ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2013-06

February 15, 2013

SERVICE ALBERTA

Case File Number F6167

Office URL: www.oipc.ab.ca

Summary: The Complainant made a complaint to the Commissioner that an employee of Sentinel Registry Ltd. (Sentinel Registry) had disclosed the Complainant's address to an individual who had then gone to the address with the intention of harassing or confronting the Complainant. In a preliminary decision, the Adjudicator determined that the *Freedom of Information and Protection of Privacy* Act applied to the complaint.

The Adjudicator determined that the Complainant's personal information had been disclosed by a registry employee without authorization, and contrary to Service Alberta's policies and procedures. She therefore determined that Service Alberta could not be said to have disclosed the Complainant's personal information.

The Adjudicator then considered whether Service Alberta had taken reasonable measures to protect the personal information of the Complainant in the MOVES database from unauthorized disclosure. The Adjudicator determined that while Service Alberta took measures to ensure that Sentinel Registry employees understood its policies and requirements, it had not taken adequate measures to monitor the manner in which Sentinel Registry employees accessed personal information from the MOVES database. She ordered the Public Body to take proactive measures to monitor Sentinel Registry employees' access of the MOVES database.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 4, 38, 40, 72; *Personal Information Protection Act*, S.A. 2003, c P-6.5 ss. 4, 34, 49

Authorities Cited: AB: Orders F2006-033; P2012-02; F2012-28; Decision F2012-D-02/ P2012-D-01/ M2012-D-01,

I. BACKGROUND

[para 1] On February 1, 2010, the Complainant made a complaint to the Commissioner that Sentinel Registry Ltd. (Sentinel Registry) had disclosed his address information and a photograph of him to an unnamed individual, who had then gone to his house and confronted him.

[para 2] The Commissioner authorized a portfolio officer to investigate and to attempt to mediate the Complainant's complaint under section 49 of the *Personal Information Protection Act* (PIPA). As mediation was unsuccessful, the matter was scheduled for a written inquiry.

[para 3] On reviewing the complaint, I identified the following preliminary issue:

> **Which Act applies to the Complainant's complaint, the *Freedom of Information and Protection of Privacy Act* or the *Personal Information Protection Act*?**

[para 4] I identified the foregoing issue because the information that was the subject of the complaint had been disclosed to the unnamed individual from a registry maintained by Service Alberta under the authority of Schedule 12 of the *Government Organization Act*. Under section 4(2) of PIPA, if information is in the control or custody of a public body, such as Service Alberta, PIPA does not apply to that information.

[para 5] I received submissions on this issue from the Complainant, Service Alberta, and Sentinel Registries. Having reviewed their submissions, I identified the following issue:

> **What legislation, if any, applies to the Complainant's complaint?**

[para 6] On April 24, 2012, I issued Decision F2012-D-02/ P2012-D-01/ M2012-D-01. I found that the *Freedom of Information and Protection of Privacy Act* applies to the Applicant's complaint, given that his complaint is one that his personal information was disclosed from the MOVES database. I determined that I have jurisdiction to decide the following issues at an inquiry:

1. **Did Service Alberta disclose the Complainant's personal information contrary to Part 2 of the FOIP Act?**

2. **Did Service Alberta make reasonable security arrangements to protect the Complainant's personal information against unauthorized disclosure, as required by section 38 of the Act?**

[para 7] The parties exchanged submissions. Sentinel Registries stated that it had provided its comments and supporting evidence to Service Alberta for the inquiry, and agreed with Service Alberta's submissions.

II. ISSUES

Issue A: Did Service Alberta disclose the Complainant's personal information contrary to Part 2 of the FOIP Act?

Issue B: Did Service Alberta make reasonable security arrangements to protect the Complainant's personal information against unauthorized disclosure, as required by section 38 of the Act?

III. DISCUSSION OF ISSUES

Issue A: Did Service Alberta disclose the Complainant's personal information contrary to Part 2 of the FOIP Act?

