SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT F-2014-002

Financial and Consumer Affairs Authority of Saskatchewan

Summary: The Office of the Saskatchewan Information and Privacy Commissioner (OIPC) received a breach of privacy complaint that related to the collection and disclosure of the Complainant's personal information and personal health information by the Saskatchewan Financial Services Commission (SFSC). During the course of the investigation, the SFSC was renamed the Financial and Consumer Affairs Authority of Saskatchewan. The Complainant alleged that the SFSC inappropriately collected and disclosed her personal information and personal health information during its Securities Division's investigation into her business dealings. The Commissioner found that the SFSC failed to demonstrate that it had authority to collect and disclose the Complainant's personal information and personal health information under *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Health Information Protection Act* (HIPA) respectively. Further, she found that the SFSC violated the data minimization principle. Finally, the Commissioner found that the SFSC failed to sufficiently safeguard the Complainant's personal information and personal health information as was lacking appropriate written policies and procedures to help ensure compliance with FOIP and HIPA when undertaking such investigations. The Commissioner recommended that the SFSC develop appropriate written policies and procedures to achieve compliance with FOIP and HIPA in the course of its investigative activities.

Statutes Cited: *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, ss. 2(1)(d)(ii), 24, 24(1), 24(1)(a), 24(1)(b), 24(1)(j), 24(1)(k)(i), 25, 26, 29(1), 29(2), 33(d); *The Health Information Protection Act*, S.S. 1999, c. H-0.021, ss. 2(b), 2(m), 2(m)(i), 2(m)(ii), 2(t)(i), 16, 23, 24, 27, 42(1)(c), 52; *The Securities Act, 1988*, S.S. 1988-89, c. S-42.2, s. 12;

Alberta's *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 4(b), 33.

Authorities Cited: Saskatchewan OIPC Investigation Reports F-2013-002, F-2012-001, F-2012-005, F-2012-002, F-2009-001, F-2007-001, LA-2013-001, LA-2010-001, H-2013-001, H-2010-001; Saskatchewan OIPC Review Report F-2014-001.

Other Sources Cited: Saskatchewan OIPC, *Helpful Tips: OIPC Guidelines for Public Bodies/Trustees in Preparing for a Review*; Government of Alberta, Service Alberta, *FOIP Guidelines and Practices* (2009); Office of the Privacy Commissioner of Canada, *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada*.

I BACKGROUND

[1] This Investigation Report involves the Financial and Consumer Affairs Authority of Saskatchewan (FCAA). When the privacy breach complaint was made to our office and during the course of the investigation, it was known as the Saskatchewan Financial Services Commission (SFSC). I will refer to it as the SFSC or FCAA as appropriate in the context throughout this Investigation Report.

[2] On or about February 14, 2012 and February 15, 2012, the Complainant appears to have raised with the SFSC her concern, among other things, that it inappropriately collected and disclosed her personal information and personal health information through the course of its investigation into her business dealings. The Complainant provided our office with a copy of the SFSC's February 22, 2012 response to her allegations.

[3] The Complainant was not satisfied with the response from the SFSC, as she contacted my office on March 8, 2012 requesting an investigation into the matter.

[4] My office provided notification letters to both the SFSC and the Complainant on or about June 14, 2012, advising that it was our intention to conduct an investigation into the Complainant's privacy related concerns. Those included concerns the Complainant had that the SFSC was "in possession of [her] medical records", "that investigators

inappropriately disclosed [her] personal information to persons not employed by the SFSC" and regarding information contained in a Notice of Hearing. In my office's June 14, 2012 letter to the SFSC, we stated the following:

> It appears that **you have not completed an internal investigation** into the complainant's allegations that investigators inappropriately disclosed the complainant's personal information to persons not employed by the SFSC. **Please conduct an internal investigation immediately and provide a copy at your earliest convenience**. Also, please advise us if, in your view, a breach (or breaches) of privacy has occurred.
>
> As well, **please advise how SFSC took into consideration the 'data minimization principle' (least amount of personal information necessary for the purpose) when the information in question was disclosed**.
>
> …Please **provide our office with any written policies or procedures** that are in place regarding the handling and security of **personal information and personal health information that is in your custody or control**…
>
> [emphasis added]

[5] On July 11, 2012, my office received a submission from the SFSC. However, the submission was deficient as it did not include all of what was requested in my office's notification letter.

[6] On October 3, 2012, my office responded to the SFSC via email advising of the deficiencies and again sought what was not provided.

[7] My office received another submission from the SFSC on November 27, 2012 dated November 23, 2012. The submission was again deficient. Also, the SFSC indicated it had not yet undertaken an internal investigation as my office had requested. Rather, it indicated that the SFSC would retain an independent reviewer "to conduct the review of the Securities Division's practices".

[8] However, no clear timeline was provided by the SFSC as to when it would be conducting and concluding its internal investigation. My office advised the SFSC via email on May 7, 2013, that it needed to provide "all materials to support the SFSC's position" by May

10, 2013. Further, my office stated: "…I note page 3 of your submission that **the SFSC intended to have an independent reviewer investigate the second issue of complaint** – the communications of investigators. However, it is now several months later and **nothing was received**." [emphasis added]

[9] On May 10, 2013, the SFSC advised my office as follows:

> As to our position with respect to the allegations made by [the Complainant] concerning the conduct of FCAA investigators, we would reiterate all of our prior submissions with respect to this issue. **I can also advise that the Head intended, and still intends, to conduct a full, formal investigation into the allegations after the Hearing Panel makes a decision in the proceedings against [the Complainant]** and her companies, which may include findings with respect to these very same allegations. **However, we are not prepared to do that until the proceedings against [the Complainant] have concluded**, as there is a very real possibility of interference with and disruption to the quasi-judicial proceedings currently underway against [the Complainant] if the FCAA were to conduct another simultaneous proceeding with respect to some of the exact same issues. Interfering with the proceedings currently underway is not in the interest of [the Complainant] or the public.
>
> [emphasis added]

[10] On or about September 10, 2013, my office provided its preliminary analysis to the SFSC. A number of recommendations were made including that the SFSC provide an apology letter to the Complainant and to develop certain policies and procedures to reflect the obligations the SFSC has under *The Freedom of Information and Protection of Privacy Act* (FOIP)[1] and *The Health Information Protection Act* (HIPA).[2]

[11] On October 11, 2013, my office received a response from the SFSC. In that response, the SFSC appeared to indicate that it would comply with my office's recommendations. On December 2, 2013, the Applicant received an apology letter from the SFSC. In addition, on December 12, 2013, the SFSC provided my office with a new policy and procedure titled, *Posting Notices of Hearing on the FCAA Website*. The apology and new policy and procedure addressed the recommendations regarding the Notice of Hearing.

