailing was from a central location and Canada Post would obviously take a different amount of time to distribute mail to certain parts of Nova Scotia to actually have the letters delivered.

Q. I didn't think you went to Almon Street, so I gotcha. Okay. When you made the decision to notify those 277,000 and you provided the split as between who got the letter that directedly referenced Social

Insurance Numbers and who didn't, when you made that decision, did you know at that point that the data breach was the cut of data from 2021?

[4:50:20] **A.** (Lanteigne) Yes, we would have.

Q. And so, Mr. Lanteigne, does that mean that what you knew at that stage was that no customer after 2021 was affected? So a new customer joined in 2022; are they off your list?

A. (Lanteigne) So at that point we wouldn't have been able to -- that was very early, Mr. Mahody, in the process. So at that point we would not have been able to -- I don't think we were in a position to rule anything out definitely at that point. We were acting on information we could confirm.

Q. Mr. Chair, it's not the cyber incident that's driven me to paper; it's just that I was more comfortable with it at this point.

There's a line regarding those communications in your rebuttal that I just wanted to take

you to. It's Exhibit N-17, and I'm at page 43 of 65.

MR. NORWOOD: N-17?

MR. MAHODY: Yes, page 43 of 65 and I'm just down at the bottom, beginning at line 26.

BY MR. MAHODY:

Q. And at line 26 Nova Scotia Power says:

> ...NS Power was able to identify customers that had their SINs compromised and sent out a different version of the May 10, 2025 direct notification letter indicating so.

And it struck me that that was a developed view of Nova Scotia Power represented here in the rebuttal evidence because the letters that went out in May of 2025, at a minimum, caused a great deal of confusion among your customers. And I know you've read the letters of comment that have come in and you'll appreciate that one of the main points that was made there, "What of my data has been exposed?"

These two lines seem to make it pretty

clear that you knew at the time that SINs have been exposed. So if Mahody got a letter with a SIN it, it meant that his SIN was in the mix, so to speak. But the Company's letters and other communications at the time don't have that same level of clarity. Why is that?

A. (Williams) So, I'm just going to talk it back to you, Mr. Mahody, so I understand -- make sure I'm on the same page as you.

What I understand the question to be is, and when you say, "Other communications," do you mean other public communications on the website and those types of things?

Q. Sure. I'm talking about the language in your May letters even where you talk about "May have included" certain information and a lot of language that has been the subject of -- a lot of critique from your customers.

A. (Williams) Yeah.

Q. It doesn't display the same

clarity frankly, from my perspective, and you can take it or not, that these lines 26 and 27 do, why wasn't this level of clarity expressed at that time?

A. (Williams) So I believe it was because there were two separate letters that were sent out on May 13th, one specific that had SINs identified and one that did not. So that distinction was made and ---

Q. And so in that letter when you say, "May have included", what you meant to do was to say, well, SINs were definitely included for the people that received those letters?

A. (Williams) No. I think it would be helpful for us to pull up one of the letters perhaps. And I'm not necessarily disputing, but I just want to make sure we're having the discussion in the kind of proper context. I just want to be clear for the record.

MR. MAHODY: I have them at N-2. Sorry, Mr. Chair, N-2 and it's IR-1 at the attachment 1.

MR. WILLIAMS: That's right, page 1 of

4?

BY MR. MAHODY:

Q. Yes.

A. (Williams) So I think ---

Q. It's Attachment 1; so it's at the end of IR-1. IR-1 was 18 pages. Thank you very much.

And Mr. Williams, if you're okay, I just want to go a couple of pages further over than this, because I want to go to the Social Insurance Number letter.

A. (Williams) Yes, it's Attachment 2.

MR. MAHODY: Sorry, did I give you N-2? Yeah, there you go. And it's now just over a couple of more pages, I think. Thank you, Mr. Norwood. This is the letter.