[para 8] The Public Body states:

> As a result of the investigation of the Complainant's concerns, SIU determined that despite and contrary to the terms of the registry agent agreement, the various mandated policies and procedures governing the disclosure of motor vehicle information (discussed in detail above), the CCE [Code of Conduct and Ethics] required of each of Sentinel's personnel, AMVIR, and the training provided to its registry agent personnel by Sentinel, this particular disclosure was made inappropriately by one of Sentinel's personnel.
>
> Section 40 of FOIP sets out a long list of categories wherein a public body may disclose personal information. Service Alberta's review of that section as it relates to the facts that are the subject of this Inquiry have [led] them to the conclusion that this particular disclosure would not have been authorized pursuant to section 40. Included in that section is subsection (f) affording a public body discretion to disclose personal information "for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure". AMVIR regulates the disclosure of personal driving and motor vehicle information as that term is defined in the *Traffic Safety Act*, such as the information stored in MOVES through section 2(1). The Registrar may only disclose such MOVES information for those purposes set out in section 2(1) (some of which are analogous to FOIP Section 40 and some are unique to AMVIR).
>
> Service Alberta, as a result of its investigation of the circumstances of the disclosure of the Complainant's address, has determined that the member of Sentinel's personnel responsible for the disclosure disclosed the Complainant's address without a valid purpose, without any proper supporting documentation as required in any of the legitimate situations described above, and without any authority to do so (whether under FOIP or AMVIR).

[para 9] Service Alberta concedes that the Complainant's personal information was disclosed for purposes not authorized by section 40 of the FOIP Act. However, it takes

the position that the disclosure was made by a registry employee without authorization and contrary to its policies and procedures.

[para 10] For the reasons discussed below, I agree with Service Alberta that if the disclosure was made contrary to its policies and procedures, and the policies and procedures were known to the employee, then the disclosure would be attributable to the actions of the rogue employee, and not Service Alberta.

[para 11] I will therefore consider whether the information management policies and procedures put in place by Service Alberta require compliance by registry employees, and, if they do, consider whether the disclosure was made in compliance with the policies and procedures, or was made without authority.

[para 12] Until I issued Decision F2012-D-02/ P2012-D-01/ M2012-D-01, the Public Body and this office took the view that the FOIP Act does not apply to the use and disclosure of personal information from the MOVES database. A document prepared by this office jointly with the Auditor General in 1998 entitled "OIPC Alberta Registries Privacy Audit" (the Audit Report) provides the basis for this position.

[para 13] The authors of the Audit Report concluded that the collection of personal information by registries is subject to Part 2 of the FOIP Act. However, section 4(1)(l)(ii), (quoted below) (then section 4(1)(h)(ii)), was interpreted as "[implying] that the use, disclosure and protection of information in the Motor Vehicles Registry is not subject to the provisions of the Act." The Audit Report recommended that personal information contained in the MOVES database be made subject to Part 2 of the FOIP Act for the following reasons:

- Albertans may reasonably expect that the protection of privacy provisions in Part 2 of the Act should apply not only to the collection of their personal information but also to the use, disclosure, and protection of that information.
- Albertans have an expectation that Alberta Registries is safeguarding their privacy and not using the personal information in its custody for revenue generation.
- Alberta Registries has been entrusted with the personal information of Albertans and therefore has a responsibility to ensure that personal information in its custody is safeguarded from unauthorized access, use and disclosure.
- Alberta Registries has the responsibility to ensure that it manages the risk of the potential misuse of personal information contained in the Motor Vehicles Registry.

[para 14] Section 4(1)(l) states:

> *4(1) This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following:*
>
> *(l) a record made from information*
>
> *(i) in the Personal Property Registry,*

> *(ii) in the office of the Registrar of Motor Vehicle Services,*
>
> *(iii) in the office of the Registrar of Corporations,*
>
> *(iv) in the office of the Registrar of Companies,*
>
> *(v) in a Land Titles Office,*
>
> *(vi) in the office of the Director, or of a district registrar, as defined in the Vital Statistics Act, or*
>
> *(vii) in a registry operated by a public body if that registry is authorized or recognized by an enactment and public access to the registry is normally permitted;*

[para 15] The interpretation set out in Decision F2012-D-02/ P2012-D-01/ M2012-D-01 differs to that in the Audit Report, in that I found that information in the MOVES database is subject to Part 2 of the FOIP Act, and that the exception created by section 4(1)(l)(ii) applies to records that are made from this information, such as records made under the authority of the Access to Motor Vehicle Information Regulation (AMVIR). As a result, I found that the use and disclosure of personal information in the MOVES database is subject to Part 2 of the FOIP Act. In my view, section 4(1)(l) is not intended to exclude information from Part 2 of the FOIP Act, but to exclude the right of access to records made from this kind of information, such as a driver's abstract. In addition, it serves to exclude *records* made from information in the MOVES database from the scope of Part 2 of the FOIP Act, presumably because it would not be practically possible to monitor or limit the use to which clients may put records, such as driver's abstracts obtained under AMVIR.