[1] *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01 (hereinafter FOIP).
[2] *The Health Information Protection Act*, S.S. 1999, c. H-0.021.

Accordingly, details regarding that portion of our investigation are not included in this Investigation Report.

[12] What I was not satisfied with was the SFSC response to my office's recommendations regarding the collection and disclosure of the Complainant's personal information and personal health information during the course of its securities investigation. The SFSC failed to provide details of when or how it intended to comply with my office's recommendations regarding the development of appropriate policies and procedures to guide its investigators to be compliant with FOIP and HIPA. Further, in an October 11, 2013 letter to our office, it stated: "…we **have yet to investigate the Complainant's allegations** due to the potential interference with the ongoing adjudication. As the adjudication is currently ongoing, we still have not investigated the allegations, **and we are not prepared to assume one way or the other concerning the veracity of the Complainant's allegations**." [emphasis added]

[13] My office responded to the SFSC on or about October 21, 2013, requesting copies of draft policies and procedures or a detailed plan outlining how and when the policies and procedures would be developed in response to the issues raised in my office's preliminary analysis within two weeks. Provided the timeline was reasonable for the development of these policies and procedures, we may have concluded the matter at that point.

[14] In its response dated November 5, 2013, the SFSC indicated it would "revise our policies to more clearly reflect that personal information and personal health information must only be collected and disclosed to the extent reasonably necessary for our purposes." However, the SFSC did not provide copies or timelines for the development of appropriate written policies and procedures to guide its investigators in achieving compliance with FOIP and HIPA as requested. It also stated, in the aforementioned letter, that it intended to retain an independent reviewer with the necessary expertise to conduct such an investigation, but had not yet done so. Due to the lack of real progress and detail on how and when it would comply with our recommendations at this late date, I proceeded to issue this Investigation Report.

II ISSUES

1. **Is the information in question "personal information" as defined by section 24(1) of *The Freedom of Information and Protection of Privacy Act* and/or "personal health information" as defined by section 2(m) of *The Health Information Protection Act*?**

2. **Did the Financial and Consumer Affairs Authority of Saskatchewan have the authority to "collect" the Complainant's personal information and personal health information in accordance with *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*?**

3. **Did the Financial and Consumer Affairs Authority of Saskatchewan have the authority to "disclose" the Complainant's personal information and personal health information in accordance with *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*?**

4. **Did the Financial and Consumer Affairs Authority of Saskatchewan have sufficient safeguards in place to reasonably protect against a similar incident from occurring again?**

III DISCUSSION OF THE ISSUES

[15] The SFSC is a "government institution" within the meaning of section 2(1)(d)(ii) of FOIP and, therefore is subject to FOIP.[3]

[16] Section 2(t)(i) of HIPA defines a "trustee" as follows:

> **2** In this Act:
> …

[3]This was also determined in Office of the Saskatchewan Information and Privacy Commissioner (hereinafter SK OIPC) Review Report F-2014-001 at [46] and [47], available at: www.oipc.sk.ca/reviews.htm.

> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> (i) a government institution;

[17] Therefore, the SFSC also qualifies as a trustee for purposes of HIPA.

[18] My authority to investigate the identified issues is found in section 33(d) of FOIP which states as follows:

> **33** The commissioner may:
> …
>
> (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.

[19] In addition, my authority to investigate is also found in sections 42(1)(c) and 52 of HIPA which state 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.
> …
>
> **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;
>
> (c) in appropriate circumstances, comment on the collection of personal health information in a manner other than directly from the individual to whom it relates;

> (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.

1. Is the information in question "personal information" as defined by section 24(1) of *The Freedom of Information and Protection of Privacy Act* and/or "personal health information" as defined by section 2(m) of *The Health Information Protection Act*?

[20] Our customary practice when dealing with a complaint under Part IV of FOIP and/or HIPA is to first determine whether there is "personal information" and/or "personal health information" involved and then to consider which of the three data transactions are engaged, i.e. collection, use and/or disclosure.

[21] The definition of personal information can be found in section 24 of FOIP and provides as follows:

> **24**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> (c) **Repealed.** 1999, c.H-0.021, s.66.
>
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
>
> (e) the home or business address, home or business telephone number or fingerprints of the individual;

(f) the personal opinions or views of the individual except where they are about another individual;

(g) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual;

(h) the views or opinions of another individual with respect to the individual;

(i) information that was obtained on a tax return or gathered for the purpose of collecting a tax;

(j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or

(k) the name of the individual where:

(i) it appears with other personal information that relates to the individual; or

(ii) the disclosure of the name itself would reveal personal information about the individual.

(1.1) "Personal information" does not include information that constitutes personal health information as defined in *The Health Information Protection Act*.

(2) **"Personal information"** does not include information that discloses:

(a) the classification, salary, discretionary benefits or employment responsibilities of an individual who is or was an officer or employee of a government institution or a member of the staff of a member of the Executive Council;

(b) the salary or benefits of a legislative secretary or a member of the Executive Council;

(c) the personal opinions or views of an individual employed by a government institution given in the course of employment, other than personal opinions or views with respect to another individual;

(d) financial or other details of a contract for personal services;

(e) details of a licence, permit or other similar discretionary benefit granted to an individual by a government institution;

(f) details of a discretionary benefit of a financial nature granted to an individual by a government institution;

(g) expenses incurred by an individual travelling at the expense of a government institution.

(3) Notwithstanding clauses (2)(e) and (f), **"personal information"** includes information that:

(a) is supplied by an individual to support an application for a discretionary benefit; and

(b) is personal information within the meaning of subsection (1).

