SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT F-2012-001

Saskatchewan Telecommunications

Summary: The OIPC received a complaint regarding an apparent over-collection of a customer's personal information by Saskatchewan Telecommunications (SaskTel) as part of its identity verification process. Though SaskTel eventually addressed the Complainant's concerns, the investigation continued as the Commissioner had concerns with SaskTel's broader collection practices. The Commissioner found that SaskTel did not have authority to collect the Saskatchewan Health Services Number. Secondly, SaskTel did not provide a satisfactory explanation as to why it needed to collect other unique identifiers over the phone since it could not verify the accuracy of same. Thirdly, the Commissioner found that SaskTel was apparently collecting third party personal information without authority. Also found was that SaskTel did not meet the notice requirements of section 26(2) of *The Freedom of Information and Protection of Privacy Act*. The Commissioner recommended that SaskTel conduct a privacy impact assessment, revise its privacy policy and prepare a script to ensure that its customers understand what is optional when providing proof of identity. He further recommended SaskTel within 60 days purge from its systems all personal information and personal health information of its customers and third parties collected without the requisite authority.

Statutes Cited: *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01 ss. 24(1)(a), 24(1)(b), 24(1)(d), 24(1)(e), 24(1)(j), 25, 26(1), 26(2), 27, 33, 59; *The Health Information Protection Act*, S.S. 1999, c. H-0.021, ss. 2(m)(v), 2(q), 2(t)(i), 11, 16, 42(1)(c), 52(a), 52(b), 52(d), 52(e); British Columbia's *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165.

Authorities Cited: Saskatchewan OIPC Investigation Reports: LA-2010-001, H-2007-001, H-2010-001; Alberta IPC Investigation Report P2004-IR-001; British Columbia IPC Investigation Reports F06-01, F06-02; OPC PIPEDA Case Summaries #2002-56, #2005-288, 2001-24.

Other Sources Cited: Saskatchewan OIPC, *Helpful Tips: Privacy Breach Guidelines*; OPC, *Fact Sheets - Best Practices for the use of Social Insurance Numbers in the private sector, Fact Sheets – Social Insurance Number, Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues, Guidelines for Identification and Authentication*; OPC and Alberta IPC, *Report of an Investigation into the Security, Collection and Retention of Personal Information*; OPC, Alberta IPC and British Columbia IPC, *Collection of Driver's Licence Numbers under Private Sector Privacy Legislation: A Guide for Retailers*; Sasktel, *General Terms of Service*; Royal Canadian Mounted Police, *Personal Information and Scams Protection – A Canadian Practical Guide*; Access and Privacy Branch, Service Alberta, *FOIP Guidelines and Practices (2009)*; British Columbia Ministry of Labour, Citizens' Services, and Open Government, *FOIPP Act Policy and Procedures Manual*; Treasury Board of Canada Secretariat, *Guidance on Preparing Information Sharing Agreements Involving Personal Information*; K. Klein and D. Kratchanov: *Government Information: The Right to Information and the Protection of Privacy in Canada, Second Edition* (Toronto: Carswell Press, 2009).

I BACKGROUND

[1] On or about September 28, 2006, my office provided notice to the parties that we were undertaking an investigation into an apparent over-collection of personal information of a customer by Saskatchewan Telecommunications (SaskTel or ST) for identity verification purposes.

[2] On October 18 and 20, 2006, SaskTel provided two brief responses via email. Included with the October 18, 2006 email were the following three attachments:

1. SaskTel's Credit Check Tool;
2. Procedure for establishing a new customer or account; and
3. Account Passwords – Description document.

[3] On or about February 27, 2007, my office asked SaskTel to provide a more detailed response to a series of questions. A detailed response was not provided until February 1, 2011. In the interim, we wrote SaskTel summarizing our understanding of the complaint, restating what in our view remained outstanding and why, and invited SaskTel again to formally respond.

[4] My office shared a preliminary assessment of the issues under consideration on or about April 12, 2012.

[5] SaskTel responded to our preliminary assessment by way of letter dated May 22, 2012.

II ISSUES

1. Did Saskatchewan Telecommunications adequately address the Complainant's concerns?

2. Is the personal information or personal health information collected directly by Saskatchewan Telecommunications from its customers excessive for the purpose of: (a) establishing identity; and (b) conducting credit checks?

3. Is Saskatchewan Telecommunications complying with section 27 of *The Freedom of Information and Protection of Privacy Act*?

4. Is Saskatchewan Telecommunications meeting the notice requirements pursuant to section 26(2) of *The Freedom of Information and Protection of Privacy Act*?

5. Do Saskatchewan Telecommunications' indirect collection practices conform with section 26 of *The Freedom of Information and Protection of Privacy Act* ?

6. Does Saskatchewan Telecommunications have appropriate safeguards in place to adequately protect its customers' personal information or personal health information?

III DISCUSSION OF THE ISSUES

[6] SaskTel is a government institution for purposes of *The Freedom of Information and Protection of Privacy Act* (FOIP).[1] FOIP is engaged as SaskTel is collecting unique identifier such as drivers' licenses and social insurance numbers (SINs), but also contact information (address, phone numbers), date of birth, employment and even financial information of its customers and others.[2]

[7] Our authority for this investigation under FOIP is as follows:

> 33 The commissioner may:
>
> ...
>
> (b) after hearing the head, recommend that a government institution:

[1] *The Freedom of Information and Protection of Privacy Act* (hereinafter FOIP), S.S. 1990-91, c. F-22.01.
[2] These data elements constitute personal information pursuant to section 24(1)(a), (b), (d), (e), and (j) of FOIP.

> (i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and
>
> (ii) destroy collections of personal information that is collected in contravention of this Act;
>
> ...
>
> (d) from time to time, carry out investigations with respect to personal information in the possession or under the control of government institutions to ensure compliance with this Part.[3]

[8] SaskTel is also a trustee for purposes of *The Health Information Protection Act* (HIPA).[4] HIPA is engaged as SaskTel collects the health services number (HSN) of some of its customers. The HSN is "registration information" and so qualifies as "personal health information" pursuant to 2(m) of HIPA as follows:

> (m) "personal health information" means, with respect to an individual, whether living or deceased:
>
> …
>
> (v) **registration information**;
>
> …
>
> (q) "**registration information**" means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and **includes the individual's health services number** and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;[5]
>
> [emphasis added]

[9] Further authority for this investigation under HIPA is as follows:

> 42(1) A person may apply to the commissioner for a review of the matter where:
>
> ...
>
> (c) the person believes that there has been a contravention of this Act.[6]

[3] *Supra* note 1 at section 33.
[4] *The Health Information Protection Act* (hereinafter HIPA), S.S. 1999, c. H-0.021, section 2(t)(i)
[5] *Ibid.* at sections 2(m)(v) and (q).
[6] *Ibid.* at section 42(1)(c).

…

52 The commissioner may:

(a) offer comment on the implications for personal health information of proposed legislative schemes or programs of trustees;

(b) after hearing a trustee, recommend that the trustee:

(i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and

(ii) destroy collections of personal health information collected in contravention of this Act;

...

(d) from time to time, carry out investigations with respect to personal health information in the custody or control of trustees to ensure compliance with this Act;

(e) comment on the implications for protection of personal health information of any aspect of the collection, storage, use or transfer of personal health information.[7]

1. Did Saskatchewan Telecommunications adequately address the Complainant's concerns?

[10] In his letter of complaint, the Complainant noted the following:

> I received my telephone bill to-day in the mail from Sasktel and I had some questions as to the amounts that are billed to my account. . . The agent asked me my name and my birth date as well as my phone # which she could already see I was calling from. **I told her that I had some questions regarding my phone bill and she informed me I would have to provide her with either my SIN # or my health card #. I asked her what either of these #'s had to do with my phone bill and she told me that I needed to provided these to her so she could be sure I was who I said I was. I told here [sic] I don't like these #'s floating around out there and would not give them to her. She said that if I wanted to discuss my bill, I would have to provide these to her. I got quite agitated and asked to speak to her manager and she told me she would give the message to her manager and they would call me back some time later. I told her that was not acceptable and I wanted to speak to her**

[7] *Ibid.* at section 52.

> **supervisor immediately. She told me she would put me on hold and see what she could do.**
>
> A few minutes later a lady came on the line identifying herself as [name removed] and said she was a supervisor and that I would have to provide them with my SIN # or drivers license # for them to verify my self [sic]. I asked what either of these two numbers had to do with SaskTel and again was told it was for identification purposes. I told her I was calling from my home and even if I was not who I said I was, I would probably be able to give them any information on the person I claimed to be as I was obviously in that persons house, and questioned what great information or service was to be gained from Sasktel by misrepresentation.
>
> After informing her I would not be giving out information other than that which pertained to Sasktel she said I could also use a password and that would alleviate any further complications. We set up a password and discussed my bill and I found out the information I was after. **She then informed me that she had my drivers licence, SIN # and health card # on file. I wanted to have this information purged and permanently erased from my file at Sasktel as there is to** [sic] **much information floating around out there and it's not acceptable**.
>
> [emphasis added]

[11] By way of letter to SaskTel dated August 20, 2010, my office provided further details of the complaint as follows:

> The Complainant alleged that when he contacted SaskTel to inquire about certain amounts billed to his telephone account, the Customer Service Representative (CSR) requested his name, birth date, and phone number, and then further requested his Social Insurance Number (SIN) or Health Services Number (HSN) to verify his identity. The Complainant refused to provide the information, and had the call escalated to a supervisor when the CSR apparently refused to provide the information he requested.
>
> After some discussions, the supervisor, [name removed], offered to set up a password as a means of identifying the complainant for the current and future calls. The Complainant accepted this option, created his unique password, and was able to receive the information he desired. In the course of the telephone call, the supervisor advised the Complainant that SaskTel had his driver's license number, SIN and HSN on file. The Complainant requested that this information be destroyed, removed from his record. This was refused, and he contacted our office to file his complaint.
>
> We have not received a formal response from SaskTel in regards to the specific complaint, so would appreciate if SaskTel could provide a copy of its internal investigation into this matter and advise as to whether or not there is a dispute with respect to the facts as presented.

[12] SaskTel provided its response via email on February 1, 2011. The following was provided in response to the above:

> We have included a summary of the situation according to our records; please advise if clarification is required. Following a review of our records, the recorded call and the account contact log, [the Complainant] did place a call into SaskTel's call centre on September 1, 2006 where the **Customer Service Representative (CSR) first asked him for his name and his date of birth**. Throughout the entire call the CSR never requested the telephone number. This has indicated to us that he had entered his actual telephone number at the beginning of the call set up. If he had not, the CSR would have also asked for his telephone number in order to retrieve the correct account information.
>
> SaskTel employs some of the latest in Call Centre technology. If a customer enters their actual telephone number, the CSR presented with the call will receive both the call and the customer's account information, displayed at their work station, simultaneously. The CSR will then ask for the customer's name and date of birth to determine if the correct account has been displayed.
>
> If the customer enters zeros or a telephone number that is not associated with an active account, no information is displayed. In this case, the CSR will first ask for the name and the telephone number of the account. When the account information is displayed, they will request that the customer provide their date of birth (DOB).
>
> **After providing his name and DOB**, [the Complainant] **was asked to provide either his Social Insurance Number (SIN) or Health Services Number (HSN).** [the Complainant] immediately objected to SaskTel asking for this information. He was of the opinion that SaskTel should be able to conduct their business with a telephone number only. He indicated on the call that we should have the number through call display and we should know who is on the line.
>
> **The CSR did her very best to explain the reason we need the information, for security purposes and to be able to identify the person who is calling is in fact the person whose name is on the account**. The CSR also attempted to explain how Call Centre technology works and the fact that we do not actually have a call display due to the specialized telephone system SaskTel employs. After a period of time, [the Complainant] requested to speak with a Manager. Although he was upset knowing SaskTel had retained some of his personal information, at no time during this call did [the Complainant] request that any information be removed from his account.
>
> **The on-call Manager spoke with** [the Complainant] **and established a password for him. A note was added to the account indicating that future transactions required the password. However, if further verification was needed, SaskTel was to verify using DOB**.