[para 16] Section 6 of the FOIP Act states in part:

> *6(1) An applicant has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.*
>
> *(2) The right of access to a record does not extend to information excepted from disclosure under Division 2 of this Part, but if that information can reasonably be severed from a record, an applicant has a right of access to the remainder of the record.*
>
> *…*

[para 17] Under section 6, the right of access extends to records. In contrast, the provisions of Part 2 of the FOIP Act apply to *personal information* in the custody or control of a public body. As a result, section 4(1)(l)(ii) may be interpreted as removing records made from information in the MOVES database from the scope of Part 1

Division 1 of the FOIP Act, but not as removing the information in the database from the scope of Part 2 of the FOIP Act.

[para 18] The Audit Report also contained recommendations to ensure the security of personal information in the MOVES database.

> It is recommended that Alberta Registries adopt fair information practices and disclose personal information only:
>
> - if the disclosure is consistent with the original purpose for which the information was collected; or
> - if there is legislative authority for disclosure; or
> - if informed consent has been obtained; or
> - if disclosure is for a purpose consistent with the provisions of sections 38, 40 and 41 of the *Freedom of Information and Protection of Privacy Act*, which specifies the circumstances under which a public body may disclose personal information.

[para 19] Service Alberta adopted this recommendation and made policies ensuring compliance with the use and disclosure provisions contained in Part 2 of the FOIP Act.

[para 20] Service Alberta's evidence establishes that it requires registry employees to sign an acknowledgement of the Code of Conduct and Ethics for registry agent personnel. Policy C.1 of this Code requires that all registry employees collect, use, and disclose personal information in accordance with the FOIP Act. Therefore, even though Service Alberta was originally of the opinion that the FOIP Act did not apply to the use and disclosure of personal information from the MOVES database, it has tried to ensure compliance with Part 2 of the FOIP Act through contractual provisions.

[para 21] It is unclear whether the version of the Code of Conduct was provided to me was in force at the time of the circumstances giving rise to the Complainant's complaint. The Code of Conduct indicates that it was revised November 30, 2011, and it is possible that some of the provisions dealing with the use and disclosure of personal information were amended subsequent to the disclosure giving rise to this inquiry. However, it is clear from the Code of Conduct – Staff Acknowledgement form, which was signed by the employee who disclosed the information and was provided for my review by Sentinel Registries and Service Alberta, that registry employees are required to "respect the policies and restrictions regarding the release of any and all personal information" and to "understand that the use and disclosure of personal information for purposes other than those authorized for Registries operations is strictly prohibited". I conclude from the contents of these forms that at the time the Complainant's information was disclosed by the employee:

1. Service Alberta created rules regarding the use and disclosure of personal information by registry employees in order to ensure compliance with Part 2 of the FOIP Act.
2. Service Alberta required registries to have registry employees read and acknowledge these rules annually to ensure compliance with them.

3. Using and disclosing personal information in situations where an employee is not authorized by Registries operations to do so was strictly prohibited.

[para 22] From the evidence provided to me by Service Alberta and Sentinel Registry, I conclude that disclosing personal information from the MOVES database to a friend for the friend's personal use is an example of a disclosure of personal information that was not authorized for Registries operations, and was therefore a use and disclosure that was prohibited by Service Alberta. I therefore also conclude that the employee's action of gaining access to and disclosing the Complainant's personal information was not authorized or directed by Service Alberta. Rather, the disclosure of the personal information in this case was done by an employee without authorization and contrary to the terms of the employee's employment.

[para 23] As the disclosure of the Complainant's personal information was made without the authority of Service Alberta and contrary to its policies, I find that the disclosure cannot be said to have been made by Service Alberta. I therefore find that Service Alberta did not disclose the Complainant's personal information contrary to Part 2 of the FOIP Act.