[22] Section 2(m) of HIPA defines personal health information as follows:

2 In this Act:

…

(m) **"personal health information"** means, with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;

(ii) information with respect to any health service provided to the individual;

(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information;

[23] The Complainant provided our office with correspondence including emails that appeared to originate from different individuals, some that had apparently been interviewed by the SFSC during its investigation into the Complainant's business dealings. One email, for example, outlines the individual's version of events during the SFSC interview: "…[The SFSC employee] asked some questions that I felt were inappropriate (your health, indications that **you'd had cosmetic surgery**… [the Complainant's sister's] health…" [emphasis added]

[24] In another email to the Complainant from another individual, apparently interviewed by SFSC employees, the following was stated:

> Per our conversation yesterday here is what [name of SFSC employee] said to me:
> …
>
> - You have only one nephew named [name removed]
> - You have named [company name] numerous different names
>
> …
>
> - Asked me about if you had paid me
> - Said you canme [sic] to [name of City] for plastic surgery
> - That you have numerous people who are suing you…

[25] The SFSC's investigation involved the gathering of information of a personal nature pertaining to the Complainant. For example, the following is personal information as defined by section 24(1) of FOIP:

- How many nephews the Complainant would be personal information pursuant to sections 24(1)(a) and 24(1)(k)(i) of FOIP; and
- Whether the Complainant had paid certain individuals and was being sued – would be personal information pursuant to sections 24(1)(b), 24(1)(j) and 24(1)(k)(i) of FOIP.

[26] It also appeared that there was personal health information involved pursuant to section 2(m) of HIPA. For instance, the following would constitute the Complainant's personal health information pursuant to sections 2(m)(i) and 2(m)(ii) of HIPA:

- Whether the Complainant had plastic surgery or not and what procedures the Complainant had done.

[27] Therefore, both FOIP and HIPA are engaged in this matter as the complaint involves the Complainant's personal information and personal health information.

2. Did the Financial Consumer Affairs Authority of Saskatchewan have the authority to "collect" the Complainant's personal information and personal health information in accordance with *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*?

[28] Based on my understanding of the complaint, it appears that the SFSC's "collection" and "disclosure" of the Complainant's personal information and personal health information is at issue and not its "use" of same. Therefore, this Investigation Report will focus on the collection and disclosure transactions only.

[29] "Collection" was defined by former Saskatchewan Information and Privacy Commissioner Gary Dickson, Q.C in his Investigation Report F-2012-001, as follows:

> [17] Alberta Services' *FOIP Guidelines and Practices (2009)* elaborates further on the definition as follows:
>
> > *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.[4]

[30] Further, section 2(b) of HIPA defines "collect" as follows:

> **2** In this Act:
> …
>
> (b) **"collect"** means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means;

[31] Sections 25 and 26 of FOIP provide the rules for the collection of personal information 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.
>
> **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);

[4]SK OIPC Investigation Report F-2012-001. Former Commissioner Dickson also relied on this definition in his Investigation Report F-2013-002 at [24]. Both Reports are available at: www.oipc.sk.ca/reviews.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 a 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.

[32] Sections 23 and 24 of HIPA provide the following for the collection of personal health information:

> **23**(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
>
> (3) **Repealed.** 2003, c.25, s.13.
>
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.
>
> **24**(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.
>
> (2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.
>
> (3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.

> (4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

[33] Government institutions, including the SFSC, are obligated under section 25 of FOIP and sections 23 and 24 of HIPA to collect only data elements (personal information and personal health information) for specific lawful purposes and that each data element collected is reasonably necessary to fulfill that purpose.

[34] The Government of Saskatchewan has not produced a comprehensive guide or manual to assist government institutions with interpreting and applying FOIP. However, the Government of Alberta has developed a manual to assist its government institutions in applying Alberta's *Freedom of Information and Protection of Privacy Act* (Alberta's FOIP).[5] Alberta's FOIP is, in a number of respects, similar to Saskatchewan's FOIP. Therefore, it is often helpful to consider Alberta's manual titled, *FOIP Guidelines and Practices* (2009).[6]

[35] Section 33 of Alberta's FOIP is similar to section 25 of Saskatchewan's FOIP. Alberta's *FOIP Guidelines and Practices* (2009) states the following in regards to the "purpose" and "consistent purpose" as it relates to the collection of personal information:

> The *purpose* means the purpose for which the information was collected under section 33. A public body can use the information for that purpose. **Typical purposes include the administration of a particular program, the delivery of a service and other directly related activities.**
>
> The purpose must conform to section 33 of the Act, which limits the purposes for which information is collected…
> …
>
> A *consistent purpose* is one that **has a direct and reasonable connection to the original purpose and that is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses the information**…[7]
>
> [emphasis added]

[5]Alberta's, *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000 c. F-25.
[6]Government of Alberta, Service Alberta, *FOIP Guidelines and Practices* (2009), available at: www.servicealberta.ca/foip/resources.cfm.
[7]*Ibid.* at p. 260.

[36] The federal Privacy Commissioner has similarly stated the following: "…For a use or disclosure to be consistent, **it must have a reasonable and direct connection to the original purpose for which it was obtained or compiled**…[8] [emphasis added]

[37] In former Commissioner Dickson's Investigation Report F-2012-001, he considered the issues of collection and purpose and stated as follows:

> [18] B.C.'s *Freedom of Information and Protection of Privacy Act*'s closest equivalent to our section 25 is section 26. 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**.
>
> [emphasis added]

[38] The importance of restrictions on collection is further outlined in Investigation Report F-2012-001 as follows:

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

[8]Office of the Privacy Commissioner of Canada, *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada*, March 2011 at p. 9, available at: www.priv.gc.ca/resource/pia-efvp/index_e.asp.

> 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 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.

[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**.

[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**.

