OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

Investigation Report F09-01

INVESTIGATION INTO DISCLOSURE OF JURORS' PERSONAL INFORMATION BY THE INSURANCE CORPORATION OF BRITISH COLUMBIA

David Loukidelis, Information and Privacy Commissioner

October 8, 2009

Quicklaw Cite: [2009] B.C.I.P.C.D. No. 21
Doc. URL: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF09-01.pdf

Summary: In April 2009, ICBC advised a trial court judge that an ICBC claims adjuster had provided personal information about the trial's jurors to the external defence counsel retained by ICBC for the trial. ICBC conducted its own internal investigation of all the jury trials that could be identified since 2000 and determined that there were five other similar incidents of jury checking. The OIPC's investigation reviewed ICBC policies and practices. While ICBC had policies in place to prohibit jury checking, those policies had not succeeded in preventing these occurrences. ICBC should focus on more specific training for claims adjusters and better communication and awareness of ICBC's privacy policies for external defence counsel.

TABLE OF CONTENTS

1.0 INTRODUCTION

[1] On April 30, 2009, the Insurance Corporation of British Columbia ("ICBC") notified the Office of the Information and Privacy Commissioner ("OIPC") that a lawyer ICBC had retained to defend an ICBC insured in personal injury litigation had asked the ICBC claims adjuster handling the file to conduct checks on the trial jurors to determine if any of them had any previous ICBC insurance claims. The adjuster checked the jurors in ICBC's databases and provided claims information to the lawyer. When ICBC management found out about this, ICBC's in-house counsel appeared before the trial judge and told him what had happened. ICBC also notified each of the jurors of the disclosure of their personal information and apologized for its actions. The personal injury case was settled and the trial was discontinued.

[2] On May 19, 2009, the lawyer who had requested the claims check and ICBC's in-house counsel appeared before the trial judge, who directed that court transcripts be sent to the Ministry of the Attorney General. The minister responsible for ICBC at the time, Hon. Iain Black, asked me to look into the disclosure by ICBC of the personal information of jurors in court proceedings and on May 27, 2009, I agreed to do this, on the following terms:

> In conducting the audit, the OIPC will:
>
> - Identify what staff in ICBC has access to personal information, the policies and practices around access to that personal information, and policies related to ICBC staff working with external contractors where personal information may be involved;
>
> - Assess the adequacy of ICBC privacy policies and management controls for ICBC contractors (*e.g.,* external counsel) or staff to ensure compliance with privacy policies or to detect non-compliance with those policies or management controls;
>
> - Identify any incidents of inappropriate access to, use or disclosure of personal information in court proceedings involving juries;
>
> - Where there has been inappropriate access to, use or disclosure of personal information in court proceedings involving juries, determine who inappropriately disclosed personal information and how, and what led to that inappropriate disclosure;
>
> - Where inappropriate disclosure has occurred, provide recommendations to government on how those affected by any incidents of inappropriate disclosure should be notified;

- Recommend any changes to improve ICBC policies, procedures, and management controls that govern ICBC staff and external counsel in court proceedings involving juries;

- Provide a detailed report with recommendations to the Minister responsible for ICBC and to the Chair of the Board of ICBC to enhance the integrity and security of personal information in ICBC related court proceedings involving juries as soon as possible or at the latest by September 30, 2009; and

- Provide to the Minister (at the same time as the report referenced above) a summary report that is consistent with *Freedom of Information and Protection of Privacy Act* provisions that the OIPC and the Minister will jointly release to the public by October 15, 2009.

[3] Because the scope of our investigation was potentially very broad, I obtained the Minister's agreement to reimburse the OIPC for the cost of retaining additional investigators to assist with our work.

[4] After it discovered what had happened, ICBC began an internal investigation into the checking of jurors' claims history.

[5] To assist with our work, I retained Scales of Governance, whose principal is Dan Rubenstein CA, who has expertise in privacy assessment and auditing. Mr. Rubinstein provided support for the preparation of our investigation and assessment plan. I also retained Deloitte Touche LLP ("Deloitte"), a firm with expertise in privacy advisory and audit services, to conduct a privacy assessment and offer recommendations.

[6] Our investigation was authorized under s. 42 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"):

> **Powers of Commissioner**
>
> 42(1) In addition to the commissioner's powers and duties under Part 5 with respect to reviews, the commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may
>
> (a) conduct investigations and audits to ensure compliance with any provision of this Act,
>
> ...

[7] Part 3 of FIPPA protects personal information, defined as "information about an identifiable individual", by laying down reasonable rules for its collection, use and disclosure by public bodies. Part 3 also contains rules for secure retention and disposal, individual access for accuracy verification and correction, and adequate accuracy and completeness if the personal information

is intended to be used in decisions that directly affect the individual. Part 3 applies to all public bodies, their officers, directors and conventional employees, their service providers and the employees and associates of their service providers. A "service provider" is defined in Schedule 1 of FIPPA as a person retained under a contract to perform services for a public body (*e.g.*, a lawyer retained by ICBC to defend one of its insured in a personal injury action). A service provider may be an individual or an organization that itself employs, retains or subcontracts staff.

2.0 OVERVIEW OF ICBC

[8] ICBC is a Crown corporation that has, since 1973, been in the business of underwriting motor vehicle insurance in British Columbia. This involves the marketing and sale of insurance products, as well as the management of an insurance claims system. Today, ICBC is the sole provider of basic motor vehicle liability insurance in British Columbia and competes with other insurance companies in the sale of optional insurance coverage. Over the years, ICBC has also taken on additional responsibilities such as driver licensing and motor vehicle registration.

[9] ICBC's Claims Division is responsible for settling insurance claims. When a claim is made, an ICBC adjuster is assigned to the file. He or she is responsible for all activity happening on that file. The adjuster begins by reviewing witness statements, talking with the claimant and examining medical and employer records where necessary. The adjuster conducts all necessary investigations, including determining the extent of coverage, interviewing witnesses and collecting medical and income information, all for the purposes of assessing and settling the claim.

[10] ICBC's Claims Division employs a large number of staff. As of August 2009, it had more than 2,711 full-time equivalents.[1] Among these positions, there are approximately 370 management positions, 505 bodily injury adjusters, 520 material damage adjusters and 323 estimators. An example of the number of claims handled by the division in a given year is available from 2008 when approximately 674,500 claims were settled. Individuals were represented by lawyers in approximately 21,500 of the settled claims. Only 299 of the claims proceeded to trial and only 37 were jury trials.

[11] For claims that go to litigation, ICBC often retains defence lawyers in private practice to represent ICBC's insured. ICBC claims adjusters work in concert with external defence counsel to provide originals of documents or files which come into the adjuster's possession. In addition, adjusters work with

---

1 An FTE of 1.0 is equivalent to a person in a paid full-time job all year. Hours worked by several employees part-time or for a part of a period are converted to an equivalent FTE.

counsel to consider the settlement strategy and theory of the defence. This may involve providing counsel instructions necessary to close the pleadings and set necessary court dates.