[para 24] I note that in previous orders of this office, for example, Order F2006-033 and F2012-28, the actions of employees who accessed information from databases, and who were found to have done so without authority, were held to be the actions of the public body by whom they were employed. However, in those cases, the public body employer argued, at least initially, that the actions of the employees were in fact authorized – the public body did not itself treat the employees in question as 'renegade' employees who were deliberately ignoring the public body's own policies and rules, and acting without even ostensible authority. In the case before me, Service Alberta's policies clearly forbid the activities that gave rise to the complaint. Moreover, the motive of the employee who disclosed the Complainant's personal information was to assist a friend, rather than to perform a service on behalf of Service Alberta. In my view it is less appropriate in a case like the present to treat the actions of an employee as an action of the public body or employer, even though that person has access to the information by virtue of their employment. To put this another way, the fact that an employee acted contrary to a public body's policies and therefore that the employee's actions are not best described as *actions* of the public body, does not mean that a public body has no responsibility if it is the case that its failure to take reasonable steps to prevent such actions contributes to what was done in a given case. In any event, the question of whether the measures that are put in place to ensure only appropriate use of personal information are adequate is essential, regardless whether or not the actions are properly attributable to the public body.

Issue B: Did Service Alberta make reasonable security arrangements to protect the Complainant's personal information against unauthorized disclosure, as required by section 38 of the Act?

[para 25] As I have found that the disclosure of the Complainant's personal information was done without authority, I will now consider whether Service Alberta made reasonable security arrangements to protect the Complainant's personal information from unauthorized disclosure.

[para 26] Section 38 of the FOIP Act states:

> *38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.*

[para 27] In Order P2012-02, the Adjudicator interpreted section 34 of the *Personal Information Protection Act* (PIPA). Section 34 of PIPA is similar to section 38 of the FOIP Act, and states:

> *34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.*

[para 28] The Adjudicator stated:

> To be in compliance with section 34, an organization is required to guard against reasonably foreseeable risks; it must implement deliberate, prudent and functional measures that demonstrate that it considered and mitigated such risks; the nature of the safeguards and measures required to be undertaken will vary according to the sensitivity of the personal information (Order P2006-008 at para. 99).

[para 29] In Order P2012-02, the Adjudicator determined that sensitivity refers to the potential consequences if the personal information is disclosed. For example, whether the individual whom the information is about could suffer harm as a result of the disclosure, or could become the victim of identity theft, are relevant questions when determining whether information is sensitive.

[para 30] Like section 34 of PIPA, section 38 imposes a duty on a public body to make reasonable security arrangements to protect personal information. In my view, a public body will have met the duty under section 38 if it demonstrates that deliberate, prudent, and functional measures have been adopted to guard against, or mitigate, a foreseeable risk. The extent to which security measures are necessary will depend on the sensitivity of the information, as discussed above.

Was the risk foreseeable?

[para 31] The Complainant's information was disclosed as a result of an unauthorized disclosure by an employee, contrary to Service Alberta's policies. In my view, this is a reasonably foreseeable risk. It is clear that Service Alberta has foreseen this risk, given that it has enacted policies and procedures prohibiting registry employees

from disclosing personal information except when authorized to do so. Moreover, it has developed measures to address the conduct of employees who do not comply with the policies and procedures. These measures include suspending or terminating access to the MOVES database, which results in an employee being unable to provide registry services for the period of suspension or termination. Termination of privileges will usually result in termination of employment as a registry employee.

What security measures are in place to guard against the risk?

[para 32] Service Alberta has created policies and procedures prohibiting registry employees from disclosing personal information in the circumstances under which the Complainant's personal information was disclosed. It has also developed disciplinary measures to address the conduct of registry employees who violate the procedures and policies. These measures include suspension and termination of access to the MOVES database. Registry employees undergo criminal records checks and are required to take training regarding the collection, use, and disclosure of personal information.

[para 33] Service Alberta states that it conducted audits of Sentinel Registry's compliance in 2008 and again in 2011. From its submissions, I understand that Service Alberta schedules audits every three years. The audits consist of 180 interview questions detailing audit steps "to determine compliance to the established policies and procedures established by Alberta Registries in all of the registry areas." As set out in its submissions, when Service Alberta conducted an audit of Sentinel Registry Ltd. in 2008, no significant security or confidentiality concerns were identified.