[emphasis added]

[39] In the SFSC's submission to my office, received July 11, 2012, it stated the following:

…

As identified in your letter, [the Complainant's] complaint involves…**alleged communications by SFSC investigators during the investigation into [the Complainant's] securities-related activities pursuant to section 12 of [*The Securities Act, 1988*]**…

Delaying the Review

…

As the head of the SFSC for the purposes of FOIP and HIPA, I view it as my role to ensure that staff of the SFSC comply with FOIP and HIPA. Included in this role is the obligation to investigate allegations of non-compliance by SFSC staff with those Acts. I acknowledge, subject to the specific objection to your jurisdiction set out above, that you have the authority to investigate a government institution's compliance with FOIP and HIPA. **However, in my view, it is much more beneficial to both your office and the government institution involved that the head of the government institution conduct the initial investigation of the matter. This will conserve both the government institution's and your office's limited resources by minimizing your office's involvement where complaints are clearly well-founded or defects in policies or procedures are evident. More importantly, it reinforces the principle that the primary responsibility for compliance with FOIP and HIPA rests with the head of the government institution**, and this principle is, in my view, fundamental to the object of those Acts.

As I have indicated to [the Complainant] in my correspondence to her dated June 2, 2011, February 22, 2012, April 10, 2012 and April 24, 2012, I intend to conduct a full investigation with respect to the privacy breaches she alleges occurred. However, I find myself constrained from conducting the investigation of these matters until the proceedings pursuant to [*The Securities Act, 1988*] have concluded. As Chair of the SFSC, I cannot make, or be seen to make, findings concerning matters that are live issues before a panel of Commissioners struck to make determinations pursuant to [*The Securities Act, 1988*]. Such action on my part would raise a host of troubling issues, including the potential to give rise to a reasonable apprehension of bias in the minds of the respondents in [*The Securities Act, 1988*] proceedings. I must take care not to do anything that might influence, or be perceived to influence, a panel of Commissioners charged with hearing a matter. **An approach that would see the same tribunal conducting two separate investigations and making two separate determinations concerning the same allegations is fraught with difficulties and not an approach I am willing to take.** It may have been different if [the Complainant] had not raised these very same issues as part of her defense in [*The Securities Act, 1988*] proceedings.

I am also concerned about the impact of your planned review on the witnesses to the Act proceedings. It is widely accepted that victims of securities fraud are very reluctant to report their experiences to regulators…

…

Another important consideration that should be taken into account is the risk of harm to [the Complainant] if your review is delayed. **Even if there were contraventions of FOIP and HIPA by SFSC staff as alleged by [the Complainant], she will not suffer any further harm as a result of your delaying the review**. The Hearing Panel has already addressed her concern with regard to the Notice of Hearing…Further, **SFSC investigators have been informed of [the Complainant's] complaints and have been reminded of their obligations under FOIP and HIPA.**

Another important fact is that **the delay necessary would be relatively short**. The hearing in the SCA proceedings had been scheduled to commence in mid-June however, the Court of Appeal ordered the hearing be stayed until [the Complainant's] appeal could be dealt with…**we anticipate [*The Securities Act, 1988*] proceedings will be concluded by year end.**

For these reasons, **I am requesting your office delay its review** until [*The Securities Act, 1988*] proceedings against [the Complainant] and her companies have concluded.

[emphasis added]

[40] On October 3, 2012, my office responded to the above submission via email stating as follows:

The [former] Commissioner has been clear in previous public Reports that **other proceedings do not impact our proceedings and that we would not delay** our investigation where there are others occurring. They are separate and apart from each other. We encourage you to refer to the [former] Commissioner's Investigation Report F-2009-001. Particularly, at paragraphs [12] and [13]. This has been the [former] Commissioner's view consistently…

Therefore, we will be proceeding with our investigation without delay.

One final note, you assert that "I find myself constrained by conducting the investigation of these matters until the proceedings pursuant to [*The Securities Act, 1988*] have concluded." We draw your attention to section 60 of FOIP which outlines the ability of the '**head' to delegate some of his or her responsibilities** to another individual. Perhaps the 'head' needs to delegate responsibility for this investigation to another individual at the SFSC.

…

We requested a number of things in our notification letter to you dated June 14, 2012…

…

We require these things by October 31, 2012. In preparing a response we recommend that you review the attached documents produced by our office. It will give you a sense of how the [former] Commissioner has approached situations such as this in the past. I have also attached a copy of our *Privacy Breach Guidelines* which should assist you in understanding our process and with preparing your response to our office.

[emphasis added]

[41] Despite my office's requests, the SFSC did not provide details of the incident, authority for each action (data transaction) taken, how the "data minimization" principle was applied and copies of relevant policies and procedures, regarding this portion of the Complainant's complaint. The SFSC stated the following in its submission received by my office November 27, 2012:

- *Details of the incident (who, what, where, when and how) for each of the allegations made by the complainant outlined in our notification letter dated June 14, 2012 (a) through (g). Ensure that you provide the authority under FOIP for each action taken in each of the allegations (a) through (g);*

…

With regard to [the Complainant's] other allegations outlined in your June 14, 2012 notification letter, **details of the incidents for each of the allegations will be included in the report of the independent reviewer I retain** to conduct the review of the Securities Division's practices.

[emphasis added]

[42] Although it indicated it would move forward with its investigation, no clear timeline was provided by the SFSC as to when it would be conducting and concluding its internal investigation. As stated earlier, my office advised the SFSC via email on May 7, 2013, that it needed to provide what was requested regarding this issue by May 10, 2013.

[43] On May 10, 2013, the SFSC sent the following in an email to my office:

As to our position with respect to the allegations made by [the Complainant] concerning the conduct of FCAA investigators, we would reiterate all of our prior submissions with respect to this issue. **I can also advise that the Head intended, and still intends, to conduct a full, formal investigation into the allegations after**

> **the Hearing Panel makes a decision in the proceedings against [the Complainant]** and her companies, which may include findings with respect to these very same allegations. **However, we are not prepared to do that until the proceedings against [the Complainant] have concluded**, as there is a very real possibility of interference with and disruption to the quasi-judicial proceedings currently underway against [the Complainant] if the FCAA were to conduct another simultaneous proceeding with respect to some of the exact same issues. Interfering with the proceedings currently underway is not in the interest of [the Complainant] or the public.
>
> [emphasis added]

[44] Section 4(b) of Alberta's FOIP excludes from its scope a "personal note, communication or draft decision created by or for a person who is acting in a judicial or quasi-judicial capacity including any authority designated by the Lieutenant Governor in Council to which the Administrative Procedures Act applies". The effect of this exclusion is to treat certain records of an administrative tribunal in a way similar to court records by excluding them from the scope of that province's FOIP Act.