On September 18, 2006 SaskTel Legal Department received a copy of a letter dated September 1, 2006 that was sent to the Saskatchewan Information and Privacy Commissioner. In the letter, [the Complainant] indicates to your office that he would like to have his Driver's License Number, SIN, and HSN information removed from the account as there is too much floating around out there. There was no indication in the letter that either a formal or informal request to have this information removed from his account was made to SaskTel.

…

In a current review of [the Complainant's] account, we have discovered that he was unable to remember his password and has required a password reset a number of times. In order to avoid any further frustration on his part we did revert back to verification of his identity with information that is contained on the account. **I would also like to note that the personal identifiers he wanted to have removed from his account, as noted in his letter dated September 1, 2006 have all been removed from his account.**

…

What is Sask Tel's response to customers who request to have this (PI) [personal information] ***removed from their file?***

Sasktel privacy policy permits a customer to remove PI from SaskTel systems.

If a request is made the Customer Service Representative (CSR) is to turn the request over to the Department Privacy Prime (DPP) who will co-ordinate the removal and work with the customer to establish a password if removal of the personal information impairs our ability to carry on a relationship with a customer.

Not in training material as there are only 1-2 requests a year. No planned change in policy.

…

Is password an option only to customers who have PI on file?

Passwords are available to all customers. **All new customers establish their initial service with SaskTel by providing personal information**. Personal information is collected directly from the customer first to conduct a credit check and then is retained to verify the customer on future interactions.

There is a PSI [Product and Service Information is an internal procedure document] regarding Account Passwords.

CSR's are trained according to the information contained within the Account Password PSI. **Passwords are an option for all customers.**

> SaskTel systems are being developed that will allow customers to retain full control over their own passwords. Customers will be able to set up a password that is based on a secret question.
>
> [emphasis added]

[13] The response provided by SaskTel is satisfactory to the extent that the Complainant apparently had the questionable data elements removed from his account and was able to set up a password. This however does not end my line of inquiry as I am concerned with SaskTel's broader collection practices.

2. Is the personal information or personal health information collected directly by Saskatchewan Telecommunications from its customers excessive for the purpose of: (a) establishing identity; and (b) conducting credit checks?

[14] The relevant section of FOIP is as follows:

> 25 No government institution shall collect personal information unless the information is **collected** for a purpose that **relates to** an existing or proposed **program or activity** of the government institution.[8]
>
> [emphasis added]

[15] Since there is no manual to assist government institutions in interpreting and applying FOIP, I will refer to manuals produced by other provinces with similar legislation.

[16] "Collect" is defined by British Columbia's (B.C.) Ministry of Labour, Citizens' Services and Open Government's *FOIPP Act Policy and Procedures Manual* (Manual) as the "means to bring or come together; assemble; accumulate; obtain (taxes, contributions, etc.) from a number of people; receive money [OED 9th]."[9]

[17] Alberta Services' *FOIP Guidelines and Practices (2009)* elaborates further on the definition as follows:

[8] *Supra* note 1 at section 25.
[9] British Columbia Ministry of Labour, Citizens' Services, and Open Government, *FOIPP Act Policy and Procedures Manual*, available at: http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page#3.

> *Collection* occurs when a public body gathers, acquires, receives or obtains personal information. It includes the gathering of information through forms, interviews, questionnaires, surveys, polling, and video surveillance. There is no restriction on how the information is collected. The means of collection may be writing, audio or videotaping, electronic data entry or other means.[10]

[18] B.C.'s *Freedom of Information and Protection of Privacy Act's* closest equivalent to our section 25 is section 26.[11] Its Manual offers clarity on the above underlined terms and phrases pertaining to collection as follows:

> **"program, operating**" is a series of functions designed to carry out all or part of a public body's mandate.
>
> "**activity**" is an individual action designed **to assist** in carrying out an operating program.
>
> To "**relate directly to**", the information must have a direct bearing on the program or activity.
>
> Public bodies should have administrative controls in place to ensure that they **collect the minimum amount of personal information necessary for purposes** permitted under section 26. For example, they may establish internal procedures for the review of forms which collect personal information, the evaluation of opinion polls, the review of contracts for services involving the collection of personal information, the review of policy manuals and other activities which entail the collection of personal information.
>
> **The public body must have a demonstrable need for the information such that the operating program or activity would not be viable without it**.[12]
>
> [emphasis added]

[19] In terms of collecting personal information, *Government Information: The Right to Information and Protection of Privacy in Canada*, offers the following helpful generalization:

> As part of its general objective of limiting the amount of personal information that government institutions may accumulate and make use of, privacy legislation contains specific restrictions on the authority of institutions to collect personal

[10] Access and Privacy, Service Alberta, *FOIP Guidelines and Practices (2009)* at p. 239, available at: http://www.servicealberta.ca/foip/resources/guidelines-and-practices.cfm.
[11] British Columbia, *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165.
[12] *Supra* note 9.

> information. **These restrictions limit both the purposes for which institutions may collect personal information and the manner in which such information may be collected**.
>
> In general terms, privacy legislation limits the entitlement of institutions to personal information so that **they may only collect such information to the extent that it is necessary or relevant to the various lawful activities of government**. Moreover, institutions may only collect personal information in certain permitted ways which have the effect of giving notice that the information is in fact being collected by a government institution and **indicating the general reason for it being collected**.[13]
>
> [emphasis added]

[20] Similarly, a publication from Treasury Board of Canada Secretariat considering collection in the context of the application of the federal *Privacy Act* notes the following:

> **The "collecting government institution" should be able to demonstrate that it has the necessary authority to collect the personal information in the circumstances.** Likewise, the "disclosing government institution" should be able to demonstrate that the personal information can be disclosed for a lawful purpose.
>
> …
>
> **Though the principle of "minimal collection" is not expressly referred to in the legislation, it *is a tenet of the Privacy Act that an institution should collect only the minimum amount of personal information necessary for the intended program or activity*. Institutions should have administrative controls in place to ensure that they do not collect any more personal information than is necessary for the related programs or activities. They must have parliamentary authority for the relevant program or activity, and a demonstrable need for each piece of personal information collected in order to carry out the program or activity**.[14]
>
> [emphasis added]

[21] What is clear from all of the above is that whatever personal information a public body collects, it must be able to demonstrate that every data element in question is required to meet a legitimate business purpose and that there is legislative authority to collect each.

---

[13] K. Klein and D. Kratchanov: *Government Information: The Right to Information and the Protection of Privacy in Canada, Second Edition* (Toronto: Carswell Press, 2009) at pp. 8-15.

[14] Treasury Board of Canada Secretariat, *Guidance on Preparing Information Sharing Agreements Involving Personal Information* (July 2010), available at: http://www.tbs-sct.gc.ca/atip-aiprp/isa-eer/isa-eerpr-eng.asp?format=print.

[22] What personal information of its customers and third parties does SaskTel collect and for what purposes? On or about October 18, 2006, SaskTel provided the following procedure for establishing a new customer account which speaks to the collection of specific data elements as follows:

> Prior to establishing a new customer or account check to make sure the customer doesn't have an existing account with SaskTel.
>
> …
>
> Enter the appropriate information into the name fields. This is the name of the person that will be responsible for the telephone account.
>
> - Last Name
> - First
> - Middle
> - Title
>
> **You *must never* take an application from someone that is calling in on another's behalf.**
>
> …
>
> **Establishing Service for a New Customer:**
>
> Once you have determined that you do indeed need to create a new Customer and Account:
>
> 1. The **Customer Summary** window will appear… Enter a ***minimum*** of 3 pieces of ID in the following fields:
>
> …
>
> - Birthdate – Enter as MM DD YY.
> - SIN – This field is optional. Ask your customer for the information. However, if they do not wish to give it to you – tab to the next field.
> - Identification – … will allow you room for either a driver's license or a health number. Click on the appropriate choice and fill in the information. If obtained enter the second number in the contact log.
>
> 2. From the **Account Menu**, select **New Account**. The **Account Information Screen (Credit Record)** will appear.
>
> 3. Complete the fields as shown in the following example.
> Employment start date is entered as MM YY.

Employment should be verified by calling the work number and verifying the customer does work there.

Credit Record

The credit record is one of the most important documents SaskTel has on a customer. Both the customer and SaskTel benefit from an accurate, complete disclosure of credit information:

- The customer benefits because SaskTel can extend the proper amount of credit before collection starts. Thus, potential customer annoyance is minimized.

- SaskTel benefits because it protects its assets yet does not expend money on unnecessary collection efforts.

Below we've provided explanations of what is to be entered into each field.
Customer's name, Roommate, Alternate Contact or Work Phone Number and Credit Check Authorized are *MANDATORY* fields.

- **Responsible Party** – The information in this field is carried forward from the New Customer and Customer Summary screen.
- **Employment** – Enter the customer's place of employment, work telephone number and the date that they started (MM YY).
- **Previous Employment** – If the customer has been at their current job for less than a year, request information on their previous employment.
- **Previous Residence** – Enter the address and telephone number of their previous service. If they haven't had service previously, ask for the address and telephone number where they are residing. If it was with their parents, make a note of that.
- **Roommate** – Enter the name(s) of any roommate(s) and their place of employment, ID and contact number. Use the contact log to add the roommate credit information. If there is no roommate you must enter "None."
- **Alternate Contact** – Ask for the name and telephone number of a parent, relative or long term contact who will be able to contact the new customer if SaskTel is unable to.
- **Remarks** - Enter any relative information such as past credit information and credit cards numbers. Never enter the expiry date of the cards.
- **Estimated Toll** – Enter the approximate amount of long distance they expect to use in a 30 day period.
- **Credit Check Authorized** – Select whether or not the customer has agreed to authorize SaskTel to perform an external credit check.

...

Additional Credit Information

Customers with long, stable employment and good earning capacity are usually the most creditworthy.

Applicants with certain types of income require further investigation. Additional information needs to be obtained for the following incomes:

- **Private income** – Applicants with private income may range from millionaire entrepreneurs to paupers who return empties for refund. Obtain the following information:
    - source of income,
    - previous service history, or
    - a service number of a member of the immediate family

- **Seasonal Worker** – Income may not be steady, while long distance usage may be high. Obtain the following information:
    - where they are employed;
    - type of work;
    - how long have they been employed;
    - service number of their employer;
    - type of employment in the off season and the service number there, and;
    - the service number of relative or friend in the city.

- **Student** – If your customer is a student, they most likely won't have a credit history. You'll need the following information:
    - name and number of the school;
    - their 6 digit student number;
    - the financial institution providing the student loan;
    - the city and service number of their parents;
    - any information regarding part-time employment;
    - the service number of a relative or friend in the city;
    - any spousal contact information and employment (if applicable); and,
    - occasionally they will have numerous roommates. If so, obtain the above information on the roommates as well.