[para 34] However, the findings of the investigation conducted by Service Alberta in 2009 into the Complainant's complaint indicate that information may have been accessed and disclosed without authority, even at the time of the 2008 audit. The audit process described by Service Alberta appears intended to test knowledge and application of policies and procedures, rather than to audit how personal information in the MOVES database is accessed.

[para 35] Service Alberta states:

> The Motor Vehicles Unit also completes regular performance reviews of motor vehicle registry transactions, for each registry agent. Reviews are based on a number of "exception reports" generated by MOVES along with a number of other contributing factors including, but not limited to the agent's historical performance, complaints, non-compliance when performing specific services, SIU investigations. During the course of Sentinel's performance reviews, there were no obvious indications of malfeasant or inappropriate activities in relation to the unauthorized release of confidential information at Sentinel's premises.

[para 36] Although the performance reviews found no indications of "malfeasant or inappropriate activities in relation to the unauthorized release of confidential information at Sentinel's premises", the subsequent investigation conducted by Service Alberta into the employee's handling of the Complainant's personal information, supports a finding that there were other incidents of unauthorized access and disclosure that went undetected at the performance review. From the description of the performance reviews, above, it is

unclear how often Service Alberta conducts performance reviews, whether they apply to all employees, or to some employees, and how extensive they are. As a result, the lack of an indication of "malfeasant or inappropriate activities" arising from an audit or review does not mean that such activities are not, or were not, taking place, or that a more thorough audit process would not have uncovered them.

[para 37] Service Alberta provided the following explanation and summary of the security measures in place to prevent unauthorized access and disclosure of personal information in the MOVES database.

> Previous decisions and investigative reports of the Office of the Information and Privacy Commissioner in relation to the obligations stated above reveal that the public body, in determining the reasonability of its security arrangements against unauthorized disclosure of personal information, ought to take into account:
>
> a) the sensitivity of the information
> b) the possibility of the information being misused
> c) the possibility of the information being disclosed to others
>
> Service Alberta views all of the personal information that it collects and maintains on MOVES as highly sensitive and confidential worthy of considerable efforts being expended in the development of systems and processes aimed at protecting personal information stored in MOVES.
>
> Accordingly Service Alberta has taken all these factors into consideration when:
>
> - Developing the agreements with registry agents with considerable attention being paid to the protection of Albertans' personal information;
> - Requiring registry agents to require police information checks prior to employing registry agent personnel;
> - Requiring registry agents to train their staff members regarding information security practices aimed at protecting client confidentiality;
> - Requiring the CCE [Code of Conduct and Ethics] to be acknowledged by all registry agent personnel on a regular basis driving home the crucial nature of ethical and respectful behavior on the part of registry agent personnel;
> - Issuing unique system access codes to people with MOVES access to both limit access to the system and to help track MOVES usage that may not be in accordance with disciplinary policies;
> - Publishing and requiring compliance with detailed MOVES and AMVIR policies that include many safeguards to ensure that only those clients with sufficient authorization gain access to particular types of MOVES information;
> - Performing regular and ad hoc audits of registry agent policy compliance to improve business and privacy practices amongst registry agents;
> - Engaging skilled investigators to respond to the complaints regarding possible unauthorized disclosures or breaches of the CCE by registry agent personnel;
> - Restricting access to the various registries by registry agent personnel for breaches of the CCE by issuing suspensions (either temporarily or permanent); and
> - Communicating to all registry agents the nature of such suspensions so as to reduce the likelihood that permanently suspended personnel will be hired to perform registry services at other registry agents.
>
> Service Alberta submits that together these measures are reasonable security measures in the circumstances

[para 38] From the foregoing, I conclude that Service Alberta has developed policies and procedures that prohibit gaining access to and disclosing personal information from the MOVES database without legal authority. It conducts audits (which I will discuss below) to ensure that its policies are understood and its procedures are being followed. It also requires registry agents to conduct criminal record checks for their employees. It publishes disciplinary measures such as termination and suspension of registry employees as a deterrent and to ensure that disciplined employees are not hired at another registry. There are mechanisms to track employees' use of the MOVES database (I will discuss these mechanisms below). Investigators are on staff to investigate complaints of unauthorized disclosure or violations of policy.