[12] ICBC claims adjusters require access to personal information in order to process claims. The types of personal information to which adjusters need access include basic personal identifiers such as name and date of birth and detailed prior claims information. Personal information related to claims is stored in either electronic claim systems or in paper files.

[13] Access to personal information stored in electronic claim systems is logically secured through role-based security rules. ICBC has approximately 80 systems that provide information related to claims. Of the 80 systems, some 25 are considered key to ICBC's claims activities. User access to these electronic information systems is managed by ICBC's Information Risk Management department. External defence counsel do not have access to ICBC's electronic claims systems.

[14] Paper claims files are stored at ICBC claim centres around the province. Claim centres each have secure areas that are accessible only by staff members who have an access card, access code or key. The physical security of claim centres is managed by ICBC's Corporate Security department.

[15] The exchange of documents between the ICBC claims adjuster and external defence counsel occurs almost exclusively in paper form. When claims-related information has to be transferred to external defence counsel for litigation purposes, this is managed by the ICBC claims adjuster. Because most claims-related information is found in paper files, the actual files are transferred.

[16] As noted above, soon after it discovered that external defence counsel had obtained claims history information about trial jurors, ICBC began its own investigation into jury checking. The investigation followed a number of paths. ICBC claims centre managers interviewed 1,037 staff who handle files involving litigation. From these numerous interviews, ICBC discovered three further incidents of jury checking, two in 2000 and one in 2006.

[17] ICBC's Special Counsel department interviewed the 87 external defence counsel who conducted jury trials for ICBC in 2008 and 2009. The lawyer involved in the incident discovered this year was interviewed and this disclosed a second incident from 2006. ICBC claims managers also reviewed the 70 litigated claims files that resulted in jury trials since 2008. The file reviews confirmed the results of the interviews with appropriate external defence counsel. Last, ICBC conducted a search of its claims systems and identified 505 jury trials, excluding those it had already identified through interviews. These files

were reviewed by the ICBC Claims Quality Review Team managers. One further incident from 2007 was found.

[18] At my request, the results of ICBC's internal investigation were then reviewed by ICBC's Internal Audit Department. The department has completed a review of the investigation and determined that all possible avenues were examined to determine when jury checking may have taken place.

[19] Copies of both the summary report and the detailed report of ICBC's Internal Audit Department are appended to this report in order to give readers a picture of ICBC's investigation and the steps undertaken to determine the extent of the jury checking issue within ICBC's Claims Division.

[20] In deciding to accept ICBC's internal investigation as a reasonable basis for this report, I have considered the scope and nature of ICBC's internal investigation and carefully reviewed ICBC's Internal Audit report. I am satisfied, as is ICBC's Internal Audit Department, that ICBC's investigators conducted a detailed and comprehensive investigation.

[21] I say this noting that ICBC's internal investigation deals with claims from 2000 to 2009, not earlier. In my initial letter to Minister Black, it was suggested that my investigation would seek to determine the extent of jury checking as far back as 1993. As we delved into the matter, however, it became apparent that prior to 2000, when ICBC implemented a new database system, it was difficult for ICBC to identify jury trials and therefore search for possible jury checking. In any event, it is likely that a claims adjuster who performed a jury check would have believed this was appropriate and would have recorded the jury check in the file. In this respect, I note that from 2000 to 2007 five additional incidents were identified and in 2008 and 2009, a period for which more extensive auditing capability was available, only the original incident was found to have occurred.

[22] More significantly, while it was important to determine the number of incidents, it has always been my view, with which ICBC agrees, that the problem had to be assessed and addressed regardless of the number of incidents.

3.0 OIPC INVESTIGATION AND ASSESSMENT

[23] As indicated earlier, I retained Deloitte to conduct a privacy assessment in order to determine if ICBC had sufficient safeguards in place to prevent the inappropriate disclosure of personal information by ICBC claims adjusters to external defence counsel. I also asked Deloitte to make any recommendations it considered necessary for improvements to ICBC's systems.

[24] Because ICBC is a public body governed under FIPPA, it must follow FIPPA's rules on collection, use and disclosure, and its actions must be

consistent with those permitted under this legislation. ICBC must have the appropriate authority to collect personal information under sections 26 and 27 of FIPPA, as well as the authority to use and disclose personal information as permitted under sections 32, 33, 33.1, 33.2 and 34 of FIPPA. It was determined that it would be appropriate to use the Generally Accepted Privacy Principles ("GAPP") framework of the Canadian Institute of Chartered Accountants as a standard by which to review ICBC's current policies, processes and practices regarding litigated claims involving ICBC claims adjusters and external defence counsel. My Office reviewed the GAPP principles as suggested by Deloitte and agreed that the principles chosen by the firm are reflective of the relevant sections of FIPPA for the purposes of this particular case.

[25] The final report submitted to me by Deloitte and reproduced in an appendix to this report below forms the majority of this section of the report.

[26] This report does not address or comment on the checking or vetting of prospective or selected jurors generally in civil litigation proceedings or in criminal proceedings.

4.0 CONCLUSION

[27] As soon as it discovered the privacy breach, ICBC disclosed the fact, accepted responsibility and diligently conducted its own investigation. ICBC did not and does not condone the practice of jury checking as occurred here, contrary to ICBC's own policies, which at the time stated that jury checking was not permitted. ICBC's published Litigation Management Strategy at the time informed external defence counsel that ICBC did not permit the practice. Nevertheless, despite this published policy, jury checking was done on this reported occasion and the investigation has uncovered five other examples since 2000. While this represents a small percentage of jury trials, that it happened at all is unacceptable.

[28] In terms of immediate steps, the recommendations in the Deloitte report reflect discussions with my Office and I adopt those recommendations. I believe that their implementation will add needed strength to an already good program of privacy compliance and will therefore monitor their implementation by ICBC. My Office will provide assistance if necessary to ICBC and will meet with ICBC in six months and again in one year to determine progress with implementation of the recommendations.

[29] Specifically, as set out in the Deloitte report, I recommend that ICBC focus on the need for more specific training for the groups that were involved in the jury checking incidents. Although ICBC had good generic training for its employees, and the Litigation Management Strategy specifically prohibited jury checking, for some reason this information did not penetrate to the individuals involved in

these inappropriate disclosures, either ICBC claims adjusters or external defence counsel. The recommendations in the Deloitte report present ways for ICBC to pursue more specific preventive, maintenance and detective controls to help ensure that all employees and contractors are aware of specific obligations to protect the privacy of their clients.

[30] In addition to the recommendations set out in the Deloitte report, another important factor is the fact that many of ICBC's information technological systems are of an older generation. As noted above, I accepted that these systems do not allow auditing at a level which would be effective at determining inappropriate access to the systems. However, I understand that there is discussion about upgrading these systems over time. I therefore strongly recommend that ICBC's privacy office have substantial input into the development of any new systems, from the very outset, to ensure that proper privacy safeguards and the security of personal information are not an afterthought. ICBC should use appropriate privacy impact assessment tools to achieve this, again, at the very outset of any planning for new information systems.