- **Unemployed** – Income may be insufficient to afford telephone service.
  Obtain the following information:
    - their source of income;
    - any previous employment;
    - any prospects for employment;
    - any spousal contact information and employment (if applicable); or,
    - their social worker's name and number.

- **Minors** – If your customer is under the age of 18 they are not contractually liable because they are a minor…

- **Aboriginal Decent** – If your customer is of aboriginal decent and living on a reserve, for tax purposes we will require their **10 digit treaty number**.

- **Major Credit Card** – in the Remarks section of the credit record enter the credit card number without the expiry date. Never record a credit card number and the **expiry date together on the same screen**.

The more information we have on all the occupants in the household the better. If there is no room on the credit record use the contact log.

[emphasis added]

[23] SaskTel also advised us on October 20, 2006 as follows:

Customer calls for DETAILED BILLING INFO or CHANGES TO ACCOUNT which impact protection of customer info (changes in billing address, publish phone number, etc.)

Verify two pieces of ID (choose from the following)

Date of Birth
Drivers License Number
Health Card Number
Social Insurance Number

Note: If two pieces of ID are not recorded on customer account, make every effort to record it.

TWO PIECES OF ID ARE NOT AVAILABLE:

Verify three of the following (choose from the following)

Spelling of home address, including postal code and spelling of last name/middle name/first name.
Home phone #
Work phone #
Account #
Password (i.e. mothers [sic] maiden name can be set up at time of call)
Last transaction on account
Other info on bill (i.e. Last billed amount, services they subscribe to)

[emphasis added]

[24] Not noted above, but in the earlier email dated October 18, 2006, SaskTel also explained that Passport, VISA, AMEX, Mastercard, Treaty Number, other identification (ID) is included in this list of desired IDs.

[25] We asked SaskTel to respond to the following:

In making our determination as to whether or not SaskTel's present practices are reasonable and appropriate in the circumstances, we will take into consideration the following:

> The terms *identification* and *authentication* are frequently used interchangeably but in fact mean different things.
>
> Put very simply, identification involves a claim or statement of identity: "I am John Doe," "I am the customer associated with this account," etc. Authentication is a verification of that claim.
>
> Identifying a customer allows a business to ensure that the customer's transactions are associated with the correct account, and that records of a customer's transactions are retrievable. The identity that is attached to the customer need not be a "real world" identity such as a name (e.g., John Doe). It could just as easily be an identity created for the purposes of the business relationship (e.g., customer A167).
>
> …
>
> An organization needs enough information about individual customers to identify them and authenticate their identity, but needs to ensure that it does not collect, use, or retain unnecessary personal information that intrudes on personal privacy.
>
> Authentication is often discussed in terms of the three factors of authentication (that is, three different kinds of things that can be used to authenticate an individual):
>
> - Something that is ***known*** to the individual (for example, a password, a personal identification number or PIN, an account number, favourite colour, name of first pet);
>
> ...
>
> Identification and authentication are fundamentally about the management of risk:
>
> - The risk to the organization of, through bad authentication practice, either denying access to a legitimate customer or giving access to an impostor;
> - The risk to individuals that their personal information is lost or inappropriately disclosed, and that their identity, finances, and privacy are compromised.
>
> "Risk" should always be understood to have two aspects: the likelihood of an event occurring and the severity of the consequences if it does occur. Proper risk management requires that both these two aspects of risk are considered.
>
> The stringency of authentication processes should be commensurate with the risk to the information being protected, risk being a function of the sensitivity of the information or service in question, the vulnerability of and the perceived threat to

that information or service. In general, the higher the risk or the more sensitive the information or service, the greater the number of factors that should be used to authenticate the individual. For example

- A simple single-factor authentication process may be appropriate to allow an individual to obtain access to voice mail or to check the account balance of a loyalty program;
- Obtaining an account balance for a utility bill may require an account or membership number and a numeric access code, (i.e., multilayer single-factor authentication); and
- Financial services that permit the issuing of payment instructions and making transfers to third-parties for large amounts may require a two-factor authentication process.[15]

We will also be taking into account the following four part reasonableness test when completing our assessment of SaskTel's present identity verification practices:

- Is the identity measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-intrusive way of achieving the same end?[16]

Our office has had an opportunity to review the policies, training material and other information that Sasktel provided. In reviewing, we have identified a series of questions for your response.

1. Does SaskTel rely solely upon identification provided over the telephone such as SIN, HSN, Driver's License Number, Passport, or Treaty Number as verification of the individual's identity because these pieces of information are the most secure or simply the most convenient?

[26] SaskTel's early submission did not address the above in any depth. For instance, it offered the following general justification for its collection practices and a vague response on the one particular question:

On November 8, 2001 the Office of the Privacy Commissioner of Canada issued case summary 2001-24 where they determined that a reasonable person would find it appropriate for a company to collect personal information for the purposes of

[15]Office of the Privacy Commissioner of Canada (hereinafter OPC), *Guidelines for Identification and Authentication* (October 2006), available at: http://www.priv.gc.ca/information/guide/auth_061013_e.cfm.
[16]OPC, *Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues* (September 2007), available at: http://www.priv.gc.ca/information/pub/ID_Paper_e.pdf

> determining if a potential customer was credit worthy or in the case of a repeat customer to confirm their identity.[17]
>
> …
>
> ***Does SaskTel (ST) rely solely on the PI provided over the phone because they are the most secure or convenient?***
>
> SaskTel's mode of operation is primarily conducted through a call centre. The need in this business model is not driven by whether or not the Personal Information (PI) is most secure or convenient rather the need is to conduct an accurate credit check and to verify the customer on future transactions.
>
> Procedures are documented in Account Information, Credit and Privacy PSI's.
>
> CSR's are trained according to the information contained within the Account Password PSI. Passwords are an option for all customers.
>
> PI will be hidden from the CSR as we move to more passwords in Customer Relationship Management (CRM).

[27] SaskTel did not explain why it required *each* data element rather it lumped all together generalizing the reasons for collecting.

[28] To get a better sense of why specific data elements are collected by SaskTel, I looked to the portion of its privacy policy on its website that speaks to purpose:

> **Why We Collect Personal Information**
>
> …SaskTel collects information about you during the application process to confirm your identity and credit history, when communicating or transacting business with you, and when providing service to you. We may also collect information about you from third parties that have the right to disclose such information to us.
> Telephone calls to or from our service representatives may be monitored or recorded for quality assurance purposes. We understand that some of this information is private, which is why we collect personal information only for the following purposes:
>
> - To establish and maintain a responsible commercial relationship with you and to provide you with ongoing service. For example, we will collect information about you during the application process to conduct a credit history and / or when communicating or transacting business with you to confirm your

[17]OPC, *PIPEDA Case Summary #2001-24* (November 8, 2001), available at: http://www.priv.gc.ca/cf-dc/2001/cf-dc_011108_e.asp.

identity; if you prefer to use pre-authorized payment for our services, we will collect bank account information in order to process payment.

- To understand your needs and develop and recommend suitable products and services. For example, we maintain a record of products and services you receive from us, and we may ask you for additional information so that we can serve you better. For instance, if you wish to view your bill using our electronic payment service, we will ask for your e-mail address.

- To manage your account and understand your needs and preferences allowing us to offer you better products and special offers that we think may be of interest to you.

- To manage and develop our business and operations, including personnel and employment matters. For example, we analyze the usage of our networks to plan for future growth. We also collect information from individuals who apply for jobs with SaskTel.

- To meet legal and regulatory requirements. For example, we may collect information in order to respond to a court order.[18]

[29] The focus of this investigation is only on what personal information and personal health information is collected by SaskTel for authentication and for determining credit worthiness, so I will not consider the appropriateness of the other purposes for which personal information and personal health information is collected noted above. Generally, in terms of the adequacy of its privacy policy, I find it to be fairly detailed. However, it does not speak to the necessity of data elements and says nothing regarding the customers' right to choose to provide data elements that are less sensitive or to provide a deposit instead of providing any unique identifiers.

[30] Though early in the process my office advised SaskTel of our concerns with its collection of unique identifiers, specifically customers' driver's licenses, SINs and HSNs, it has not addressed those concerns to our satisfaction. Instead, as noted in its final submission to our office dated May 22, 2012, it advised us that it had no intention of revising its practices as follows:

[18]Saskatchewan Telecommunications (hereinafter Sasktel), *Privacy* (March 16, 2012), available at: http://www.sasktel.com/about-us/legal-and-regulatory/privacy.html?Link=FooterPrivacy&campaign=Home.

The CRM project changed and reduced the information collected from a customer. The information collected today is listed below:

- First and Last Name
- Mailing and service Address
- Phone number and an alternate contact number
- Email Address
- Personal identification: Date of Birth, Passport, SIN, Student ID, Health Card, Treaty Card, Drivers [sic] License. Date of Birth is usually always requested. All other pieces of identification are optional however two pieces are requested.
- Authentication Question
- Authentication Answer
- Password

…

The information collected during the service application process is retained and used to authenticate callers later. Knowing who is calling and being assured we are dealing with the person whose name is on the account is critical to our business, to our brand and to our customers. SaskTel creates and retains extremely sensitive personal information and if released it could jeopardize a person's life. In previous information, provided to your office, we provided you with real life examples of how an unauthorized disclosure of a non-published number, for example, can put a person's life in danger. The vast majority of our business is conducted over the phone. Knowing the identity of the person calling is absolutely critical in our line of work. A mistake on our part could cost a person his or her life.

When a customer calls in or comes into the SaskTel store requesting detailed billing information for example, SaskTel will:

Verify the customer's name and phone number, and that they are the **Billing Name** on the account.

Verify first by asking for the Password or the Answer to their authentication question, if these have been established by the customer. It is not uncommon for customers to forget their passwords or answer to their authentication question. When that occurs SaskTel will then verify the caller from information stored within our systems.

If a Password or authentication question is not used by the customer then SaskTel will verify **2** pieces of information out of the below list:

- Date of Birth
- Drivers License number
- Health Card Number
- Social Insurance Number

If the above 2 pieces of ID are not available, we will verify **3** of the following:

- Account Number (CAN)
- Spelling of Home Address, including postal code and spelling of last name/middle name/first name
- Work phone number
- Last transaction on the account
- Last billed amount
- Services they subscribe to

If the customer is unable to satisfy any of the above, and are unable to call back with their identification, we will refer them to the SaskTel store to present their ID in person.

As SaskTel moves to a greater use of passwords and secret questions, where the customer is in control of the information used for authentication, there is high likelihood of the customer forgetting their password and answer to their secret question. Information is retained by SaskTel in order to verify the customer, should they forget a password or answer to the secret question. In this case to ask a customer to a store, in person to show their ID, may be a burden and hardship.

Social Insurance Numbers

[31] In terms of collecting its customers' SINs, we advised SaskTel as follows:

The use of SIN has been widely discouraged, and is not considered to be a "best practice". In one Privacy Commissioner of Canada publication, Fact Sheet, the following caution is offered:

Why is my SIN so important to personal information and privacy?

- The SIN may be a key piece of information to open the door to your personal information.

- Computer technology makes it possible to use the SIN to find and match your information from one database to another; without your knowledge, a detailed profile could be drawn about you. This amounts to "data surveillance" or monitoring of your daily life, which can pose a serious threat to our privacy and autonomy.

- Your SIN can be used to steal your identity. Along with other personal information, someone may be able to use your SIN to apply for a credit card or open a bank account, rent vehicles, equipment, or accommodation in your name, leaving you responsible for the bills, charges, bad cheques, and taxes.