Is the information that was disclosed sensitive?

[para 39] The registry employee disclosed the address of the Complainant to an individual who sought that information in order to go to his home and confront the Complainant. In this case, the evidence of the Complainant is that the consequence of the disclosure was harassment and the possibility that it will now be necessary to move to another address to avoid further harassment by the individual who obtained the address.

[para 40] While the potential of harassment itself establishes that address information is sensitive, there also exists the potential for physical harm when confidential address information is disclosed. Individuals may elect to keep their addresses unavailable to the public in order to ensure that certain individuals do not learn where they live. If address information is disclosed to such a person by a registry employee, it is foreseeable that the individual who sought to have an unlisted address would be exposed to harm.

[para 41] Moreover address information, combined with details of a driver's license contained in the MOVES database, is information sufficient to create a false driver's license and to expose registry clients to theft of their identities.

[para 42] For the reasons above, I conclude that the personal information that was disclosed from the MOVES database was sensitive, as is potentially all personal information stored in the MOVES database.

Are there reasonable steps that could have been taken to mitigate the risk of unauthorized disclosure that were not taken?

[para 43] Service Alberta provided the details of the investigation that it conducted into the Complainant's complaint. This information was submitted, and accepted, *in camera* on the basis that it would disclose investigation methodology and the personal information of those who participated in the investigation. The details and results of the investigation are contained in a two-page briefing note entitled "Advice to the Director".

[para 44] From the evidence before me, I conclude that the only reason Service Alberta became aware that a Sentinel Registry employee had disclosed the Complainant's personal information without authority was the complaint made by the Complainant. Had the individual who appeared at the Complainant's house not revealed the source of the address information, it appears that the unauthorized access and disclosure of the Complainant's personal information would never have become known to Service Alberta. Moreover, the investigation it conducted following the complaint revealed the possibility of other violations of Service Alberta's personal information access policies and procedures, which would also not have become known, but for the complaint.

[para 45] From its evidence regarding the findings of its investigation, I infer that Service Alberta does not regularly monitor registry employees' access of personal data in the MOVES database, but rather, its focus is placed on monitoring understanding of procedures and policies. I make this finding on the basis that what it found in its investigation was not discovered by its previous audits, even though it is likely that at the time of the audits, personal information from the MOVES database was being improperly accessed and disclosed (Bullet 1 and Bullet 6 of the Briefing Note).

[para 46] If Service Alberta were regularly tracking the manner in which the information it makes available to registry employees is accessed, then it would likely have identified the activities referred to in Bullet 1 and Bullet 6 of the Briefing Note prior to the disclosure of the Complainant's personal information.

[para 47] While I find that the policies and procedures Service Alberta has put in place are reasonable, they are insufficient, in and of themselves, to mitigate the risk that a registry employee may not follow them as intended, or disregard them, as happened in this case. If a public body does not create a mechanism to ensure compliance with its policies or procedures, such as regularly monitoring and auditing how employees access personal information, then it is essentially relying on an "honour system" to protect personal information. Establishing that an employee understands policies and procedures does not necessarily mean that the employee will follow them.

[para 48] With regard to determining whether employees are using the personal information in the MOVES database appropriately, Service Alberta possibly employs a complaint driven model, as it states that its investigators are responsible for conducting investigations into complaints. While Service Alberta states that it has developed mechanisms to track employees' use of the MOVES database, it is unclear whether it employs these mechanisms in circumstances where a complaint of unauthorized disclosure has *not* been made. Certainly, a complaint led to the investigation into the registry employee's use of the MOVES database in the matter before me. As it is not necessarily the case that an individual whose personal information was disclosed without authority would be in a position to know that a registry was the source of the disclosure, it appears possible that instances of unauthorized access may go uninvestigated. The *in camera* evidence submitted by Service Alberta supports this conclusion.

[para 49] It appears that Service Alberta does not proactively investigate the possibility of unauthorized access to the MOVES database, in that it does not regularly monitor employees' access. Service Alberta's audit process, as it has been described to me, does not address or investigate employees' actual usage of the MOVES database, but rather, poses questions regarding knowledge of policies and procedures. Moreover, audits take place every three years and are scheduled, which may not be sufficiently frequent or random to act as a deterrent. The audit process essentially tests knowledge; however, employees may choose not to follow policies and procedures despite having adequate knowledge of them. Consequently, it may be that the prospect of an investigation by Service Alberta is sufficiently remote so as not to amount to a deterrent to an employee who may choose not to follow Service Alberta's policies regarding unauthorized access.