[31] Further, although ICBC currently uses a role-based access model for its information systems, it is my understanding that ICBC claim adjusters have access to virtually the entire claims system. While this is in some respects not surprising given the nature of their work, I also recommend that ICBC review the present role-based access model for this system, since decisions on permitted access may have been made in the past when a different approach to privacy existed. For example, some degree of geographically-restricted access may be possible, under which ICBC adjusters have access only to information related to files in their region. At all events, as it moves forward with new information systems investments, ICBC should seriously re-examine the access needs of all employees to ensure that they meet current legislated standards and industry practices.

[32] I believe that ICBC's privacy office has done a very good job in developing and implementing general privacy awareness training and practices for an organization which is required to maintain extensive personal information holdings. It is important that information and privacy continue to have a significant place in the governance structure of ICBC, which is required to maintain a large amount of often sensitive personal information of citizens. I therefore recommend that ICBC take this opportunity to ensure that its privacy office has a significant voice in the organization, such that it is able to accomplish its objectives.

[33] Under the direction of Jon Schubert, President and Chief Executive Officer, and his colleagues, ICBC has cooperated fully with our work, for which we are appreciative.

[34] Jim Burrows, Acting Manager, Mediation and Investigation, co-ordinated this investigation and prepared this report.

Appendix 1 — Deloitte Touche LLP Report

Appendix 2 — ICBC Internal Investigation Report

Appendix 3 — ICBC Internal Investigation Report — Details Summary

Appendix 4 — ICBC's Response to Report Recommendations

October 8, 2009

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

OIPC File: F09-38265

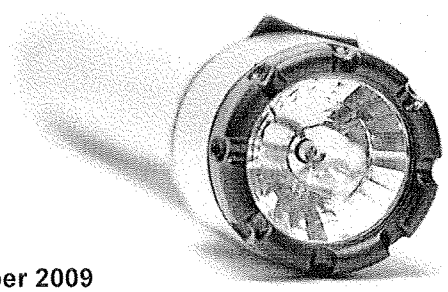
APPENDIX 1

Deloitte Touche LLP Report

Deloitte.

Report to the Office of the Information & Privacy Commissioner

Insurance Corporation of British Columbia – Protection of personal information in the litigated claims process



September 2009

Table of contents

Executive summary

On May 28, 2009, the Information and Privacy Commissioner announced his intent to undertake a privacy assessment of Insurance Corporation of British Columbia (ICBC) jury trials and the disclosure of personal information of jurors involved in ICBC jury trials. Deloitte was engaged by the Commissioner to perform a privacy assessment of the management, preventative, and detective controls in place at ICBC at the time of review.

This privacy assessment was performed to determine whether ICBC had designed and implemented sufficient safeguards over the disclosure of personal information in the litigated claims process. In consultation with the Office of the Information and Privacy Commissioner (OIPC), the scope of this review was limited to controls in place over the disclosure of personal information between the ICBC claims adjuster and external defence counsel at the time of the review.

For our review, we used the Generally Accepted Privacy Principles (GAPP) as a framework for addressing and assessing each of the significant and relevant aspects of the Freedom of Information and Protection of Privacy Act (FIPPA) as they pertain to privacy practices.

Summary of observations

At the time of our review, we observed that ICBC had in place a number of adequately designed processes. These included a dedicated team of resources focusing on privacy within ICBC, a well-structured process for receiving and handling privacy incidents, and IT security measures to prevent unauthorized access to IT systems. In addition, we observed that there are deficiencies and opportunities for improvement to the design of management, preventative, and detective controls.

For management controls, the following was observed:

- **A lack of clear privacy guidelines for ICBC claims adjusters and external defence counsel** (!): Policies and procedures documenting ICBC's privacy practices are available; however we did not identify sufficiently clear privacy guidelines and practices for ICBC claims adjusters and external defence counsel documenting specific ICBC privacy practices.
- **A lack of tracking on privacy policy changes** (⚠): ICBC's Information and Privacy department update privacy policies based on changes to legislations applicable to ICBC and changes to business operations. However, there is no tracking of when policies are updated to facilitate effective communication of changes to employees.

For preventative controls, the following was observed:

- **Inadequate privacy training to ICBC claims adjusters** (!): Privacy training is provided to claims employees including ICBC claims adjusters, however training is generic and does not provide sufficient guidance on the specific issues that ICBC claims adjusters deal with on the use and disclosure of personal information on a daily basis.
- **Inconsistent frequency of privacy training to ICBC claims adjusters** (!): Privacy training is provided to claims employees including ICBC claims adjusters, however privacy training is not mandatory and there is no requirement to refresh knowledge on a regular basis. It was noted that privacy training will be mandatory for all ICBC employees in 2010.
- **Inadequate awareness of ICBC's privacy requirements by external defence counsel** (!): The Litigation Management Strategy is a set of procedures provided to external defence counsel law firms containing privacy policies and obligations of law firms. However, ICBC does not provide adequate awareness of its privacy requirements to external defence counsel.

- **A lack of acknowledgement of ICBC policies by external defence counsel** (!): ICBC does not have a policy in place requiring external defence counsel to acknowledge their understanding and compliance with ICBC privacy policies.
- **Privacy considerations are not accounted for in the external defence counsel selection process** (⚠): Although law firms involved in privacy incidents will likely be terminated by ICBC and not contracted in the future, the external defence counsel selection process used to evaluate external defence counsel law firms does not account for privacy considerations such as privacy incidents or breaches resulting from the law firm.

For detective controls, the following was observed:

- **A lack of proactive identification of privacy issues** (!): Although there is an established process for handling privacy incidents reported by individuals, ICBC does not have processes in place to proactively identify privacy incidents.

Privacy assessment

Introduction

On May 28, 2009, the Information and Privacy Commissioner announced his intent to undertake a privacy assessment of ICBC jury trials and the disclosure of personal information of jurors involved in ICBC jury trials. In a letter to the Minister responsible for ICBC, the Commissioner stated that the work would be presented to the Minister by September 2009 with a public report by October 15, 2009. Investigative work has already taken place and the Commissioner engaged Deloitte to perform the privacy assessment.

This privacy assessment was performed to determine whether ICBC had designed and implemented sufficient safeguards over the disclosure of personal information in the litigated claims process.

Scope

The process for adjudicating litigated claims at ICBC involves various ICBC employees and external contractors. In consultation with the Office of the Information and Privacy Commissioner ("OIPC"), the scope of this review was limited to controls in place over the disclosure of personal information between the ICBC claims adjusters and external defence counsel at the time of the review. Specifically, this includes policies, procedures, and processes relating to litigated claims in the ICBC Claims Division involving the claims adjuster and external defence counsel:

- Disclosure of information from adjusters to external defence counsel;
- Logical security safeguards protecting personal information contained in application systems containing litigated claims data; and
- Physical security safeguards protecting personal information for open and/or active litigated claims.

External defence counsel is engaged by ICBC to act on their behalf on the litigation aspects of a claim.