[45] The Legislative Assembly of Saskatchewan, however, evidently made the decision to treat any administrative tribunal and the records in their possession, or under their control, no differently than the records of any other government institution.

[46] The SFSC indicated in its submission, received July 11, 2012 that the communications by SFSC investigators occurred during an investigation pursuant to section 12 of *The Securities Act, 1988*.[9] Section 12 of *The Securities Act, 1988* states as follows:

> **12**(1) Where, on a statement made under oath, it appears probable to the Commission that any person or company has:
>
> (a) contravened any provision of this Act, the regulations or a decision of the Commission;
>
> (b) committed an offence under the *Criminal Code* in connection with a transaction relating to securities or exchange contracts;
>
> (c) committed any act that may be unfair, oppressive, injurious, inequitable or improper to or discriminatory against:

[9] *The Securities Act, 1988,* S.S. 1988-89, c. S-42.2.

(i) any holder, prospective holder, purchaser or prospective purchaser of any securities of that person or company;

(ii) any purchaser or prospective purchaser of an exchange contract; or

(iii) any creditor, prospective creditor of that person or company, or other person or company, otherwise beneficially interested in that person or company;

(d) committed any act whereby an unfair advantage may be secured by that person or company over any other person or company;

the Commission may, by order, appoint a person to make those investigations that it considers expedient for the due administration of this Act and the regulations.

(2) The Commission may, by order, appoint a person to make any investigation that it considers necessary respecting all or any of the following:

(a) any matter relating to the administration of this Act and the regulations;

(b) any matter relating to trading in securities or exchange contracts;

(c) any matter relating to trading in securities or exchange contracts in any other jurisdiction; or

(d) any matter relating to the administration of the laws of another jurisdiction that govern trading in securities or exchange contracts.

(3) In an order made pursuant to subsection (1) or (2), the Commission shall prescribe the scope of the investigation that is to be carried out pursuant to the order.

(4) **For the purposes of an investigation ordered pursuant to this section, the person appointed to make the investigation may, with respect to the person who or company that is the subject of the investigation, investigate, inquire into and examine**:

(a) the affairs of that person or company;

(b) any books, papers, documents, records, correspondence, communications, negotiations, transactions, investigations, loans, borrowings and payments to, by, on behalf of or in relation to or connected with that person or company;

(c) the property, assets or things owned, acquired or alienated in whole or in part by the person or company or any person or company acting on behalf of or as agent for that person or company;

> **(d) the assets at any time held by, the liabilities, debts, undertakings and obligations at any time existing and the financial or other conditions at any time prevailing with respect to that person or company; and**
>
> **(e) the relationship that may at any time exist or have existed between that person or company and any other person or company by reason of:**
>
> **(i) investments;**
>
> **(ii) commissions promised, secured or paid;**
>
> **(iii) interests held or acquired;**
>
> **(iv) the loaning or borrowing of money, securities or other property;**
>
> **(v) the transfer, negotiation or holding of securities or exchange contracts;**
>
> **(vi) interlocking directorates;**
>
> **(vii) common control;**
>
> **(viii) undue influence or control; or**
>
> **(ix) any other relationship**.
>
> (4.1) For the purposes of an investigation pursuant to this section, a person appointed to make the investigation may examine any documents, records or other things mentioned in subsection (4), whether they are in the possession or control of:
>
> (a) the person who or company that is the subject of the investigation; or
>
> (b) another person or company.
>
> …
>
> [emphasis added]

[47] The SFSC's October 11, 2013 letter to my office also spoke generally as to what it would require in the course of an investigation and under what authority as follows:

> In fact, it is subsections 12 (1) and (2) that determine the scope of FCAA's authority to investigate…
>
> …
>
> Subsections 12(1) and (2) determine the types of matters that can be investigated and in doing so, establish the outer parameters of relevance in terms of any investigation. **Within these broad parameters, the nature of each particular investigation will**

> **determine the precise boundaries of relevance for that investigation**. Subsection 12(4) speaks to the types of documents, materials or things that can be inquired into and examined for the purposes of investigating a matter within the purview of subsections 12(1) and (2). Clause 12(4) is itself extremely broad and would allow FCAA investigators to investigate or inquire into just about any factual matter relating to a person or company, **provided the factual matter was relevant** for the purposes of the particular investigation, which in turn must fall within the parameters set out in subsection 12(1) or (2).
>
> [emphasis added]

[48] The above is too generalized to be of any particular assistance in determining whether or not SFSC had *specific* authority to collect the personal information and personal health information of the Complainant in this particular case. Further, above the SFSC appears to acknowledge that relevancy is a factor but at no time during my office's investigation did it explain how each data element was relevant, even though we afforded it many opportunities to provide further explanation.

[49] In former Commissioner Dickson's Investigation Report LA-2010-001, he discussed the burden of proof requirement, as it relates to privacy breach investigations, as follows:

> [26] The statute does not define burden of proof in a breach of privacy investigation in the context of an impugned disclosure. **In these circumstances, I find that the burden must be borne by the local authority as only the local authority would have intimate knowledge of the circumstances surrounding the disclosure**. That burden of proof is assessed on the basis of a balance of probabilities.[10]
>
> [emphasis added]

[50] This decision making on a balance of probabilities is best described in my office's resource, *Helpful Tips: OIPC Guidelines for Public Bodies/Trustees in Preparing for a Review*. In each case before me, I must decide which evidence to rely on and how much weight to give that evidence:

> …To be successful, the party will be required to prove certain facts and issues according to a particular standard of proof. The standard of proof is "on a balance of probabilities" or "on a preponderance of evidence." A party will have proven its case on a "balance of probabilities" if the Commissioner is able to say: "*I think it more*

[10]SK OIPC Investigation Report LA-2010-001 at [26], available at: www.oipc.sk.ca/reviews.htm.