...

> Under the new law, organizations like banks, telecommunications companies and airlines cannot require you to consent to the collection, use or disclosure of your personal information unless it is required for a specific and legitimate purpose.
>
> This means that unless an organization can demonstrate that your SIN is required by law, or that no alternative identifier would suffice to complete the transaction, you cannot be denied a product or service on the grounds of your refusal to provide your SIN.[19]

Further in Alberta Office of the Information and Privacy Commissioner's Investigation Report P2004-IR-001, we note the following finding with respect to requiring a SIN for the purpose of a credit check:

> [1] In January and February of 2004, a number of individuals contacted the Office of the Information and Privacy Commissioner (OIPC) to report that EPCOR, an electric utility company (the "organization"), collected and used their personal information contrary to the *Personal Information Protection Act* (PIPA or "the Act"). The complainants were concerned about the amount and type of personal information collected for the purposes of identifying customers over the telephone, conducting credit checks and managing accounts (for example, when customers called in to change a service, change demographic information or provide a meter reading). The complainants stated that it was unreasonable to be required to disclose sensitive personal information such as Social Insurance Numbers (SIN), Alberta drivers license numbers, passport numbers, etc. for the purposes of managing accounts. They were most concerned about the collection, use and retention of their SIN as a form of identification and as a requirement for credit checks. ...
>
> ...
>
> [9] **Credit reporting agencies do not require an individual's SIN to provide a credit check; the SIN is an optional element**. Other forms of personal information may be provided instead. However, credit reporting agencies confirm that the SIN improves accuracy and speeds up the process of obtaining a credit report.
>
> …
>
> [20] **I find it unreasonable for the organization to require a SIN if the credit reporting bureaus do not**.[20]

[emphasis added]

[19]OPC, *Fact Sheets – Social Insurance Number*, available at: http://www.priv.gc.ca/fs-fi/02_05_d_02_e.cfm.
[20]Office of the Information and Privacy Commissioner of Alberta (hereinafter AB IPC), Investigation Report P2010-IR-001, available at: www.oipc.ab.ca.

[32] If credit reporting agencies do not require an individual's SIN to provide a credit check, then why does SaskTel?

[33] Further, in terms of necessity, the following taken from the Office of the Privacy Commissioner of Canada's (OPC) office's website regarding the use of the SIN is insightful:

> *Principle 4.3.3*: "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes."
>
> - **Identification purposes are not in themselves considered a legitimate basis for requiring an individual to provide the SIN.** If the SIN is being requested for purposes of identification only, the organization must not in any way suggest to the individual that the SIN is required as a condition for providing a product or service or otherwise establishing a business relationship.
>
> - **Even where it is reasonable for an organization to ask a customer for proof of identity, a request for the SIN in particular must be represented and treated as optional. In verifying identity, an organization may request the SIN as one option among others, but never as a requirement in itself**.
>
> - When banks or other credit-granting institutions need to confirm identity for the purposes of running a credit check on a loan applicant, it is acceptable to ask for the SIN as one among several identification options, but it should not be required as a condition for granting credit.[21]
>
> [emphasis added]

[34] Again in SaskTel's training materials provided to our office, the following is stated in terms of when to request the SIN:

> Once you have determined that you do indeed need to create a new Customer and Account:
>
> 1. The Customer Summary window will appear…**Enter a minimum of 3 pieces of ID in the following fields:**

[21]OPC, *Fact Sheets - Best Practices for the use of Social Insurance Numbers in the private sector*, available at: http://www.priv.gc.ca/fs-fi/02_05_d_21_e.cfm#contenttop.

…

- Birthdate – Enter as MM DD YY.
- **SIN – This field is optional. Ask your customer for the information. However, if they do not wish to give it to you – tab to the next field**.
- Identification – SIMON will allow you room for either a driver's license or a health number. Click on the appropriate choice and fill in the information. If obtained enter the second number in the contact log.

[emphasis added]

[35] Further on this issue, taken from SaskTel's internal *Credit Check Tool*, is the following:

> The more customer information entered on this form, the more accurate this credit check decision will be.
>
> It could be considered a disservice to the customer if we do not fill in all of the information possible. Accurate data in = accurate results back.
>
> **If we miss the address, SIN or Credit Card, we're missing the good data associated with that ID**.
>
> …
>
> Personal Information
>
> …
>
> Identification
>
> - Required: two of the following items must be entered.
> - **SIN/SSN: Social Insurance Number is preferred by SaskTel**
> - Driver's License
> - Health Card Number
> - Other ID : (visa, amex, mc, treaty #, other ID)
>
> [emphasis added]

[36] It appears that the SIN is specifically asked for; as noted above, it is preferred by SaskTel. Instead of stating upfront it is optional, what is apparent is that SaskTel employees are only advised to accept other ID if the customer objects. At what point in the process does SaskTel *explicitly* tell its customers' providing is optional? I could not find any evidence that it does so at any time.

Health Services Numbers

[37] On the collection of the HSN, we advised SaskTel as follows:

> The definition of registration information includes the HSN in section 2(q) of HIPA is limited to "…information about an individual that is collected for the purposes of registering the individual for the **provision of health services** …". Given that Crown corporations are clearly defined as trustees under HIPA and that one's HSN is clearly "registration information" within the meaning of HIPA, a Crown corporation will need to consider section 4(3) of HIPA and determine whether FOIP has any application. In that event, authority for its collection, use and disclosure would have to be found in HIPA. Any trustee that has personal health information in its control should be mindful that the scheme of HIPA, the preamble of HIPA, and the general rules that bind every trustee underscore the sensitive nature of personal health information.
>
> In absence of clear legal authority to collect HSN of its customers, we remind you that section 52 of HIPA permits our office to recommend that a trustee "cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and destroy collections of personal health information collected in contravention of this Act" [Section 52(b)].

[38] Section 11 of HIPA is engaged as SaskTel collects HSNs. The section reads as follows:

> 11(1) An individual has the right to refuse to produce his or her health services number or any other prescribed identifying number to any person, other than a trustee who is providing a health service, as a condition of receiving a service.
>
> (2) Except as provided in subsection (3), no person shall require an individual to produce a health services number as a condition of receiving any product or service.
>
> (3) A person may require the production of another person's health services number:
>
> (a) for purposes related to:
>
> (i) the provision of publicly funded health services to the other person;
>
> (ii) the provision of a health service or program by a trustee; or
>
> (b) where authorized to do so by an Act or regulation.[22]

[22] *Supra* note 4 at section 11.

[39] Section 11 limits the collection of the HSN to purposes relating to the provision of health services or where authorized to do so by another law. SaskTel is clearly not in the business of providing diagnosis, treatment and care. SaskTel also has not provided any evidence that another law gives it authority to collect the HSN for its own purposes. Therefore, I find that SaskTel is not authorized to collect it. Accordingly, I recommend that SaskTel cease collecting immediately and destroy all collections of HSNs in its custody or control.

Driver's License Numbers

[40] In our correspondence with SaskTel on the matter of the collection of driver's license numbers, my office advised as follows:

> A number of Privacy Commissioners have also reminded those that would collect the driver's license that it is *not* a universal identity card but is a way for drivers to prove he/she is authorized to operate a motor vehicle and to enable the enforcement of traffic laws. **Further, there is consensus that recording driver's licence numbers is unnecessary in many instances as the goal may be achieved short of recording** (i.e. simply examining identification, recording the person's name as it appears on the licence, or perhaps by also recording the address displayed on the licence).[23] **If a customer attends on site, does SaskTel presently record the driver's license, or is the card just 'viewed' and a notation made that it was checked?**
>
> [emphasis added]

[41] The answer provided to the above bolded question was that it is only examined.

[42] We asked SaskTel what its understanding was of industry standards. Its early response to this question was vague as follows:

> On November 8, 2001 the Office of the Privacy Commissioner of Canada issued case summary 2001-24 where they determined that a reasonable person would find it appropriate for a company to collect personal information for the purposes of

[23]OPC, AB IPC and Office of the Information and Privacy Commissioner of British Columbia (hereinafter BC IPC), *Collection of Driver's Licence Numbers under Private Sector Privacy Legislation: A Guide for Retailers*, available at: http://www.priv.gc.ca/information/pub/guide_edl_e.pdf.

> determining if a potential customer was credit worthy or in the case of a repeat customer to confirm their identity.[24]
>
> **An individual complained that a telecom company's collection of personal information was inappropriate and if you refused to provide the two pieces of information the telecom company required a deposit before starting service**. The purpose for collecting the information is to run a credit check in order to determine a person's credit worthiness. Sufficient information is required in order to obtain a match within the credit bureaus database of information. **The provision of telephone services also constitutes an extension of credit.** Some telecom services, such a local phone services, are billed in advance while some, such as long distance charges are billed later. **This is a form of credit as customers are permitted to make long distance calls and are then billed after the calls are complete**.
>
> The Federal privacy office concluded that the policies and procedures of this telephone company were appropriate as the telephone company needed to determine the credit worthiness of a customer and on future transactions to confirm the identity of the person. **SaskTel's policy and procedures are consistent with this finding and with industry practices**.
>
> …
>
> ***Has SaskTel reviewed the practices of other industries that as part of their normal processes must established*** [sic] ***the ID of an individual via the phone?***
>
> > **SaskTel continually reviews the industry and privacy best practices and the collection, use and disclosure practices of other telephone companies in Canada. Current SaskTel policies and procedures are consistent with many other industry players.**
>
> [emphasis added]

[43] SaskTel did not indicate what those industry standards are and if those comply with privacy law and privacy best practices. In its submission dated May 22, 2012, SaskTel reiterated that it believes its practices are not out of line with what other companies may ask but again did not provide any specifics as to what those "other Crowns, businesses and those in the credit industries" collect. SaskTel is bound by FOIP and must comply with its Part IV regarding the protection of privacy; those organizations from which it may model its practices may not be similarly bound.

[24] *Supra* note 17.

[44] How many unique identifiers are too many, if acceptable to collect at all? On this question, I considered another case summary from the OPC:

> *Application*: Principle 4.4, which states that the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
>
> - **The Assistant Privacy Commissioner began her deliberations by noting that in previous findings involving telephone or wireless services issued by the Office, it was determined that the collection of two pieces of identification for the purposes of confirming creditworthiness or identity was reasonable**. (This fact was noted during the investigation, but the company continued to maintain its position.)
>
> - The investigation into this complaint established that the company was requiring three pieces of identification to activate an account: two were needed to ensure that the company obtained the correct credit bureau information and a third was required to positively identify the applicant.
>
> - Although the company maintained that its purposes could only be achieved with three pieces of identification, the Assistant Commissioner disagreed. For example, she noted that a driver's licence or passport meets the need to visually authenticate identity and provides verification of the date of birth, which is needed to obtain accurate information from the credit bureau. By asking for one of those, in combination with a credit card or bank information (which supports both identity authentication and accurate credit information), the company could still achieve its objectives. **In the Assistant Commissioner's view, a third piece of identification is not needed, and is not in fact industry practice**.
>
> - She therefore found that the company was requiring more personal information than necessary, contrary to Principle 4.4 of Schedule 1.
>
> ***Accordingly, the Assistant Commissioner concluded that the complaint was well-founded.***
>
> **Further Considerations**
>
> The Assistant Commissioner recommended that the company amend its policy to require only two pieces of personal identification and report back to her within 60 days on its progress in this regard.[25]
>
> [emphasis added]

[25]OPC, *PIPEDA Case Summary #2005-288* (February 1, 2005), available at: http://www.priv.gc.ca/cf-dc/2005/288_050201_e.cfm.