Methodology

ICBC is required to comply with FIPPA. FIPPA governs how ICBC collects, uses, discloses, protects, and destroys personal information. As such, this assessment was be guided by FIPPA.

It was determined that the Generally Accepted Privacy Principles (GAPP) framework addressed each of the significant and relevant aspects of FIPPA as they pertain to privacy practices. Areas of GAPP, which are not relevant to FIPPA, were not included in our scope. As part of the planning activities, the relevant provisions of FIPPA were analyzed and mapped to the relevant sections of GAPP. The GAPP framework was used to establish the primary assessment objectives and expected control activities for this assessment.

To determine the GAPP principles relevant for our review, we evaluated each principle area and supporting components based on 2 factors:

1. Applicability to the privacy breach resulting from the claims adjuster/external defence counsel relationship for litigated claims.
2. Applicability to the supporting control environment relating to the privacy breach resulting from the claims adjuster/external defence counsel relationship for litigated claims.

Based on our understanding of risks identified by ICBC and OIPC through interviews and discussions, we identified specific assessment objectives and assessment criteria to refine the scope of our work using

the above 2 factors. For each GAPP assessment objective, we assigned a ranking of High (H), Medium (M), or Low (L) to each factor. Assessment objectives where one or both factors were deemed High were considered in-scope for this assessment. Using this scoping criteria, together with the OIPC, the GAPP principle areas applicable and in-scope for this assessment were determined.

Assessment approach

We conducted the following procedures in performing this assessment:

1. We conducted interviews with key individuals in the Information and Privacy, Claims, Information Technology, Corporate Legal, Employee Relations, and Information Risk Management departments to understand the current processes and controls in place.
2. We reviewed supporting documentation, such as policies and procedures, to corroborate our discussions and understanding on the design of controls in place.
3. We documented our observations and validated the accuracy of our observations with ICBC management.

Assessment summary

In order to assist with our understanding of the ICBC privacy control environment, we categorized the assessment objectives in each GAPP principle area into three types of controls:

- Management (M),
- Preventative (P), and
- Detective (D).

In the table below, we outlined the GAPP principles and assessment objectives applicable to this assessment along with the summary of conclusions for each assessment objective. In the Assessment Conclusions column, we indicated the summary of our assessment conclusions for management (M), preventative (P), and detective (D) controls as follows:

✓ = Control is designed and implemented appropriately to meet the assessment objective.

! = Control deficiency/deficiencies exist that impair the achievement of the assessment objective.

△ = Control improvements were identified that would assist in more effectively meeting the assessment objective.

GAPP Principle Area	Assessment Objective		Assessment conclusions		
			M	P	D
Management - ICBC defines, documents, communicates, and assigns accountability for its litigated claims privacy policies and procedures.	1.1	Privacy policies are in place and documented	✓		
	1.2	Privacy policies are communicated to ICBC claims adjusters		!	
	1.3	Responsibility and accountability for privacy within ICBC are assigned	✓		
	1.4	Changes to ICBC privacy policies are reviewed and approved	△		
	1.5	ICBC policies and procedures are consistent with FIPPA	✓		
	1.6	Contracts with external defence counsel are consistent with ICBC privacy policies and procedures	✓		
	1.7	ICBC IT security policies are consistent with privacy policies	✓		
	1.8	Sufficient supporting resources are available to implement privacy policies	✓		
	1.9	Qualifications of personnel responsible for protecting privacy and personal information within ICBC are established	✓		

GAPP Principle Area		Assessment Objective	Assessment conclusions		
			M	IP	D
	1.10	Changes in ICBC business and regulatory environments are reviewed for privacy requirements	✓		
Use - ICBC limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.	2.1	Privacy policies that address the use of personal information are in place	!		
	2.2	Use and retention policies are communicated to individuals	✓		
	2.3	Personal information related to litigated claims is used only for the purpose identified in the notice and with the individual's consent or for the purposes for which it was collected or a purpose consistent with such a purpose	✓		
Disclosure to Third Parties - ICBC discloses personal information to external defence counsel only for the purposes identified in the notice and with the implicit or explicit consent of the individual.	3.1	Privacy policies that address the disclosure of personal information to external defence counsel are in place	✓		
	3.2	ICBC privacy policies are communicated to external defence counsel		!	
	3.3	Privacy policies that address the consistent use of personal information as stated in the notice to individuals by external defence counsel are in place		▲	
	3.4	Agreements for external defence counsel to protect personal information are in place		✓	
	3.5	Remedial action is taken when there is misuse of personal information by external defence counsel			✓
Security for Privacy - ICBC protects personal information against unauthorized access (both physical and logical).	4.1	Privacy policies that address the security of personal information in litigated claims data is in place	✓		
	4.2	A security program to protect personal information related to litigated claims is documented and in place	✓	✓	
	4.3	Logical access to personal information related to litigated claims is appropriately restricted		✓	!
	4.4	Physical access to personal information related to litigated claims is appropriately restricted		✓	
	4.5	Transmission of personal information between ICBC claims adjusters and external defence counsel is protected		✓	
	4.6	Test of the effectiveness of logical and physical security safeguards of personal information contained in litigated claims data is performed on an annual basis		✓	
Monitoring and Enforcement - ICBC monitors compliance with its litigated claims privacy policies and procedures and has procedures to address privacy-related complaints and disputes.	5.1	Policies that address the monitoring and enforcement of ICBC privacy policies are in place	✓		
	5.2	Individuals are informed on how to communicate privacy complaints	✓		
	5.3	A process for handling, addressing, resolving, and documenting all privacy complaints is in place			✓
	5.4	Reviews of compliance with ICBC privacy policies and procedures are performed			!
	5.5	Instances of non-compliance with ICBC privacy policies are documented and remediated on a timely basis			✓

Detailed observations and recommendations

Our detailed observations and recommendations are presented in the three categories of management, preventative, and detective controls. For each category, we provided a description on the summary of controls in place at ICBC at the point of our review, a summary of assessment observations, and suggested recommendations.

Management controls

Management controls represent measures in place for an organization to establish and communicate policies and procedures as a standard of expectation to all employees. Specifically for privacy, this includes establishing privacy policies and procedures, making policies available to all employees, and communicating updates or changes to policies. Adherence to privacy policies and consequences of non-compliance should be communicated all employees. In addition, management controls include the establishment of dedicated resources to manage the overall privacy mandate within the organization.

Summary of controls in place

We identified the following management controls in place at the time of our review:

A. ICBC's Information and Privacy Department
(Relates to Assessment Objectives 1.3, 1.8, 1.9, 5.2)

ICBC has established a dedicated Information and Privacy department that is delegated directly by the ICBC President and CEO to administer ICBC's obligations under FIPPA. The department reports to the Vice President of Communications and consists of 3 managers, 3 fair practice advisors, 8 senior information officers, 6 information access privacy clerks, and 2 administrative assistants. Of these 22 employees, 4.5 full time employees are mainly responsible for privacy related issues. The other employees focus mainly on freedom of information requests. The Information and Privacy department is responsible for documenting, implementing, enforcing, monitoring, and updating privacy policies throughout the corporation.