BY MR. MAHODY:

Q. So I'm at -- in the paragraph that begins, "The types of impacted personal information"?

A. (Williams) Yes.

Q. The second sentence says, "This may have included one or more of the following." So you understand at that point the customer receives this and they're reading the letter that you've written, and it says, "May have included"; but it doesn't say, same clarity that your rebuttal evidence says about "No, we've identified who had SINs that were in the mix."

A. (Williams) Well, we were able to identify that and that's why there were two separate letters created and two separate letters sent out. The one that you're looking at here, which is Attachment 2, and on the second -- the end of the second last sentence that says, "And Social Insurance Number." On Attachment 1, that language is not included, so there was the concerted effort to identify -- and specifically identify those Social Insurance Numbers and notify them as opposed to those customers that did not have Social Insurance Numbers included and ensure that we were not unnecessarily

notifying them in relation to their Social Insurance Number. And that's, I think, in recognition that Social Insurance Number is generally understood to be more sensitive than the other information here.

In order to get to the point that I think you're getting at, which is the "may" of the wording, I think you have to go to the first sentence which says:

> The types of impacted personal information varied by individual customer independent in part on the information provided by each customer...

So that the "may" is recognizing two things, that we were trying to act at a pace that would appropriately notify everyone and we didn't have time to develop a number of different types of letters that could go to different people depending on what precise information, but we thought it was important to draw the distinction between SINs and no SINs. And so that's why you have a list of a number of different personal information data points.

But also important, and this goes back to the discussion we had earlier today, not you and I, but in this room, that relates to when we say impacted, it's difficult for us to determine exactly what was taking our access, but we know it was exposed as a result or potentially exposed as a result of the attack.

So I think the language is as prescriptive and as helpful as possible in the circumstances.

Again, to undertake what you are suggesting, which is to have each individual customer receive a personalized letter with what information you did or did not have, would have been a much bigger endeavour and would have taken a significant amount of -- more time.

Q. But despite the best efforts of your CSRs between 2018 and 2024, the vast majority of your customers, who were customers as of 2018, you had their SINs?

A. (Williams) Well, again, that's because of the cut in 2021.

Q. I understand why it is. But what I'm saying to you is that where was the -- why the equivocation in the letter talking about "may"? Why not just say to customers, "Look, your SIN has been part of this breach"? But you don't say that. You say, "may have been part of the breach." And that's driven hundreds of communications received from customers.

A. (Williams) But that's in part the reality where it may have been part of the breach. So we had it, but whether or not it was part of the breach or not is, as I've said, not something that can be determined with any type of certainty. So the "may" language is the most responsible and most accurate language possible.

[5:00:10] **MR. MAHODY:** Mr. Chair, I don't think I have much left, but I would like the ability, if I do have something to follow up on tomorrow, and I'd like to do that. But other than that, I think I'm close to being

done, but I'm also right up against the 5:00 deadline.

THE CHAIR: Yeah. And normally I would probably let you go and finish, but I think we do need to stop, and you can pick up tomorrow with anything that you have extra or may arise.

MR. MAHODY: I'll have less tomorrow than I'd have if I kept going for the next few minutes. Thank you.

THE CHAIR: All right, we'll adjourn for the evening and resume tomorrow at 9 o'clock.

To the panel, again, you remain under oath, so you can't discuss your testimony with anyone.

I will alert everyone that we also have -- it's not a hard stop; it's a hard break tomorrow at -- we probably need to stop at about 5 to 11:00 in the morning and break for about 20 or 30 minutes at that point in time. So we'll try to work our midmorning break around that particular time.

Other than that, everyone have a good

evening, and we'll see you all in the morning.

And we're just going to pack up, so all do the same, please.

--- Upon adjourning at 5:01 p.m.

CERTIFICATE OF COURT TRANSCRIBER

I, Patricia Cantle, hereby certify that I have transcribed the foregoing, and it is a true and accurate transcript of the evidence given in this matter, M12600.

Patricia Cantle
Registration No. 2017-001
ICDR, ICDT
Certificate No. IAPRT-2142

Halifax, Nova Scotia
Tuesday, August 18, 2026