[para 50] I also find that the fact that the employment of the employee who disclosed the Complainant's personal information without authority was terminated will not necessarily operate as an effective deterrent against unauthorized disclosure by other employees. If a rogue employee is satisfied that unauthorized access and disclosure will go undetected, that employee may access and disclose personal information despite the threat of termination.

[para 51] Given the sensitivity of the personal information in the MOVES database, and given that it is a requirement for Albertans to submit their personal information to this database in order to obtain identification or a driver's license, it may be necessary for Service Alberta to adopt more extensive proactive measures to protect the personal information of the Complainant, and that of other Albertans, from unauthorized disclosure by registry employees, such as regularly monitoring use of the MOVES database, even in the absence of a complaint.

Remedy

[para 52] It appears from the evidence before me that had the Public Body reviewed the manner in which personal information was being accessed from the MOVES database by employees of Sentinel Registry, it would have discovered that its policies and procedures were not being followed and could have taken measures to address this situation. Had it done so, prior to the events at issue in this case, it is likely that the Complainant's personal information would not have been disclosed as it was.

[para 53] The evidence also suggests that the personal information of individuals other than the Complainant also may have been accessed by Sentinel registry employees from the MOVES database without legal authority. The potential exists that this information may also have been improperly used or disclosed. Given that individuals who obtain information without legal authorization do not always reveal the source of their information, it is possible that there are, or have been, unauthorized uses and disclosures of personal information from the MOVES database by Sentinel Registry employees that may not have come to light through the Public Body's investigations.

[para 54] The submissions of Service Alberta indicate that it is committed to ensuring the safety of personal information contained in the MOVES database, and I accept that this is so. However, I cannot ignore that there appear to be insufficient measures in place to monitor and ensure Sentinel Registry employees' compliance with legislative requirements when they access personal data, with the result that the personal information of the Complainant, and other Albertans, is subject to the risk of unauthorized access and disclosure. As the Complainant's personal information has already been improperly disclosed to an individual to whom he did not want this information to be disclosed, ordering Service Alberta to take steps to ensure that this does not happen again to his information may appear to be the equivalent of ordering it to close the stable doors. However, there is some benefit to ordering Service Alberta to take proactive measures to monitor the manner in which Sentinel Registry employees gain access to personal information from the MOVES database, as doing so will contribute to increased security against unauthorized access not only in relation to the Complainant's personal information, but also that of other Albertans whose information is stored in the database.

[para 55] I note that many of the findings I have made regarding the measures Service Alberta takes to protect information from unauthorized disclosure may apply equally to registries other than Sentinel Registry. However, the scope of this inquiry is limited to consideration of the circumstances giving rise to the disclosure of the Complainant's personal information by an employee of Sentinel Registry and the submissions of the parties reflect this. Therefore, the issue of whether Service Alberta takes adequate measures to protect personal information in the MOVES database from unauthorized access and disclosure by registry employees, other than Sentinel Registry employees, must be left for another day.

IV. ORDER

[para 56] I make this Order under section 72 of the Act.

[para 57] As I have found that the Complainant's personal information was disclosed by a registry employee without authorization, it follows that I find that Service Alberta did not disclose the Complainant's personal information contrary to Part 2 of the FOIP Act.

[para 58] As I have found that Service Alberta has not taken all reasonable measures to protect against the risk of unauthorized access or disclosure, I order Service Alberta to monitor search access, and operator service transactions at Sentinel Registries (as was done in its investigation of November 17, 2009) to ensure that the Complainant's personal information, and, as a result, that of other Albertans, is being accessed only in accordance with the Act. Service Alberta may determine the frequency with which it must review transactions proactively in order to reasonably guard against the risk of unauthorized access and disclosure of personal information.

[para 59] I further order the Public Body to notify me, in writing, within 50 days of

receiving a copy of this Order, that it has complied with the Order.

_____
Teresa Cunningham
Adjudicator