> *likely, or more probable, than not.*" This means that the Commissioner is convinced by the persuasiveness and/or accuracy of one party's evidence over the others.[11]

[51] The SFSC has not demonstrated, to my satisfaction, how each data element was necessary such that the operation of the program or activity [its investigation] could not have been viable without it.

[52] Therefore, I find that the SFSC failed to demonstrate that it had authority to collect the Complainant's personal information and personal health information.

3. Did the Financial and Consumer Affairs Authority of Saskatchewan have the authority to "disclose" the Complainant's personal information and personal health information in accordance with *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*?

[53] In former Commissioner Dickson's Investigation Report F-2007-001, he defined "disclosure" as follows:

> [179] Disclosure is not defined by FOIP. We have however defined disclosure as follows:
>
> > **Disclosure is the sharing of personal information with a separate entity**, not a division or branch of the public body or trustee in possession or control of that record/information.[12]
>
> [emphasis added]

[54] Disclosure appears to have occurred, in this case, when the SFSC provided details of the Complainants circumstances to third parties during interviews and information gathering as part of its securities investigation.

---

[11]SK OIPC Resource, *Helpful Tips: OIPC Guidelines for Public Bodies/Trustees in Preparing for a Review*, at p. 9, available at: www.oipc.sk.ca/resources.htm.

[12]SK OIPC Investigation Report F-2007-001, available at: www.oipc.sk.ca/reviews.htm. Also discussed in SK OIPC Investigation Reports F-2007-001 at [179], F-2009-001 at [78], F-2012-002 at [36], F-2012-005 at footnote 31, F-2013-002 at footnote 12, LA-2013-001 at [26] and H-2013-001 at [36], available at: www.oipc.sk.ca/reviews.htm.

[55] Section 29 of FOIP provides for the disclosure of personal information with consent of the subject individual or in limited circumstances without the consent. Section 29(1) of FOIP provides as follow:

> **29**(1) No government institution shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 30.

[56] There is no evidence that the Complainant offered her consent to authorize the SFSC to disclose her personal information to third parties as part of its investigation. Therefore, the SFSC would have to justify any disclosure by means of one of the subsections enumerated at section 29(2) of FOIP. Section 29(2) of FOIP provides as follows:

> **29**(2) Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed:
>
> (a) for the purpose for which the information was obtained or compiled by the government institution or for a use that is consistent with that purpose;
>
> (b) for the purpose of complying with:
>
> (i) a subpoena or warrant issued or order made by a court, person or body that has the authority to compel the production of information; or
>
> (ii) rules of court that relate to the production of information;
>
> (c) to the Attorney General for Saskatchewan or to his or her agent or legal counsel for use in providing legal services;
>
> (d) to legal counsel for a government institution for use in providing legal services to the government institution;
>
> (e) for the purpose of enforcing any legal right that the Government of Saskatchewan or a government institution has against any individual;
>
> (f) for the purpose of locating an individual in order to:
>
> (i) collect a debt owing to Her Majesty in right of Saskatchewan or to a government institution by that individual; or
>
> (ii) make a payment owing to that individual by Her Majesty in right of Saskatchewan or by a government institution;

(g) to a prescribed law enforcement agency or a prescribed investigative body:

(i) on the request of the law enforcement agency or investigative body;

(ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and

(iii) if any prescribed requirements are met;

(h) pursuant to an agreement or arrangement between the Government of Saskatchewan or a government institution and:

(i) the Government of Canada or its agencies, Crown corporations or other institutions;

(ii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iii) the government of a foreign jurisdiction or its institutions;

(iv) an international organization of states or its institutions; or

(v) a local authority as defined in the regulations;

for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(h.1) for any purpose related to the detection, investigation or prevention of an act or omission that might constitute a terrorist activity as defined in the *Criminal Code*, to:

(i) the Government of Canada or its agencies, Crown corporations or other institutions;

(ii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iii) the government of a foreign jurisdiction or its institutions;

(iv) an international organization of states or its institutions; or

(v) a local authority as defined in the regulations;

(i) for the purpose of complying with:

(i) an Act or a regulation;

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

(iii) a treaty, agreement or arrangement made pursuant to an Act or an Act of the Parliament of Canada;

(j) where disclosure is by a law enforcement agency:

(i) to a law enforcement agency in Canada; or

(ii) to a law enforcement agency in a foreign country;

pursuant to an arrangement, a written agreement or treaty or to legislative authority;

(k) to any person or body for research or statistical purposes if the head:

(i) is satisfied that the purpose for which the information is to be disclosed is not contrary to the public interest and cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates; and

(ii) obtains from the person or body a written agreement not to make a subsequent disclosure of the information in a form that could reasonably be expected to identify the individual to whom it relates;

(l) for the purpose of:

(i) management;

(ii) audit; or

(iii) administration of personnel;

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

(m) where necessary to protect the mental or physical health or safety of any individual;

(n) in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased;

(o) for any purpose where, in the opinion of the head:

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or

> (ii) disclosure would clearly benefit the individual to whom the information relates;
>
> (p) where the information is publicly available;
>
> (q) to the office of the Provincial Auditor, or to any other prescribed person or body, for audit purposes;
>
> (r) to the Ombudsman;
>
> (s) to the commissioner;
>
> (t) for any purpose in accordance with any Act or regulation that authorizes disclosure; or
>
> (u) as prescribed in the regulations.

[57] For the disclosure of personal health information without consent, the SFSC would have to justify its disclosure by means of one of the subsections enumerated at section 27 of HIPA.

[58] Section 27 of HIPA provides as follows:

> **27**(1) A trustee shall not disclose personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section, section 28 or section 29.
>
> (2) A subject individual is deemed to consent to the disclosure of personal health information:
>
> (a) for the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose;
>
> (b) for the purpose of arranging, assessing the need for, providing, continuing, or supporting the provision of, a service requested or required by the subject individual; or
>
> (c) to the subject individual's next of kin or someone with whom the subject individual has a close personal relationship if:
>
> (i) the disclosure relates to health services currently being provided to the subject individual; and

(ii) the subject individual has not expressed a contrary intention to a disclosure of that type.