Employees hired into the department have been transferred from other departments within ICBC due to their experience at ICBC and interest in privacy. Although there are no requirements for privacy designations before being hired into the Information and Privacy department, training is provided to employees within the department once they are hired. Such training includes annual privacy conferences held by the provincial government and privacy classes held by the University of Alberta. In addition, the members of the Information and Privacy department belong to a number of privacy professional organizations such as the local chapter of the International Association of Privacy Professionals. They also subscribe to different privacy related newsletters and dashboards to stay up-to-date on current privacy legislation and requirements.

Employees are informed on how to contact the Information and Privacy department through the Information and Privacy department site on the ICBC intranet, privacy brochures and posters, and the Privacy Incident Response document. The email and phone number contact information to the Manager of Information and Privacy are specified on these publications. In addition, the ICBC intranet

provides a privacy incident web reporting tool that allows for privacy incident reporting through an online form.

B. Privacy Policies and Procedures

(Relates to Assessment Objectives 1.1, 1.4, 1.5, 1.6, 1.7, 1.10, 2.1, 2.2, 2.3, 3.1, 4.1, 4.2, 5.1)

The Information and Privacy department is responsible for communicating, updating, and creating privacy policies. ICBC's privacy policies, procedures, practices are documented and embedded into various policies and manuals. These include:

i) **Code of Ethics** – ICBC's Code of Ethics is a set of principles and guidelines that every ICBC employee is expected to follow in their daily work. Included in this document are privacy obligations of employees that address the use, confidentiality, security, and disclosure of information. The Code of Ethics is required to be acknowledged and signed-off by all new employees to ICBC.

ii) **Corporate Policy Guide** – The Corporate Policy Guide contains corporate policies on various topics. This guide is available on the ICBC intranet and is accessible to all ICBC employees. Part of the guide includes privacy policies including:

- confidentiality;
- release of information including disclosure to other agencies;
- retention of documentation;
- information systems security policies and principles; and
- E-business.

iii) **Claims Procedure Manual** – ICBC claims division has its own set of detailed procedures which outlines specific information for claims employees. Privacy is addressed in various sections of this manual including:

- Section 1.9 Releasing Corporate Information
- Section 8.13 Personal Information Protection Act
- Section 13.15 Implied Undertaking of Confidentiality

iv) **IT Security Policies** – ICBC's Information Risk Management group is responsible for the management and implementation of the IT Security Program and for maintaining the Information Systems Security Policy framework. The purpose of the IT Security Program is to protect the information assets of ICBC from threats. As part of the framework, there are 12 security principles that support this purpose. One of these principles includes protecting privacy as follows: "ICBC will ensure the protection of private information by establishing and documenting policies, standards, procedures, guidelines, and best practices; by managing the information lifecycle to protect information and information systems from unauthorized access and disclosure; and by ensuring compliance with auditing, legal, and legislated requirements" (ICBC Information Security Principles, Section 2.2, Protect Privacy).

v) **Litigation Management Strategy** – The Litigation Management Strategy (LMS) is a manual provided to external defence counsel law firms contracted with ICBC to provide litigation services. The LMS outlines ICBC's expectations of counsel that includes guidelines for billing, file management, allocation of ICBC claims adjusters and external defence counsel functions and responsibilities, and file handling procedures. The LMS is provided to external defence counsel through the ICBC external counsel website.

External defence counsel are required to visit the site on a regular basis for updated instructions and information on new and emerging legal issues and trends. Privacy is discussed in Section 10 of the LMS and specifically states that "jury checking is not a permissible practice under Part 3 of FIPPA. ICBC staff has been advised that accessing ICBC's databases for this purpose is prohibited" (Litigation Management Strategy, Section 10.10, Freedom of Information). At the time of our review, we did not identify that ICBC had a mechanism in place to provide a privacy awareness program and monitor the acknowledgement of the LMS.

Policies and procedures are reviewed on a regular basis by the Information and Privacy department to determine whether ICBC policies reflect changes based on FIPPA requirements, provincial

legislation, and business processes. Various working committees are established to address and stay updated on changes. Such groups include the Information Security and Privacy Steering Committee and the Issues Committee to discuss high profile issues, including privacy incidents, affecting ICBC. In addition, the Information and Privacy department are integrated into major business change projects to determine effects on privacy policies. Privacy Impact Assessments are performed to determine the effects of changes to the business and privacy considerations.

C. Information Security and Privacy Steering Committee

(Relates to Assessment Objectives 1.3, 1.7)

ICBC has established an Information Security and Privacy (IS&P) Steering Committee comprised of representatives from Information Risk Management, Employee Relations, Corporate Audit Services, General Counsel, IT Architecture, Claims, Insurance, Finance, and also subject matter experts from Information Risk Management, Privacy, Corporate Security and Information Management, Communications, and Information and Privacy groups. The Steering Committee meets on a monthly basis to discuss relevant topics dealing with information security and privacy. Examples of discussion areas may include key incidents arising in privacy, topics to be included in the security awareness campaign or recent IT security threats. In addition, changes to IT security or privacy policies are reviewed and approved in these meetings by committee members.

D. External Defence Counsel Selection Process

(Relates to Assessment Objective 1.6)

The external defence counsel relationship with ICBC is managed by the ICBC Claims Legal Services group. This group is responsible for managing the portfolio of external defence counsel and administering the contracts between the law firms and ICBC. This includes the external defence counsel selection process whereby law firms go through a contracting phase prior to becoming a law firm for ICBC, and the Litigation Management Strategy, which documents the expectations and privacy requirements external defence counsel are responsible for with respect to handling litigated claims.

i. **External Defence Counsel Selection Process** – The external defence counsel selection process is the method used to select external defence counsel law firms for performing ICBC claims litigations. The selection process occurs every three years and involves obtaining criteria which external defence counsel law firms are rated on. Criteria such as customer satisfaction as rated by the ICBC claims adjusters, percentage of plaintiff work performed by the law firm, degree of succession planning by the law firm, and counsel past performance on trials. Based on these criteria, law firms with favourable ratings are selected. Selected law firms are then contracted through the Strategic Alliance Agreement.

   The Strategic Alliance Agreement is the contract between external defence counsel law firms and ICBC. As part of the agreement, privacy is addressed at a high level as it relates to collection, use, retention, and disclosure of personal information. In addition, the agreement states that law firms and legal team members must observe all of ICBC's policies, guidelines, and procedures, including those outlined in the Litigation Management Strategy.

Observations and Recommendations

Observation 1: Clear Guidelines on Privacy (!)

(Relates to Assessment Objectives 2.1)

Assessment Observation: We observed that ICBC has not documented specific guidelines and practices that ICBC claims adjusters and external defence counsel deal with on a day-to-day basis involving the use and disclosure of personal information. The existing privacy policies and procedures which exist at the time of our review were general and embedded within other policy or procedure manuals. Examples of these specific guidelines include practices which are permissible in court but not

permissible under ICBC policies or other decisions which ICBC have made in terms of specific procedures or practices.