[45] Further, my office asked SaskTel to respond to the following bolded question. Its response is noted below.

> ***Is password an option only to customers who have PI on file?***
>
> Passwords are available to all customers. All new customers establish their initial service with SaskTel by providing personal information. Personal information is collected directly from the customer first to conduct a credit check and then is retained to verify the customer on future interactions.
>
> There is PSI regarding Account Passwords.
>
> CSR's are trained according to the information contained within the Account Password PSI. Passwords are an option for all customers.
>
> SaskTel systems are being developed that will allow customers to retain full control over their own passwords. Customers will be able to set up a password that is based on a secret question.

[46] If a password may be set-up, then what is the need for collecting any unique identifiers? This remains unclear.

[47] In keeping with the above noted OPC decision, it would appear the collection of three pieces of ID would be excessive.[26] In any event, whether or not SaskTel should collect *any* has not yet been determined as it has not demonstrated that the collection of each data element is necessary and authorized by law.

[48] The other purpose that SaskTel collects personal information under consideration in this Report is to determine creditworthiness.

[49] At first blush, the extent of personal information collected for credit purposes seems excessive. Bills come monthly; if a customer does not pay the amount owing, then SaskTel can take immediate action to address. Again, what about the option to just

[26]The above example involves a private sector company bound by a different type of law than SaskTel, a public body: *Personal Information Protection and Electronic Documents Act*, not FOIP.

provide a deposit? On this point, SaskTel in its most recent submission notes the following:

> SaskTel is a credit granting institution as we do provide services in advance without knowing that they will be paid for by the customer. … Unlike a bank, SaskTel does not have an asset it can repossess. Although court action is an option, it is rarely used. All debts at SaskTel are managed by an internal collection group with the assistance of an external collection agency as required.

[50] Customers have a right to know what his/her options are at the time of collection. This issue however will be addressed further under the notice section of this analysis.

[51] I understand that some flexibility may be needed as not all customers will be able to provide exactly the same information to prove creditworthiness; however, every data element collected must be justified and justified in conjunction with the others collected. If less information would suffice for the noted purposes, then the collection of more is excessive and in violation of FOIP. SaskTel should determine the least amount of personal information necessary for each purpose and collect only the minimal amount of personal information for both.

[52] It is clear that SaskTel also collects personal information of third parties. I will however deal with the indirect collection of third parties under another section of this analysis.

3. Is Saskatchewan Telecommunications complying with section 27 of *The Freedom of Information and Protection of Privacy Act*?

[53] The relevant section in FOIP is as follows:

> 27 A government institution shall ensure that personal information being used by the government institution for an administrative purpose is as accurate and complete as is reasonably possible.[27]

[54] The same Service Alberta resource noted earlier provides the following on accuracy:

[27] *Supra* note 1 at section 27.

> Section 35(a) requires the public body to make every reasonable effort to ensure that personal information is accurate and complete.
>
> A public body makes *every reasonable effort* when it is thorough and comprehensive in identifying practicable means to assure that personal information used to make a particular decision affecting the individual is accurate and complete.
>
> *Accurate* means careful, precise, lacking errors.
>
> *Complete* means including every item or element; without omissions or deficiencies; not lacking in any element or particular. Information is *complete* when all the information necessary to make the decision, and only the information that will be used for that purpose, is collected.
>
> Generally, if a public body collects personal information directly, it is likely to meet the requirement of making every reasonable effort to ensure that information is accurate and complete. This is especially so if the individual has signed a statement indicating that the information is accurate and complete. However, the burden of making every reasonable effort is higher when the consequences of a decision are greater.
>
> Public bodies should have adequate procedures in place to properly verify the accuracy and completeness of any personal information crucial to an application, transaction or action at the time the information is provided (see *IPC Orders 98-002* and *2001-004*).[28]

[55] SaskTel provided the following response to the bolded question below:

> ***How does ST know that the drivers' license numbers, SIN or HSN are valid?***
>
> SaskTel uses a check digit algorithm to validate SIN. For drivers licence and HSN SaskTel validates the number provided by ensuring we have been given the correct number of digits.

[56] SaskTel also provided a response to the following bolded question:

> ***If a customer goes into the store and shows a drivers license is it recorded or just noted?***
>
> It is only noted/examined by the CSR when used to verify the identity of the customer on site.

[28] *Supra* note 10 at p. 251.

[57] The above is of positive note. However, if SaskTel does not need to record in person, then why is it necessary to do so if the customer calls?

[58] If making inquiries over the phone, why would name, contact and account related information and date of birth not be sufficient proof of identity, especially when coupled with a password? This too remains unclear.

[59] If the only way to verify the accuracy of any unique identifier is as earlier noted, then section 27 is not being met. Further, if the number given does not have to be accurate then I do not understand why SaskTel collects drivers' license numbers, SINs and any other unique identifiers as acts only as another password that must be the same every time the individual calls in about his or her account. These questions have yet to be satisfactorily answered by SaskTel.

4. Is Saskatchewan Telecommunications meeting the notice requirements pursuant to section 26(2) of *The Freedom of Information and Protection of Privacy Act*?

[60] As I have already determined that the collection of most of the above noted data elements is directly from the data source, it follows that it must be in compliance with section 26(2) of FOIP. That provision is as follows:

> 26(2) A government institution that collects personal information that is required by subsection (1) to be **collected directly from an individual shall inform the individual of the purpose for which the information is collected** unless the information is exempted by the regulations from the application of this subsection.
>
> [emphasis added]

[61] Notification allows customers to understand the purpose, nature and extent of collection of personal information. Without this information, customers are unable to ensure that their rights under FOIP are respected.

[62] The following is also from Service Alberta's *FOIP Guidelines and Practices (2009)* resource referenced earlier:

> Examples of cases where collection of personal information requires notification under this provision include collection of personal information for enrolment in a program, to receive a service or to apply for a benefit, collection of personal information on a client survey and collection of individually identifying information on a course evaluation form.
>
> …
>
> Notification may be given in many ways. It may be
>
> - printed on a collection form;
> - contained on a separate sheet or in a brochure accompanying a form;
> - presented in a pop-up window linked to an online form;
> - published in a calendar of a post-secondary institution or an information brochure about a program that is provided to all applicants;
> - displayed on a notice hung on the wall or placed on a service counter; or
> - given orally, for example, during a phone call.
>
> …
>
> **The notice should be given at the time that the personal information is being collected**. In *IPC Investigation Report 2000-IR-007*, the Commissioner found that a school should have provided students or parents with a notification statement when school photographs were being taken rather than during the registration process since the collection of student photographs was not part of registration.
>
> …
>
> **When a notification is given orally, either in person or over the telephone, it is a good practice to refer the individual to a written copy of the notice or to provide a printed copy either at the counter or later by mail, and to retain a record that the notice was given**.[29]
>
> [emphasis added]

[63] The following case summary from the OPC speaks directly to the issue of notice:

> When the complainant attempted to obtain a new telephone service from the company in question, an operator asked her to supply two pieces of personal identification. When the complainant expressed reluctance, the operator told her that she would have to provide a deposit if she did not comply.

[29] *Ibid.* at p. 249.

It is company policy for operators to ask new subscribers for two pieces of identification, to demand a deposit in cases of refusal, and to explain the information collection simply as confirmation of identity. However, in cases where an applicant is a new customer with no previous business relationship with the company, the actual purpose of the collection is to run a credit check on the applicant, in accordance with CRTC regulations, given that the provision of telephone services constitutes an extension of credit on the company's part ...

Application: **Principle 4.2.3 states that purposes should be identified at or before the time of collection**. **Principle 4.3.2 states that organizations must make a reasonable effort to advise the individual concerned of the purposes for which the information will be used and must do so in such manner that the individual can reasonably understand. Principle 4.3.3 states that organizations must not, as a condition of supplying a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes**. Section 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Regarding Principle 4.3.3 and section 5(3), the Commissioner determined that a reasonable person would consider it appropriate for the company to collect personal information for the purpose of confirming whether a potential customer is credit worthy or, in the case of repeat customers, confirming identity.

He concluded that this aspect of the complaint was not well-founded.

Regarding Principles 4.2.3 and 4.3.2, the Commissioner determined that a reasonable person would conclude that the company did not explicitly state the purpose for its collection of personal information with respect to first-time subscribers.

He concluded that this aspect of the complaint was well-founded.

Further Considerations

As a result of the investigation of a similar complaint, the company in question had agreed to amend its practice in identifying purposes. **Specifically, the company was to inform first-time subscribers that the purpose of its information collection is to assess credit-worthiness given that the company supplies credit in the form of long-distance calling service.** It had not had time to implement the agreed upon changes when the complainant in this instance filed her complaint.[30]

[emphasis added]

[30]OPC, *PIPEDA Case Summary #2002-56* (July 2, 2002), available at: http://www.priv.gc.ca/cf-dc/2002/cf-dc_020702_2_e.cfm.

[64] As with the above example, we asked SaskTel about what it tells its customers upfront. On this question, SaskTel advised as follows:

> ***How does ST make it clear to customers calling in that he or she has options with respect to identifiers he or she provides?***
> SaskTel privacy policy describes the collection, use and disclosure of PI collected.
>
> SaskTel's privacy PSI describes the options a customer has in terms of what personal identifiers a customer may provide.
>
> CSR's are trained and coached according to the Account Information, Credit and Privacy PSI's.
>
> No change when new system, CRM, is implemented.

[65] The above does not specifically address the bolded question. We requested that SaskTel provide us with a copy of the policy referenced for our review so we may assess its adequacy. It did not.

[66] I note however that SaskTel has a privacy policy on its website which offers the following limited information:

> **What Are Your Choices?**
>
> We would like to have your consent to continue to collect, use and disclose your personal information for the purposes that we have outlined. However, you do have choices.
>
> - **You can have your name removed from our telephone, mail or e-mail marketing lists**. By doing so, you may not be made aware of certain products, services, and promotions offered by SaskTel. However, you will continue to be contacted as necessary to service your account, and you will receive marketing information included with your regular account mailings. Please allow us 30 days to complete your request. Some of our promotions may already be in progress when you submit your request, therefore you may be contacted during this time. If at any time you wish to reverse your decision, you may contact us at 1-800-352-7238. (SaskTel cellular customers may call 1-800-667-2355 to change their preferences)
>
> …
>
> - **You may refuse to provide personal information to us. You may also withdraw your consent at any time, subject to legal, contractual or**

> **practical restrictions and reasonable notice. However, in either case, this may limit our ability to serve you**.
>
> When you contact us, we will confirm that you are the registered customer. Please know that withdrawing your consent may prevent us from providing you with service and products in certain circumstances.[31]
>
> [emphasis added]

[67] SaskTel's website also offers the following information regarding deposits:

> SaskTel is proud to be the communications company of choice in our province, serving our customers on a world class communications network that is second to none. SaskTel reminds customers to pay for services provided upon receipt of their bill to avoid interruption or suspension of services. SaskTel provides customers with friendly reminders by phone and notifications on monthly telephone bills when a customer's account has not been kept current.
>
> SaskTel applies the following guidelines to customers' accounts in order to ensure timely payment for services provided. The following guidelines are in accordance with the terms and conditions of service as outlined in the attached document.
>
> - **SaskTel may require a deposit from customers who have unsatisfactory or no credit history with SaskTel and do not provide SaskTel with proof of current creditworthiness**.
> - SaskTel obligates its customers to pay in full all charges on their monthly bills by the due date specified.
> - SaskTel will immediately act to collect payment from customers with past due charges on their accounts.
> - SaskTel will apply late payment charges to the accounts of customers with past due charges on their accounts.
> - SaskTel may suspend service to, and terminate the accounts of, customers who fail to pay past due charges on accounts for which they are responsible, or who refuse to make payment arrangements that are acceptable to SaskTel.
> - SaskTel may disclose customers' account information to agencies outside of SaskTel for the purposes of evaluating customers' creditworthiness and/or collecting outstanding arrears on customers' accounts[32]
>
> [emphasis added]

[31] *Supra* note 18.
[32] Sasktel, *SaskTel Credit Policy and Collection Guidelines*, available at: http://www.sasktel.com/about-us/legal-and-regulatory/non-tariff-indices/non-tariff-sasktel-credit-policy-and-collection-guidelines.html.