(3) A trustee shall not disclose personal health information on the basis of a consent pursuant to subsection (2) unless:

(a) in the case of a trustee other than a health professional, the trustee has established policies and procedures to restrict the disclosure of personal health information to those persons who require the information to carry out a purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act; or

(b) in the case of a trustee who is a health professional, the trustee makes the disclosure in accordance with the ethical practices of the trustee's profession.

(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

(a) where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person;

(b) where, in the opinion of the trustee, disclosure is necessary for monitoring, preventing or revealing fraudulent, abusive or dangerous use of publicly funded health services;

(c) where the disclosure is being made to a trustee that is the successor of the trustee that has custody or control of the information, if the trustee makes a reasonable attempt to inform the subject individuals of the disclosure;

(d) to a person who, pursuant to *The Health Care Directives and Substitute Health Care Decision Makers Act*, is entitled to make a health care decision, as defined in that Act, on behalf of the subject individual, where the personal health information is required to make a health care decision with respect to that individual;

(e) if the subject individual is deceased:

(i) where the disclosure is being made to the personal representative of the subject individual for a purpose related to the administration of the subject individual's estate; or

(ii) where the information relates to circumstances surrounding the death of the subject individual or services recently received by the subject individual, and the disclosure:

(A) is made to a member of the subject individual's immediate family or to anyone else with whom the subject individual had a close personal relationship; and

(B) is made in accordance with established policies and procedures of the trustee, or where the trustee is a health professional, made in accordance with the ethical practices of that profession;

(f) where the disclosure is being made in accordance with section 22 to another trustee or an information management service provider that is a designated archive;

(g) where the disclosure is being made to a standards or quality of care committee established by one or more trustees to study or evaluate health services practice in a health services facility, health region or other health service area that is the responsibility of the trustee, if the committee:

(i) uses the information only for the purpose for which it was disclosed;

(ii) does not make a further disclosure of the information; and

(iii) takes reasonable steps to preserve the confidentiality of the information;

(h) subject to subsection (5), where the disclosure is being made to a health professional body or a prescribed professional body that requires the information for the purposes of carrying out its duties pursuant to an Act with respect to regulating the profession;

(i) where the disclosure is being made for the purpose of commencing or conducting a proceeding before a court or tribunal or for the purpose of complying with:

(i) an order or demand made or subpoena or warrant issued by a court, person or body that has the authority to compel the production of information; or

(ii) rules of court that relate to the production of information;

(j) subject to subsection (6), where the disclosure is being made for the provision of health or social services to the subject individual, if, in the opinion of the trustee, disclosure of the personal health information will clearly benefit the health or well-being of the subject individual, but only where it is not reasonably practicable to obtain consent;

(k) where the disclosure is being made for the purpose of:

(i) obtaining payment for the provision of services to the subject individual; or

(ii) planning, delivering, evaluating or monitoring a program of the trustee;

(l) where the disclosure is permitted pursuant to any Act or regulation;

(m) where the disclosure is being made to the trustee's legal counsel for the purpose of providing legal services to the trustee;

(n) in the case of a trustee who controls the operation of a pharmacy as defined in *The Pharmacy Act, 1996*, a physician, a dentist or the minister, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to *The Medical Profession Act, 1981* and approved by the minister;

(o) in the case of a trustee who controls the operation of a pharmacy as defined in *The Pharmacy Act, 1996*, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to *The Pharmacy Act, 1996* and approved by the minister;

(p) in prescribed circumstances.

[59] As noted earlier, the SFSC offered no specific authority to my office to support its disclosure of any of the Complainant's personal information or personal health information pursuant to FOIP or HIPA in the course of its investigation. It also repeatedly indicated it would not provide any details of the events until its own independent investigator completed an internal investigation at some unknown future date.

[60] With respect, my office has been tasked with the mandate to oversee government institution's (such as the SFSC's) compliance with FOIP and HIPA. The scheme of both FOIP and HIPA is about timely resolution of complaints and the SFSC's response is simply not consistent to this extent. Timely investigations often result in changes to practice and prevention of additional privacy breaches. Until the SFSC completes its independent investigation, at some unknown future date, additional privacy breaches could be occurring involving other citizens. This is unacceptable.

[61] The burden of proof in demonstrating its authority to disclose under FOIP and HIPA lies with the SFSC. It could not have undertaken the investigation in question without

sharing at least some information about the Complainant with third parties, which is evident.

[62] Therefore, the SFSC has failed to demonstrate that it had authority under FOIP and HIPA to disclose the Complainant's personal information and personal health information to third parties.

[63] Even if the SFSC had demonstrated it had general authority to collect and disclose under FOIP and HIPA, in this case, the 'data minimization' principle must still be considered and abided by when collecting, using and/or disclosing personal information and/or personal health information. This principle is explicit in HIPA and implicit in FOIP. Former Commissioner Dickson discussed this in his Investigation Report F-2012-005, as follows:

> [66] These two principles underlie section 28 of FOIP and section 23 and 26 of HIPA. The need-to-know principle means that SGI should collect, use and disclose only on a need-to-know basis. As well, data minimization means that SGI should collect, use or disclose the least amount of identifying information necessary for the purpose.[13]

[64] My office requested the SFSC provide representation to my office on how it had taken the principle of data minimization into consideration when the information in question was disclosed by its investigators. In its letter dated November 23, 2012, the SFSC stated: "… the report of the independent reviewer I retain to conduct the review of the Securities Division's practices will address our compliance with the 'data minimization principle'." No such report, however, was provided to my office in the course of this investigation.

[65] Therefore, the SFSC also has failed to demonstrate that it abided by the data minimization principle in this case.

[13]SK OIPC Investigation Report F-2012-005, available at: www.oipc.sk.ca/reviews.htm. Also referenced in SK OIPC Investigation Reports F-2007-001 at [209] to [210], F-2009-001 at [92], H-2010-001 at [61], LA-2010-001 at [47], F-2012-005 at [65] to [68], and H-2013-001 at [54] to [56], available at: www.oipc.sk.ca/reviews.htm.