We noted that since the jury breach incident, ICBC established the Claims Privacy Framework group which is responsible for tracking common themes, defining solutions, and defining consistent approaches to the most common issues in accordance with current privacy policies or ICBC practices. At the time of our review, the results of Claims Privacy Framework group had not yet been incorporated into the Claims Procedure Manual.

Recommendation: We recommend that a clear and concise set of guidelines for privacy relating to ICBC claims adjusters and external defence counsel be developed to assist with communicating privacy policies and practices. Such guidelines may be in the form of Frequently Asked Questions or a webpage containing privacy considerations and illustrative examples that claims adjusters and external defence counsel deal with on a daily basis.

Observation 2: History Log for Privacy Policy Changes (▲)

(Relates to Assessment Objectives 1.4)

Assessment Observation: We observed an opportunity for improvement for tracking changes to ICBC privacy policies and procedures. We observed that ICBC does not retain a history log of changes made to privacy policy or procedures. The update of privacy policies and procedures is coordinated through ICBC's Information and Privacy Department.

Recommendation: We recommend that a history log of changes made to privacy policies and procedures be developed to assist with the tracking of changes due to changes in legislation or business processes. A log of changes would provide a tracking of updates made to policies and procedures to improve communication of changes to employees.

Preventative controls

Preventative controls are measures in place to deter both unintentional and intentional actions which lead to privacy incidents. This includes regular training and awareness programs on privacy policies and practices to all employees. Training and awareness educate individuals and assist in preventing privacy incidents. In addition, preventative controls include having security processes in place, through IT systems and physical facilities, to prevent unauthorized access. These types of security processes assist with discouraging both unintentional and intentional actions could lead to privacy incidents.

Summary of controls in place

We identified the following preventative controls in place at the time of our review:

E. Privacy Training and Awareness

(Relates to Assessment Objective 1.2)

ICBC has a number of different methods in providing training and generating awareness on privacy issues. These training and awareness initiatives are implemented by various departments including the Information and Privacy, Information Risk Management, and Learning and Development departments.

- **New Employee On-boarding** – The Employee Relations department has a new employee on-boarding presentation which is used for training new employees at ICBC. For non-managers, this presentation includes a 15 minute overview from the Information and Privacy department on employee's privacy responsibilities. For managers, this presentation is 1 hour long. In addition, new employees must sign the Code of Ethics prior to joining the corporation. The Code of Ethics includes criteria for the use and confidentiality of corporate and personal information.

- **Company Wide Privacy Tutorial** – The Information and Privacy department developed an online tutorial in 2007 addressing privacy topics and issues. The tutorial covers topics including a background of FIPPA, a definition of personal information, unauthorized use or retention, inappropriate disclosure, and the privacy incident protocols for reporting complaints or privacy incidents. At the end of the privacy tutorial, there is an acknowledgement page which asks for the individual's acknowledgement of their privacy responsibilities. The privacy tutorial includes questions to reinforce understanding.

  This privacy tutorial is available company-wide to all ICBC employees, including ICBC claims adjusters, through the ICBC corporate intranet. At the time of our review, the privacy tutorial is voluntary for ICBC employees to complete, however ICBC has plans in place to make the tutorial mandatory for all ICBC employees in 2010.

- **Privacy Awareness** – The Information and Privacy department developed privacy awareness materials such as posters, door hangers, and brochures in order to generate awareness for privacy. These materials included information on the employee's responsibilities for privacy, tips for improving privacy and security, and the contact information of the Information and Privacy department for further questions. We observed that these materials were distributed and hung through-out the ICBC head office and at the Capilano claims center where we performed a site visit.

  In addition, the Information and Privacy department provides road show presentations on privacy to various claim centers. These presentations are performed on an ad-hoc basis, at the request of the claim center or due to an incident or concerns regarding privacy. The presentation topics cover information on FIPPA, key steps in protecting privacy, office practices for keeping a clean desk, the use of screen savers, and methods of securing customer information at the end of the day.

- **IT Security Tutorial** – The Information Risk Management department developed an online tutorial addressing IT security and privacy. The tutorial covers topics including IT security principles for privacy, workstation security, security on system access and electronic data, and the protocols for reporting security incidents and violations. At the end of the IT security tutorial, there is an acknowledgement page which asks for the individual's acknowledgement on information systems security. The IT security tutorial includes questions and videos to reinforce understanding. In order to pass the tutorial, participants are required to get at least 80% of the questions correct.

  This IT security tutorial is available to all ICBC employees, including ICBC claims adjusters, through the ICBC corporate intranet. At the time of our review, the IT security tutorial is voluntary for ICBC employees to complete, however ICBC had plans in place to make the tutorial mandatory for all ICBC employees in 2010.

F. Logical Security Safeguards to Litigated Claims Systems

(Relates to Assessment Objectives 4.3, 4.6)

The Information Risk Management (IRM) group of ICBC's Information Systems Division is responsible for the management and implementation of ICBC's IT security program and IS security policies. The Chief Information Officer has executive ownership over this IT security program. As part of this program, there are 12 security principles that support the protection of ICBC assets from threats. One of these principles includes the protection of privacy. The IRM group has the following logical security safeguards in place for restricting access to claims systems:

- **Password Policies** – Access to ICBC networks and claims systems are restricted by the use of assigned user ID's and passwords. Each employee, including litigated claims adjusters, is required to have a unique ID to log-on to ICBC networks and claims systems. Password policies are handled by an application called IDMan which manages the configurations for password complexity, password length, and password expiry. At the time of our review on the design of the password configuration policies, we found no deficiencies.
- **Role Based Access** – The system access rights to claims systems is restricted by job roles which is documented and defined. ICBC claims adjusters each have their own user ID/password and are granted access to only those systems which they have been authorized to. This role based access is managed by super profiles and other defined system access rights.

- Super profiles are a combination of individual system profiles that have been bundled for various job roles and have been pre-approved by data owners. In addition to super profiles, there are location-specific systems that have been documented and defined for all claim center locations. System access is only granted to those individuals who are working in a particular role at a particular location.
- **Data Access Request Process** – The management of user access to claims systems is handled through the Data Access Request (DART) process. DART is a workflow application which manages the approvals for new user access rights, modification to existing users rights, and removal of user access rights. A DART is required before any addition, changes, or deletions to system access are made.

  The process starts with a request through the DART form. The DART form is completed by the individual's manager and must contain the employee's full name, RACF ID (for existing employees), and a description of the access required. The DART form is then forwarded to the Information Risk Management (IRM) group. For new employees, IRM would perform a check in the SAP Human Resources system to ensure that the individual has been already set-up by HR prior to any access being granted. For existing employees, IRM would confirm the individual's job role in the SAP Human Resources system. Once confirmed, IRM would determine the access rights required by the role based on defined and documented access requirements. IRM would then add the appropriate managers required for access rights approval and forward the DART form to that individual for approval. Once the DART form has been approved, IRM would grant access.