[68] All of the above is too vague to be particularly informative to customers as it makes no mention of the options to provide contact and account related information, pay a deposit or set-up a password *instead* of providing unique identifiers and/or other sensitive personal information.

[69] In an email dated October 18, 2006, SaskTel's Privacy Officer noted the following on deposits:

> Attached is a Powerpoint presentation used to training [sic] our reps when conducting a credit check. **If a customer objects to a credit check they can still obtain service by putting down a deposit or reasonable alternative** (ie bank note). SaskTel has provisions within our Terms of Service to conduct a credit check without first obtaining customer consent however our normal business practice is to obtain customer consent.
>
> …
>
> I think its [sic] also important to note in our industry we are in fact extending credit to customers. A customer uses our service (ie long distance) but doesn't get billed for that use until the next month. From a business perspective it is very important to accurately assess the creditworthiness of our customer so we do place some emphasis on this and have put in place tools to help us out. A customer can very easily and quickly run up hundreds if not thousands of dollars in charges over a month.
>
> [emphasis added]

[70] A hyperlink on SaskTel's online credit policy and collection guidelines reveals a 30 page document titled *General Terms of Service, CRTC 21411*. On the collection of personal information, the following is noted:

> **SaskTel's Rights**
>
> **62 Deposits and Deposit Alternatives from Customers**
>
> 62.1 SaskTel may require a deposit from a customer only in the following circumstances:
>
> (a) before service is provided, if the customer has no credit history with SaskTel and does not provide proof of creditworthiness that is satisfactory to SaskTel,
>
> (b) if the customer has an unsatisfactory credit rating with SaskTel, based on payment practices over the previous six years for SaskTel services, and does not provide SaskTel with satisfactory current proof of creditworthiness, *or*

(c) if the customer clearly presents an abnormal risk of loss.

62.2 SaskTel must not require a customer to pay a deposit or provide a deposit alternative in an amount greater than all anticipated charges, including message toll charges, for three months of service.

62.3 If SaskTel requires a deposit, it must tell the customer why the deposit is required and also tell the customer that the following deposit alternatives are acceptable:

(a) a written guarantee from another person whose creditworthiness has been established to SaskTel's satisfaction,

(b) a bank letter of credit,

(c) an arrangement for payment of the customer's account by another person whose creditworthiness has been established to SaskTel's satisfaction, *or*

(d) under the circumstances, any other reasonable alternative the customer proposes.

62.4 The amount of any deposit required by SaskTel may be reduced if the customer requests that SaskTel block all message toll calls which would be charged to the customer's account.

62.5 SaskTel shall pay monthly interest on advance deposits held at a rate of interest equivalent to the rate of interest paid by the Canadian Imperial Bank of Commerce (CIBC) on Bonus Savings accounts as modified by CIBC from time to time.

62.6 SaskTel must show the amount of the customer's deposit on the customer's monthly bill.

62.7 SaskTel will review both the requirement and the amount for a deposit or deposit alternative at least once every six months or whenever the customer requests. If SaskTel finds that the amount of the deposit or deposit alternative exceeds anticipated charges for three months of service, including message toll service, SaskTel must refund the excess amount of the deposit or reduce the required amount of the deposit alternative to the appropriate level.[33]

[71] In terms of advice regarding the option for a customer to provide a deposit, SaskTel's internal *Credit Check Tool* offers the following direction:

[33]Sasktel, *General Terms of Service* (October 11, 2000), pp. 46 & 47, available at: http://sasktel.com/attachments/sasktel-credit-policy-and-collection-guidelines.pdf. Also note at 51.1 the following is stated: "Canadian Radio-television and Telecommunications Commission ("CRTC") is the federal regulatory body which regulates [SaskTel]. 51.2 These General Terms of Service bind both SaskTel and SaskTel's customers."

> The Decision "Unknown Risk"
> - **Customer has not established any credit and requires security**. SaskTel isn't sure of the propensity to pay.
>
> - A compromise between SaskTel and the customer is offering the choice of:
>
> - **Deposit**
> - **Preauthorized Payment (Bank or Credit Card)**
>
> [emphasis added]

[72] In its May 22, 2012 submission SaskTel offered the following update on when a deposit is warranted in its view:

> The first step in our credit check process is to compare the information provided by the customer, in the application process to SaskTel, against our internal records. We will look to see if the individual was a previous customer and match the data provided. If the customer provides a drivers license number, we will search our records looking for a match. If a match is found then the Customer Services Representative (CSR) will be advised to obtain a deposit, in the case of a credit risk or if they are a good credit risk according to our records, the CSR is advised to proceed with the order without a deposit.
>
> If no match is found then an external credit check may be undertaken, with the consent of the applicant, using the information provided to us by the customer. Once again, if a match is found SaskTel will either obtain a deposit or if the person's credit rating is good, proceed with the customer's request. If no match is found a deposit is requested.
>
> Deposits range from $75 to $500 depending on the service a customer may select. SaskTel now also accepts pre-authorized payments and will offer to a customer the option of having a guarantor co sign for service. However, for a person on low income or social assistance this can be prohibitive. **Moving to a deposit only policy may deny a person access to an essential service**…
>
> [emphasis added]

[73] My office did not suggest that SaskTel should move to a deposit only policy. Rather, our suggestion was to offer it as an option to those customers that do not wish to share unique identifiers or other sensitive information.

[74] Included in SaskTel's notice and other literature for the public should be a prominent statement advising customers of his or her right to pay a deposit or to set-up a password instead of giving personal information that he or she may object to providing.

[75] Without a clear script, accurate notices online, other print options and adequate training, I find that SaskTel is noncompliant with section 26(2) of FOIP.

Role of ExpressAddress

[76] On SaskTel's website,[34] there is a link to ExpressAddress. What is ExpressAddress? On its home page, the following is noted:

> **Welcome to ExpressAddress!**
>
> **ExpressAddress offers residential customers a convenient way to notify multiple Saskatchewan organizations of your move.**
>
> **To connect, transfer, disconnect or update your address for:**
>
> - telephone
> - water and sewer
> - vehicle registration
> - natural gas
> - health cards
> - library cards
> - driver's licence
> - security services
> - electricity
> - pet licences
> - internet
> - tv

and more...[35]

[77] On the above noted home page is also the word "Go". Once clicked, the following information is displayed:

> **Before you begin...** you may need the following information to complete your move online.
>
> **Identification such as:**
>
> - Driver's Licence
> - Provincial Health Card
> - Social Insurance Number

[34]Sasktel, *Changing your billing address,* available at: http://support.sasktel.com/app/answers/detail/a_id/15548.
[35]ExpressAddress, *Welcome to ExpressAddress,* available at: https://www.expressaddress.com/s/index.htm.

> The organizations that you select may require additional identification to process your request. If you do not wish to provide this information online please contact the organizations directly.
>
> **Account Numbers**
>
> - Current statements from each organization that you are notifying
> - Driver's Licence and Vehicle Registrations[36]

[78] On ExpressAddress' participating organizations services page, SaskTel is listed.[37] I am unclear as to the nature of their relationship. Does ExpressAddress function as an information service provider? Have both signed a service agreement or have a contract in place? In its final submission to us, SaskTel did not provide any response to our earlier recommendation to "review its arrangement with ExpressAddress to ensure that it is not collecting any personal information that it does not have a legitimate need and right to have." This recommendation still stands.

5. Do Saskatchewan Telecommunications' indirect collection practices conform with section 26 of *The Freedom of Information and Protection of Privacy Act*?

[79] The following statement from SaskTel's materials is of great concern:

> **The more information we have on all the occupants in the household the better. If there is no room on the credit record use the contact log.**
>
> [emphasis added]

[80] The applicable section of FOIP is as follows:

> 26(1) A government institution shall, where reasonably practicable, collect personal information directly from the individual to whom it relates, **except where**:
>
> (a) the individual authorizes collection by other methods;
>
> (b) the information is information that may be disclosed to the government institution pursuant to subsection 29(2);

[36] *Ibid.*
[37] Expressaddress, *participating organization services*, available at: https://www.expressaddress.com/s/services/all_organization_services.htm.

(c) the information:

(i) is collected in the course of, or pertains to, law enforcement activities, including the detection, investigation, prevention or prosecution of an offence and the enforcement of:

(A) an Act or a regulation; or

(B) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada; or

(ii) pertains to:

(A) the history, release or supervision of persons in custody, on parole or on probation; or

(B) the security of correctional institutions;

(d) the information is collected for the purpose of commencing or conducting proceeding or possible proceeding before a court or tribunal;

(e) the information is collected, and is necessary, for the purpose of:

(i) determining the eligibility of an individual to:

(A) participate in a program of; or

(B) receive a product or service from;

the Government of Saskatchewan or a government institution, in the course of processing an application made by or on behalf of the individual to whom the information relates; or

(ii) verifying the eligibility of an individual who is participating in a program of or receiving a product or service from the Government of Saskatchewan or a government institution;

(f) the information is collected for the purpose of:

(i) management;

(ii) audit; or

(iii) administration of personnel;

of the Government of Saskatchewan or one or more government institutions;

> (g) the commissioner has, pursuant to clause 33(c), authorized collection of the information in a manner other than directly from the individual to whom it relates; or
>
> (h) another manner of collection is authorized pursuant to another Act or a regulation.
>
> (2) A government institution that collects personal information that is required by subsection (1) to be collected directly from an individual shall inform the individual of the purpose for which the information is collected unless the information is exempted by the regulations from the application of this subsection.
>
> (3) Subsections (1) and (2) do not apply where compliance with them might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected.[38]
>
> [emphasis added]

[81] SaskTel's internal procedures advises its staff as follows: "Alternate Contact – Ask for the name and telephone number of a parent, relative or long term contact who will be able to contact the new customer if SaskTel is unable to." For seasonal workers, collect "[t]he service number of relative or friend in the city."

[82] SaskTel had at least at one time collected information on roommates, alternate contacts, friends and others and appears to have verified with its customers' employers employment status. Does SaskTel tell its customers that it will contact his or her employers? I found nothing to indicate it does. Yet in its training materials clearly it is stated: "[y]ou *must never* take an application from someone that is calling in on another's behalf." SaskTel recognizes it is not appropriate to take an application from someone calling in on someone else's behalf; however it appears it has actively collected personal information of third parties without any apparent authority.[39]

[83] It is interesting that SaskTel states that "you must never take an application from someone that is calling in on another's behalf," but does indirectly by asking the principal customer for information on his or her roommates: "enter the name(s) of any

[38] *Supra* note 1 at section 26.
[39] No section of FOIP was raised by SaskTel to justify its actions and it does not appear it sought the express consent of third parties to collect the information in question either.

roommate(s) and their place of employment, ID and contact number." This is more than an indirect collection; it appears SaskTel is allowing the primary to act as the roommate's surrogate. For this to happen, authority under section 59 of FOIP must be evident.[40] I find it is not.