4. Did the Financial and Consumer Affairs Authority of Saskatchewan have sufficient safeguards in place to reasonably protect against a similar incident from occurring again?

[66] It is common that my office reviews policies and procedures of government institutions (along with local authorities and trustees) during compliance investigations. I am of the opinion that compliance with FOIP and HIPA would be difficult, if not impossible, without appropriate written policies and procedures to guide a government institution's employees in the proper handling and safeguarding of personal information and personal health information.

[67] In fact, section 16 of HIPA requires trustees to have adequate written policies and procedures in place to sufficiently protect personal health information. Section 16 of HIPA states 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.
>
> [emphasis added]

[68] In former Commissioner Dickson's Investigation Report LA-2013-001, he discussed the need for written policies and procedures to safeguard personal information and personal health information:

> [54] I have discussed in Investigation Report F-2007-001 what is required of a trustee in order to comply with section 16 of HIPA. This includes having written policies and procedures:
>
> > [48] As of this date, there have been no regulations enacted under HIPA that are relevant to the standards required of a health information trustee such as WCB for *administrative, technical or physical safeguards"*. Our office has concluded in past Reports that section 16 requires that a trustee establish written policies and procedures.
>
> …
>
> [56] LA FOIP does not contain the same explicit language as that in section 16 of HIPA; it is my view nonetheless that it is implicit that all local authorities must also have adequate safeguards in place to protect personal information in its possession or control.[14] Therefore, I would expect that to be compliant with Part IV of LA FOIP, a local authority would have written policies and procedures for its employees.
>
> [57] **Without written policies and procedures a local authority and trustee has not taken reasonable steps to safeguard personal information or personal health information in its possession/custody and control**.
>
> …
>
> [59] Providence is expected to have written policies and procedures to safeguard and advise its employees on the proper handling of employee and patient personal information and personal health information. **To not have them is to risk further privacy breaches as a result of misinformed staff or other preventable circumstances.**
>
> [emphasis added]

[69] I am of the same view.

[70] The SFSC provided the following to my office with regards to its policies and procedures related to this issue in its submission, received by my office on November 27, 2012:

> - *[OIPC Requested] Copies of policies/procedures that apply to this situation;*
>
> …
>
> …we have written policies on the use and disclosure of personal information in general, however, **these policies do not speak to the use and disclosure of personal information and personal health information by investigators** in furtherance of investigations pursuant to *The Securities Act, 1988*. **I anticipate that the final**

[14]Supra note 4 at [89], former Commissioner Dickson noted that this is an expectation of government institutions subject to FOIP.

> **report of the independent reviewer I retain to conduct the review of the Securities Division's practices will provide the foundation from which a written policy on this discrete issue can be developed**. Please note that the Authority takes compliance with its privacy obligations very seriously and is very diligent in ensuring staff is made aware of the importance of complying with FOIP.
>
> [emphasis added]

[71] As noted above, the SFSC did not have specific written policies or procedures in place to guide its investigators with the proper handling and safeguarding of personal information and personal health information during its investigation of the Complainant's business dealings. This constitutes a failure to have adequate safeguards in place to sufficiently protect personal information and personal health information as required under FOIP and HIPA. FOIP has been in force since 1992. HIPA has been in force since 2003. No explanation has been offered by the SFSC as to why appropriate policies and procedures are not already in place.

[72] My office provided the SFSC with its preliminary analysis, findings and recommendations on or about September 10, 2013, in an attempt to informally resolve the matter. My office recommended that the SFSC develop and/or update its policies and procedures to guide its investigators to be compliant with FOIP and HIPA.

[73] In its October 11, 2013 letter, the SFSC indicated it would "prepare more specific policies and procedures for FCAA investigators aimed at ensuring compliance with the privacy provisions under *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*, to the extent those Acts apply." However, no details or timelines for development or implementation of this work was provided to my office. After subsequently requesting that the SFSC either provide copies of the changed draft policies and procedures or a detailed plan outlining how the policies and procedures would be reviewed and revised within two weeks, it responded as follows: "You asked that we provide this material or information to you within two weeks. We could not meet the timeline you set."

[74] In its letter to my office dated November 5, 2013, the SFSC did advise however that its "staff investigators have been reminded of their responsibility to only collect and disclose personal information or personal health information where reasonably necessary for the purposes of our investigation." This does not go far enough in my view. Leaving aside this complaint, a policy and procedure should have already been in place prior to the current complaint arising to guide investigators in adhering to the data minimization principle. Regardless of what outcome the SFSC's own investigation produces, this is a requirement of FOIP and HIPA.

[75] Therefore, I find that the SFSC has inadequate safeguards to sufficiently protect personal information and personal health information assembled and shared in the course of its securities investigations.

IV FINDINGS

[76] I find that the Financial and Consumer Affairs Authority of Saskatchewan has failed to demonstrate that it had authority to collect the Complainant's personal information and personal health information under *The Freedom of Information and Protection of Privacy Act* or *The Health Information Protection Act*.

[77] I find that the Financial and Consumer Affairs Authority of Saskatchewan has failed to demonstrate that it had authority under *The Freedom of Information and Protection of Privacy Act* or *The Health Information Protection Act* to disclose the Complainant's personal information and personal health information to third parties.

[78] I find that the Financial and Consumer Affairs Authority of Saskatchewan has failed to demonstrate that it abided by the data minimization principle when it collected and disclosed the Complainant's personal information and personal health information to and from third parties who did not appear to have a demonstrable need-to-know.

[79] I find that the Financial and Consumer Affairs Authority of Saskatchewan has insufficient safeguards to protect personal information and personal health information it

assembled and shared in the course of its securities investigations due to its lack of written policies and procedures related to *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*.

V RECOMMENDATION

[80] I recommend that the Financial and Consumer Affairs Authority of Saskatchewan promptly develop appropriate written policies and procedures to guide its employees who are responsible for securities investigations to ensure compliance with the privacy provisions under *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act.*

Dated at Regina, in the Province of Saskatchewan, this 28th day of March, 2014.

DIANE ALDRIDGE
Acting Saskatchewan Information and Privacy Commissioner