- **Review of Access Rights** – Review of access rights are performed for both regular users and users with privileged access. For regular users, a review of access rights for users at claim centers, including ICBC litigated claims adjusters, is performed on a yearly basis by the Manager of Claims Workforce Planning. The review involves confirming that super profiles have been assigned correctly based on the individual's job roles. Exceptions are noted and flagged for further follow-up with the individual's manager and with the Information Risk Management group.
- For privileged users, a review of access rights is performed on a monthly basis by the Information Risk Management group. The review involves confirming that privileged rights (e.g. systems administrator access) to claims data or systems are still appropriate. Exceptions are raised to the Manager of Information Risk Management.
- **Tests of Security** – The Information Technology group performs various types of self-assessments on IT security throughout the year. These include network assessments and vulnerability tests performed on a regular basis and operational risk assessments when significant configuration changes are made. IT security programs are also reviewed by Corporate Audit Service and through third party assessments

G. Physical Security Safeguards to Litigated Claims Files at Claim Centers

(Relates to Assessment Objectives 4.4, 4.5)

Litigated claims files which ICBC are in possession of are stored at ICBC claim centers. The area within claim centers where litigated claim files are stored is physically safeguarded. Active litigated claims files are stored within the secured area where adjusters sit. Access to the secured area within the claim center is restricted using doors which require access cards. Only authorized individuals working at the claims center have access rights to the secured area. The access cards are managed and issued by the ICBC Corporate Security group.

The main method for transferring litigated claims information between claims adjusters and external defence counsel occurs in the form of paper files. The transfer of physical files is performed through a mailing service used as a standard in the legal community. The claims adjusters have the responsibility for keeping track of the location of files before they are sent to document retention. Claim files that have been recently closed are also stored within the secured area of the claim center. An additional wired area with a cage fence with code lock is used to further restrict access to these files. Only staff with authorized access to the claim center has access to the file cage. The code to the cage is changed every 2-3 years. Recently closed files are stored here before they are sent off to the retention center.

Observations and Recommendations

Observation 3: Privacy Training specific for ICBC Claims Adjusters (!)

(Relates to Assessment Objective 1.2)

Assessment Observation: We observed that the privacy training available through tutorials and new employee on-boarding sessions at the time of our review provided training on general privacy concepts for the organization as a whole. However, privacy training does not address specific privacy issues related to claims adjusters. As claims adjusters are required to handle personal information on a daily basis, specifically related to use and disclosure, privacy training specific for claims adjusters addressing acceptable privacy practices would assist in their understanding and compliance with privacy policies.

Recommendation: We recommend that training with specific content relating to privacy issues which claims adjusters deal with on a daily basis be provided to assist in their understanding and compliance with privacy policies. Such training may include specific privacy considerations or illustrative examples relevant to ICBC claims adjusters.

Observation 4: Frequency of Privacy Training for ICBC Claims Adjusters (!)

(Relates to Assessment Objective 1.2)

Assessment Observation: We observed that claims adjusters do not receive privacy training on an annual basis. Although all claims employees were required to complete the Privacy Tutorial as a result of the jury breach incident, it is not mandatory for employees, including ICBC claims adjusters, to take the tutorial and review it on a regular basis.

Recommendation: We recommend that mandatory privacy training for claims adjusters be provided to assist with the communication and compliance with privacy policies and practices. For example, requirements for employees to complete the training, testing at the end of the training, and logging training attendance on an annual basis would assist with reminding employees of privacy obligations, as well as communicating updates to privacy policies and practices.

Observation 5: Privacy Awareness of ICBC's Privacy Requirements by External Defence Counsel (!)

(Relates to Assessment Objective 3.2)

Assessment Observation: We observed that ICBC does not provide adequate awareness of its privacy requirements to external defence counsel. Although the Litigation Management Strategy (LMS) is available to external defence counsel, it contains information which may not be relevant to individual external defence counsel members and the specifics of the day-to-day activities they deal with in relation to use and disclosure of personal information.

Recommendation: We recommend that an awareness program, with specific content relating to privacy issues which relates to external defence counsel, be developed to assist in their understanding and compliance with privacy policies. This program may include a tutorial with specific privacy considerations or illustrative examples relevant to external defence counsel.

Observation 6: Acknowledgement of Privacy Policies by External Defence Counsel (!)

(Relates to Assessment Objective 3.2)

Assessment Observation: We observed that ICBC has not established a policy which requires external defence counsel to acknowledge ICBC's privacy policies. Although the Litigation Management Strategy (LMS) is available to external defence counsel law firms through the ICBC external counsel website, and the LMS is referenced in the Strategic Alliance Agreement between ICBC and law firms, there is no requirement for individual counsel members within the law firms to acknowledge their understanding of

privacy policies and a mechanism for ICBC to monitor their adherence to privacy policies through sign-off on a regular basis.

Recommendation: We recommend that ICBC establish a policy requiring individual external defence counsel members to sign-off on ICBC's privacy policies and acknowledge their acceptance, understanding, and compliance with them on annual basis.

Observation 7: Privacy Considerations in the External Defence Counsel Selection Process ( )

(Relates to Assessment Objectives 3.3)

Assessment Observation: We observed an opportunity for improvement in the external defence counsel selection process whereby ICBC selects external defence counsel law firms for performing ICBC claims litigations. We observed that the selection criteria did not address privacy considerations such as privacy incidents or breaches resulting from the law firm. Although such incidents are accounted for when contracting with a law firm, the selection criteria does not directly address privacy considerations.

Recommendation: We recommend that as part of the counsel selection process, privacy considerations be accounted for. Such considerations may include the number of privacy breaches, or the percentage external defence counsel who have not acknowledge privacy policies or completed privacy awareness program provided by ICBC.

Detective controls

Detective controls are measures in place to identify instances of non-compliance with organizational policies and procedures. This includes regular monitoring of controls, identification of incidents and a process for handling instances of non-compliance. Effective detective controls act as a deterrent to individuals who seek to intentionally violate established corporate policies.

Summary of controls in place

H. Privacy Incident Reporting
(Relates to Assessment Objective 5.3)

The Information and Privacy department has channels for customers and employees to report privacy incidents and complaints. Customers are informed on how to contact ICBC with privacy complaints either through ICBC personnel or through ICBC publication notices. Customers can make privacy complaints directly through their claims adjuster or through the Customer Relations department. For ICBC publication notices, contact information to the Information and Privacy department is available on the ICBC website and in the "we're listening" brochure.

I. Privacy Incident Response Protocol
(Relates to Assessment Objective 5.4, 5.5)

The Information and Privacy department has an established set of protocols which are followed for handling privacy complaints and incidents. This same protocol is used for handling complaints and incidents raised by customers, employees, or third parties such as external defence counsel. This protocol includes procedures for investigating, tracking, documenting, and resolving privacy complaints and incidents. When a potential incident or complaint has been identified or made, the protocols are to:

- **Record the Complaint** – Privacy complaints and potential incidents are forwarded to the Information and Security department. Once received, the complaint is entered into the Feedback Tracking System (FTS) which logs and tracks the complaints. Every complaint or incident is logged and given a file number and an individual from the Information and Privacy department is assigned to the file. Details of the complaint or incident such as the description of the complaint, the division affected, the impact to personal information, and remediation actions are recorded.