[84] It clearly states at section 58 of SaskTel's *General Terms for Service Policy* that it is the customer that is responsible for charges:

> **58 Customer's Responsibility for Charges**
>
> 58.1 The customer must pay all applicable monthly charges in advance. Other periodic charges and applicable service charges must be paid in accordance with the SaskTel Tariff. The customer must also pay for all calls:
>
> (a) placed from the customer's telephone line,
>
> (b) placed through the demarcation at which the customer receives service,
>
> (c) received at the customer's telephone line or through the demarcation where the charges have been accepted by a person receiving the call, *or*
>
> (d) charged to the customer's telephone number (or customer's SaskTel account), the customer's SaskTel Calling Card or to the customer through other credit arrangements approved by SaskTel.
>
> 58.2 The customer must pay for these calls regardless of whether the person who;
>
> (a) placed the call,
>
> (b) accepted the charges, or
>
> (c) charged the call

[40] Section 59 of FOIP reads as follows:

59 Any right or power conferred on an individual by this Act may be exercised:

(a) where the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate;

(b) where a personal guardian or property guardian has been appointed for the individual, by the guardian if the exercise of the right or power relates to the powers and duties of the guardian;

(c) where a power of attorney has been granted, by the attorney if the exercise of the right or power relates to the powers and duties of the attorney conferred by the power of attorney;

(d) where the individual is less than 18 years of age, by the individual's legal custodian in situations where, in the opinion of the head, the exercise of the right or power would not constitute an unreasonable invasion of the privacy of the individual; or

(e) by any person with written authorization from the individual to act on the individual's behalf.

had the customer's permission to do so.

58.3 SaskTel, if it so elects, may collect all or part of the charges referred to in Item 58.1 from the person placing the call or from any person who may otherwise be responsible for the charges incurred.[41]

[85] What is the need then for roommate information? In the preliminary assessment my office shared with SaskTel, we indicated that unless SaskTel is able to demonstrate that its collection practices are compliant with FOIP, it should cease collecting immediately.

[86] In its response to our assessment, SaskTel advised as follows:

> The Customer Relationship Management (CRM) project within SaskTel has significantly changed the customer application process now in place for customers who are applying for service at SaskTel.
>
> One of the more significant changes with CRM, in addition to reduced personal data collection, **is the move to only have one name on the bill and to hold the one person accountable for any outstanding amounts**. This means that SaskTel **only collects information about the person whose name will appear on the billing statement**. The customer information collected in the service application process is also used to authenticate a customer who may call in later and to assess their creditworthiness. For example, **information about a roommate** or using credit card information **is no longer requested as part of the application process**.
>
> [emphasis added]

[87] I applaud SaskTel for the above. I am however clearly concerned with the breadth of personal information previously collected indirectly by SaskTel on its customers' roommates, friends, parents and others without apparent authority. SaskTel has not indicated at what point this practice began and ended and has not indicated that it has purged its system of and no longer uses this information. I therefore recommend that SaskTel purge its systems of all data collected indirectly about its customers and third parties collected without the requisite authority within 60 days of receipt of this Report.

[41] *Supra* note 33.

6. Does Saskatchewan Telecommunications have appropriate safeguards in place to adequately protect its customers' personal information or personal health information?

[88] As already discussed, SaskTel has and is collecting a great deal of personal information from its customers and other third parties. As SaskTel also collects personal health information,[42] section 16 of HIPA is engaged. It provides as follows:

> 16 Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.[43]

[89] FOIP does not contain the same explicit language noted above; it is my view nonetheless that all government institutions must also have adequate safeguards in place to protect personal information in its possession or control.

[90] On the matter of safeguards, SaskTel provided the following submission:

> SaskTel employs some of the latest in Call Centre technology. If a customer enters their actual telephone number, the CSR presented with the call will receive both the call and the customer's account information, displayed at their work station, simultaneously. The CSR will then ask for the customer's name and date of birth to determine if the correct account has been displayed.

[42] The health services number of some of its customers and potentially of some third parties.
[43] *Supra* note 4 at section 16.

If the customer enters zeros or a telephone number that is not associated with an active account, no information is displayed. In this case, the CSR will first ask for the name and the telephone number of the account. When the account information is displayed, they will request that the customer provide their date of birth (DOB).

…

The vast majority of SaskTel's business is handled over the telephone. New service is established with customers whom we may never see in person. Services are added, changed and deleted over the telephone. As the province grows and technology becomes more widespread more of our business will be conducted over the phone and now electronically over the internet or on a wireless basis using applications and a smart phone.

…

From a customer standpoint we retain some very sensitive personal information. SaskTel has the customer's call detail for telephone service, cell service and text message service. The call detail provides the date, time and number of the person you called. We are often contacted by a customer or their legal counsel who is going through a break up in their relationship and are asked to provide the call detail of the other party involved. The customer is of the view that if they can provide who the other party called it will help them build their case against the other's infidelity. Only the person on the account has a right to access this information and it must be protected from unauthorized disclosure by SaskTel.

Customers will often choose not to display their telephone number of have their number or address not published in the phone book for one reason or another. A prison guard may not want to have their name or number displayed when they are placing a telephone call. They may not want to have the number or addressed published in a phone book. This is done in order to protect them.

For someone who is trying to reclaim their life … If this was to happen the customer would be exposed to potential harm.

SaskTel has many privacy enhancing features available for customers to subscribe to. If we were to inadvertently disclose their personal information to the wrong person we could literally put the person's life in grave danger. To publish a number accidentally could have devastating effects.

Many customers call into SaskTel to have their email or voice mail passwords reset. Resetting a password could permit the caller full access to a customer's email or voice mail. Providing access to the wrong persons can have detrimental repercussions.

…

In addition to our provincial privacy legislation, SaskTel is also governed on a Federal level by the Canadian Radio-television and Telecommunications Commission

> (CRTC). SaskTel must follow the Terms of Service as approved by the CRTC. The terms do contain provisions to maintain the confidentiality of customer records. **Unless the customer provides express consent or disclosure is pursuant to legal power, all information kept by SaskTel cannot be disclosed to anyone other than the customer with the exception of listed name, address, and phone number.** These are very strong provisions that place limits on our ability to disclose personal information. **The terms also provide clear direction requiring SaskTel to ensure we are dealing with the person whose name is on the account**.
>
> …
>
> SaskTel recently started work on a program called Customer Relationship Management (CRM) whose objective is to enable our CSRs to serve customers in a more efficient manner. In addition to implementing new technology, a component of this program will include implementing business simplification opportunities. This has resulted in a detailed analysis on several of our processes, one being the collection of customer information. We are in the process of reviewing the collection of customer information to ensure we limit what we collect while still meeting our business requirements. **The project team is mindful of our privacy obligations as they work to meet SaskTel's business requirements, while continuing to meet our customer's satisfaction expectations**.
>
> **As part of CRM, SaskTel has also started work on implementing the technical ability for all customers to have an account password. The new industry standard capability is fully managed by the customer and is based on a customer selected secret question**.
>
> [emphasis added]

[91] The above does not offer much in terms of what specific safeguards SaskTel utilizes to protect privacy. Rather its submission speaks to why it is important to keep confidential the personal information it collects.

[92] Along with its above noted submission, SaskTel provided answers to the following questions posed by my office. I note the questions were reframed somewhat by SaskTel as follows:

> ***Does SaskTel (ST) rely solely on the PI provided over the phone because they are the most secure or convenient?***
>
> SaskTel's mode of operation is primarily conducted through a call centre.…
>
> Procedures are documented in Account Information, Credit and Privacy PSI's.

> CSR's are trained according to the information contained within the Account Password PSI. Passwords are an option for all customers.
>
> **PI will be hidden from the CSR as we move to more passwords in Customer Relationship Management (CRM).**
>
> …
>
> ***Has SaskTel experienced any fraudulent activity as a result of this practice?***
>
> SaskTel is unaware of any fraudulent or criminal activity. To the best of our knowledge there are no open police investigation or has any of this type of activity been reported to SaskTel Corp Security. …
>
> ***Who has access to the PI?***
>
> Access to personal information is based on a need to know or need to access as outlined in the Code of Business Conduct and Corporate Security Policy.
>
> SaskTel has an internal authorization procedure to grant access to internal systems.
>
> Code of Conduct is reviewed with every employee once a year.
>
> ***Is an audit trail maintained each time a customer's personal information is retrieved and viewed by call center staff or other staff?***
>
> ***Is this audited at regular intervals or randomly?***
>
> ***Please explain why or why not?***
>
> **SaskTel has many internal system with varying degrees of audit trails or logs. The primary systems which contain PI do have admin, physical and logical controls in place.**
>
> **In the future, systems such as CRM will have the capability.**
>
> **System audits are periodic**. The requirement to undertake an audit may be determined by recent issues, risk assessment, management request etc.
>
> **SaskTel has a very active internal audit program that staffed internally and reports directly to the President. SaskTel Corporate Security is also very active and is currently embarking on a vulnerabilities program**…
>
> [emphasis added]

[93] The above is impressive as it may help to detect and deter any potential misuse of personal information or personal health information contained within its systems. It is

not evident however that SaskTel has considered the sensitivity factor of the personal information or personal health information it collects and altered its practices accordingly based on the subsequent risks posed to the data subjects in question if a breach occurs.

[94] I previously raised with SaskTel the following regarding risk management:

> Identification and authentication are fundamentally about the management of risk:
>
> - The risk to the organization of, through bad authentication practice, either denying access to a legitimate customer or giving access to an impostor;
> - **The risk to individuals that their personal information is lost or inappropriately disclosed, and that their identity, finances, and privacy are compromised**.
>
> "Risk" should always be understood to have two aspects: the likelihood of an event occurring and the severity of the consequences if it does occur. Proper risk management requires that both these two aspects of risk are considered.
>
> **The stringency of authentication processes should be commensurate with the risk to the information being protected, risk being a function of the sensitivity of the information or service in question, the vulnerability of and the perceived threat to that information or service**.
>
> [emphasis added]

[95] From the OPC and Office of the Information and Privacy Commissioner of Alberta's *Report of an Investigation into the Security, Collection and Retention of Personal Information TJX Companies Inc. /Winners Merchant International L.P*. is the following on sensitivity of personal information:

> 75. The sensitivity of personal information is a consideration in an assessment of harm and risk. Certain types of personal information can be used to harm or perpetrate fraud against individuals more easily than other information.
>
> 76. We are of the opinion that "reasonable security measures" compels organizations to consider the possible harm to individuals if the information were in the wrong hands. Principle 4.7.2 of PIPEDA explicitly recommends that organizations consider sensitivity when implementing security measures.[44]

[44]OPC and AB IPC, *Report of an Investigation into the Security, Collection and Retention of Personal Information* (September 25, 2007), available at: http://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp.

[96] In our publication *Helpful Tips: Privacy Breach Guidelines*, my office discussed what constitutes 'sensitive information' as follows:

> What data elements have been breached? Generally, the more sensitive the information, the higher the risk. PHI, Social Insurance Numbers, and/or financial information that could be used for identity theft are examples of sensitive information.[45]

[97] The following on identity theft/fraud is taken from a publication titled *Personal Information and Scams Protection - A Canadian Practical Guide* from the RCMP's website:

> The RCMP defines identity fraud as the unauthorized acquisition, possession or trafficking of personal information, or, the unauthorized use of information to create a fictitious identity or to assume/takeover an existing identity in order to obtain financial gain, goods or services, or to conceal criminal activities. **Your Social Insurance Number, birth certificate, passport and driver's licence are the prime information targeted by criminals**...[46]
>
> [emphasis added]

[98] Personal information and personal health information needs to be protected by security safeguards appropriate to the sensitivity of the information. The more sensitive the information, the higher the level of protection should be.[47] It however does not appear that SaskTel has classified the data collected in question nor conducted a risk assessment.

[99] SaskTel is doing some very positive things. However, I find that SaskTel's efforts are falling short in terms of FOIP and HIPA compliance. This is due in part to its apparent desire to collect as much personal information on its customers and associated third parties as possible contrary to the 'data minimization principle'.[48] Also, I find this as SaskTel has offered little in terms of what specific physical, administrative and technical

[45]Saskatchewan Office of the Information and Privacy Commissioner (hereinafter SK OIPC), *Helpful Tips: Privacy Breach Guidelines*, p. 8, available at: www.oipc.sk.ca/resources.htm.
[46]Royal Canadian Mounted Police, *Personal Information and Scams Protection – A Canadian Practical Guide* (March 1, 2007), available at: http://www.rcmp-grc.gc.ca/scams-fraudes/canad-practical-pratique-guide-eng.htm.
[47]In SK OIPC Investigation Report H-2007-001 at [44], I quoted BC IPC Investigation Report F06-01 which quotes another BC IPC Investigation Report F06-02. Both references speak to this need.
[48]The practice of disclosing the least amount of information when required is called the 'data minimization principle'. For more see SK OIPC Investigation Report LA-2010-001 at [47] to [48] available at www.oipc.sk.ca/reviews.htm.

safeguards it has in place to protect personal information and personal health information in its possession/custody or control.

[100] Now that SaskTel is moving to the new system noted, it has the opportunity to fully examine its collection and security practices by conducting a Privacy Impact Assessment (PIA).[49] From our perspective, it is critical that SaskTel start the PIA process immediately. Once it is determined which data elements are crucial, tied to legitimate business purposes and it is able to demonstrate its authority to collect, the primary question to address will be "are security measures in place commensurate with the sensitivity of the information recorded?"

[101] My office shared our preliminary assessment with SaskTel on or about April 12, 2012. Its response dated May 22, 2012 did not speak directly to the recommendations made and rather than stating if it would or would not comply with our recommendations, offered the following remarks:

> **It is well known within SaskTel that any employee who uses or discloses customer information, and is not authorized to do so as part of their job, will be terminated**. SaskTel starts with the premise that a breach of privacy starts with termination and if circumstances warrant, discipline will be something less that [sic] termination…
>
> **SaskTel's activities are guided by a set of values and principles designed to help employees make ethical decisions. This set of values, principles and the guidelines are SaskTel's Code of Business Conduct. The Code of Business Conduct is not, nor can it be, a detailed list of guidelines to cover every conceivable ethical, moral or legal circumstance that may confront SaskTel employees. Employees are asked to use common sense and sound judgment in many situations. SaskTel expects all employees to uphold the corporate values in their work activities**.
>
> The Partnership for Excellence (PFE) is a participative process, which is meant to encourage all employees to take responsibility for continuous improvement in their jobs and their personal development. It is not simply an annual review of an individual's achievements and successes…
>
> …

[49] Template available at: www.oipc.sk.ca/resources.htm.

> Each year managers review the Confidentiality Checklist with each employee and provide them with a copy of the Master Agreement for Local Interconnection (MALI). Both of these documents are attachments to the PFE form and must be signed by the manager and submitted every year to Human Resources. We view it as critically important for employees to be made aware of the need to safeguard SaskTel information. Employees need to know what information needs to be safeguarded as well as *how* they are expected to safeguard such information. Completing the confidentiality checklist, which highlights key policies and procedures, serves as an annual reminder, reinforcing the importance of safeguarding SaskTel information. Managers must submit the completed checklist with each PFE or it will not be considered complete.
>
> As part of the confidentiality checklist, Managers review: The Code of Business Conduct, SaskTel's Term of Service, MALI and our obligations to ensure the protection of the personal information of employees and customers in accordance with SaskTel's privacy management policies, principles and practices derived from Saskatchewan's *Freedom of Information and Protection of Privacy Act* [sic], our Privacy Framework and the Canadian Standards Association (CSA) Model code for the Protection of Personal Information.
>
> The following is provided to employees during the PFE process:
>
> > *Confidential, proprietary and/or employee information may be used only in the conduct of business by authorized personnel and accessed by or disclosed to only those who "need to know" or as prescribed by law and SaskTel policies and procedures. Unauthorized accessing, personal use or disclosure of customer, competitor or corporate information will be subject to discipline action, up to and including dismissal.*
>
> All access to CRM is roll-based. This means that when an employee is set up for access to CRM they only receive the access that they require to perform their job. Every employee has a unique user ID and password. Employee authentication is controlled…
>
> The primary call centre locations have security guards…
>
> **SaskTel also has a full-time Security department … who help define and enforce the various administrative, technical and physical safeguards in place around SaskTel.**
>
> [emphasis added]

[102] In some respects SaskTel is taking a proactive approach to ensure FOIP compliance by its employees. In others, it is not. It is troubling that SaskTel does not mention HIPA at all in its materials or responses when it is clearly engaged. Also of concern is that SaskTel

has not apparently conducted a PIA or risk assessment in its move to its new system. In the case of a government institution bound by FOIP and HIPA, I find the reliance on its employees to make ethical decisions based on values, principles and common sense is insufficient to ensure compliance with these laws. I am reassured to a certain extent as SaskTel managers revisit privacy obligations with its employees on a regular basis and that it would consider employee discipline if appropriate in the circumstances. With reference to Code of Business Conduct, values, principles and guidelines, what is most important is full compliance with the statutes that govern namely FOIP and HIPA. To the extent that any conflict exists, the legislation must prevail.[50]

[103] In its final response to my office, on June 29, 2012, SaskTel restated our earlier recommendations and provided its response to each in italics as follows:

> **Recommendations:**
>
> 1. That SaskTel conduct a privacy impact assessment as part of its Customer Relationship Management program to ensure that any new proposed practice or processes will be compliant with FOIP and HIPA.
>
> *SaskTel agrees to conduct a privacy impact assessment.*
>
> 2. That SaskTel immediately cease collecting its customers' HSN and develop a plan to purge its systems of it.
>
> *SaskTel, as a trustee, is of the view that in order to continue to run an effective and efficient business operation, related to the delivery of our programs and activities, the collection of HSN is required. It is important and contributes to our overall financial health. Although clearly optional, it may assist in the reduction of bad debt reduction. From a customer standpoint, this optional piece of information may also help to establish a credit rating with SaskTel. HSN may be used to help establish a customers* [sic] *credit worthiness, establish their identity when first establishing service, collection of a debt and to help verify a customer when they call into SaskTel at a later date.*
>
> 3. That unless SaskTel is able to establish the necessity of and its authority to collect, that it cease collecting its customers' SIN, student and driver's licenses numbers.
>
> *SaskTel is of the view that in order to continue to run an effective and efficient business operation, related to the delivery of our programs and activities, the*

[50]SK OIPC, Investigation Report H-2010-001 at [42] to [44]; available online: http://www.oipc.sk.ca/reviews.htm.

collection of SIN, student numbers or drivers license is required. It is important to our overall financial health. These pieces of information assist SaskTel in the reduction of bad debt reduction. From a customer standpoint, these optional pieces of information may also help to establish a credit rating with SaskTel. These pieces of information may help and may be used to establish a customers [sic] *credit worthiness, establish their identity when first establishing service, collection of a debt and to help verify a customer when they call into SaskTel at a later date.*

Where financing of a program or activity is requested by the customer, SIN is a distinct identifier that may be used to determine a customers [sic] *credit and financial status.*

SaskTel will not refuse service if any customer objects to the disclosure of their SIN. In the provision of service SaskTel will generally request 2 pieces of identification.

4. That SaskTel review its arrangement with express address to ensure it is not collecting any personal information that it does not have a legitimate need and right to have.

SaskTel agrees to review express address.

5. That SaskTel immediately cease collecting third party personal information from its customers without the consent of the third parties in question unless the requisite authority and necessity is first established.

SaskTel agrees to cease collecting third party information but will rather endeavour to collect it directly from the person to whom it relates.

6. That SaskTel review its collection practices for purposes of determining credit worthiness to ensure is keeping with the data minimization principle.

SaskTel agrees to undertake a review of our collection practices to determine credit worthiness.

7. That SaskTel improve its privacy policy and develop a script to better meet its notice requirement as previously detailed in this analysis.

SaskTel agrees to improve its privacy policy and develop a process to meet the notice requirement.

[104] As SaskTel did not agree to comply with all of my recommendations as noted above, I have determined it necessary to issue this Report. I am especially troubled by SaskTel's decision to continue to collect the HSN.

IV FINDINGS

[105] I find that Saskatchewan Telecommunications does not have the requisite authority to collect its customers' health services numbers.

[106] I find that Saskatchewan Telecommunications has not justified its collection of other unique identifiers and many of those data elements used to establish credit worthiness.

[107] I find that Saskatchewan Telecommunications is not compliant with section 27 of *The Freedom of Information and Protection of Privacy Act*.

[108] I find that Saskatchewan Telecommunications has not demonstrated it has authority to indirectly collect third party personal information of its customers' families and associates.

[109] I find that Saskatchewan Telecommunications is not fully meeting the notice requirements of subsection 26(2) of *The Freedom of Information and Protection of Privacy Act* in its collection of its customers' personal information.

[110] I find that Saskatchewan Telecommunications' safeguards are insufficient to fully protect personal information and personal health information in Saskatchewan Telecommunications' possession/custody or control.

V RECOMMENDATIONS

[111] That Saskatchewan Telecommunications conduct a Privacy Impact Assessment as part of its Customer Relationship Management program to ensure that any new proposed practice or processes will be compliant with *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*.

[112] That Saskatchewan Telecommunications immediately cease collecting its customers' health services numbers.

[113] That unless Saskatchewan Telecommunications is able to establish the necessity of and its authority to collect, that it cease collecting its customers' unique identifiers.

[114] That Saskatchewan Telecommunications review its arrangement with ExpressAddress to ensure it is not collecting any personal information that it does not have a legitimate need and right to collect.

[115] That Saskatchewan Telecommunications immediately cease collecting third party personal information from its customers without the consent of the third parties in question unless the requisite authority and necessity is first established.

[116] That Saskatchewan Telecommunications review its collection practices for purposes of determining credit worthiness to ensure it is keeping with the data minimization principle.

[117] That Saskatchewan Telecommunications improve its privacy policy and develop a script to better meet its notice requirement as previously detailed in this Report.

[118] That Saskatchewan Telecommunications purge its systems of all data collected without the requisite authority within 60 days of receipt of this Report.

Dated at Regina, in the Province of Saskatchewan, this 27th day of August, 2012.

R. GARY DICKSON, Q.C.
Saskatchewan Information and Privacy Commissioner