- **Activate the Privacy Incident Response Team** – For small complaints or incidents that can be resolved quickly, the Information and Privacy department would work with the affected divisions to resolve the issues. For larger complaints or incidents, the Privacy Incident Response Team is activated. The degree of activation and the size of the team depend on the seriousness of the incident. The severity of a complaint or incident is based on criteria such as the prospect of harm to the individual, the liability to the corporation, and the advice of OIPC.
- The Privacy Incident Response Team may be comprised of individuals from Information and Privacy, Corporate Communications, Information Risk Management, Employee Relations, Legal, or business areas affected. The main responsibility of this team is to contain the breach, investigate the incident, ensure appropriate communication to affected parties and management, and develop recommendations for corrective action.
- **Perform and Conclude on the Investigation and Make Recommendations** – The investigation stage is coordinated by the Information and Privacy department and may include investigative resources from Employee Relations and Information Risk Management (IRM). Evidence such as audit logs, data dumps from phone records, cell phone records, emails, and mainframe may be obtained for investigation by IRM. After sufficient investigation is performed, employee interviews are conducted by Employee Relations to further the investigation. Based on the evidence, a conclusion of either "founded" or "unfounded" is made at the end of the investigation. For founded complaints or incidents, the appropriate notifications are made, efforts are made to contain the breach, recommendations are made to improve existing practices, and employee sanctions are recommended. Sanctions may range from a letter of expectation to suspension or termination.
- **Notify OIPC and Individuals Affected** – Once a complaint or incident has been confirmed, the appropriate individuals affected by the breach are notified. In addition, the OIPC is notified depending on the seriousness and nature of the breach.
- **Reporting and Trending of Past Incidents** – The Information and Privacy department is responsible for identifying trends of past privacy complaints and incidents. Reports are generated from the Feedback Tracking System which contains all privacy complaints. Serious incidents are reported to executives at the bi-weekly issues meetings. In addition, trending to industry surveys based on the types of incidents is performed on an ad-hoc basis. This trending analysis of privacy complaints is reactive, but may lead to increased training or initiatives in particular areas of the business. An example of this would be the broker privacy initiative which was launched as a result of increased incidents of missing or stolen files at broker offices.

Observations and Recommendations

Observation 8: Proactive Identification of Privacy Issues (!)

(Relates to Assessment Objectives 4.3, 5.4)

Assessment Observation: We observed that ICBC has not implemented controls to proactively identify privacy policy violations by ICBC employees or external defence counsel. Although reporting and trending of privacy incidents are performed by the Information and Privacy department on an ad-hoc basis, more regular proactive self-assessments of compliance with privacy policies would assist in identifying areas which require increased awareness or training. In addition, awareness of proactive monitoring initiatives would also act as a deterrent for non-compliance.

Recommendation: We recommend that regular reviews of ICBC claims adjusters and external defence counsel activities are conducted to identify potential inappropriate activities. Such review may involve conducting self-assessments or the review of IT system audit logs. Conducting self-assessments such as a survey with generic privacy questions to claims adjusters or external defence counsel may assist in identifying privacy violations and training gaps individuals may have. This survey may include different privacy scenarios and provide additional awareness in areas where privacy violations are a concern. This type of surveying may lead to further investigations in areas of concern. In addition, review of IT system audit logs through reporting of specific activity or criteria may also assist in identifying potential inappropriate activities. At the time of our assessment, it was noted that discussions have been underway on proactive identification of audit logs by the Information Risk Management department.

Deloitte

Proud to be the Official Supplier of Professional Services to
the Vancouver 2010 Olympic and Paralympic Winter Games

1858 150 2008
Deloitte celebrates
150 years of professional service

50 BEST EMPLOYERS IN CANADA 2009
REPORT ON BUSINESS

www.deloitte.ca

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 7,700 people in 57 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. Deloitte is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

APPENDIX 2

ICBC Internal Investigation Report

Corporate Audit Services

REVIEW OF ICBC's INVESTIGATION INTO INAPPROPRIATE ACCESS OF JURY CLAIMS INFORMATION

Distribution:

David Loukidelis, Information and Privacy Commissioner for B.C.
James K. Burrows, Portfolio Officer, Office of the Independent Privacy Commissioner of BC

Prepared by: M. Burnett
Contact: L. Lewicki

2009-PAS

October 5, 2009

EXECUTIVE SUMMARY

Corporate Audit Services (CAS) reviewed the internal investigation conducted by the Claims division to determine if the April 2009 incident, in which the claims history of jurors was inappropriately accessed, was an isolated event or the extent to which this practice was being used by adjusters and defence counsel. For the period of review, January 2000 to June 2009, Claims management identified approximately 500 claims resolved by jury trials. The investigation revealed five additional confirmed incidents from 2000 to 2007.

Given ICBC's obligations under the *Freedom of Information and Protection of Privacy Act* (FIPPA), even one incident where personal information is inappropriately accessed and disclosed is unacceptable. It is this focus on compliance with privacy legislation that drove ICBC to conduct a comprehensive investigation into the treatment of juror information.

INCIDENT BACKGROUND

On April 27, 2009 ICBC defence counsel (the law firm) requested from ICBC claims information on jurors in the trial. Contrary to ICBC's corporate policy and Code of Ethics, as well as the Litigation Management Strategy manual that ICBC issues to all defence counsel, the ICBC adjuster provided that information to defence counsel.

ICBC management immediately implemented its Privacy Incident Response protocol which involved informing others, investigating the cause of the breach and making recommendations to prevent a recurrence. The incident response team consisted of members from Claims Field Services, Employee Relations, Corporate Law and Privacy and Freedom of Information departments. The incident response team reported the breach to the court, terminated defence counsel, sanctioned the employee and informed the Office of the Independent Privacy Commissioner (OIPC). ICBC also apologized to the jurors, in writing, and worked with the court and plaintiff counsel to ensure the plaintiff's claim was not impacted by the breach.

OIPC INVESTIGATION SCOPE

On May 25, 2009 ICBC's Board of Directors asked the Minister responsible for ICBC for an independent audit into the access, use and disclosure of personal information in the conduct of ICBC court proceedings involving juries. The Minister asked the OIPC to undertake this audit with the mandate to focus on "court proceedings involving juries since the *Freedom of Information and Protection of Privacy Act* came into effect (1993), including any instances where court proceedings were settled before going to trial but where the jury was selected or about to be selected, where information is practicably available".[1]

[1] Letter from David Loukidelis, Information and Privacy Commissioner for British Columbia dated May 27, 2009

ICBC INVESTIGATION OBJECTIVE, SCOPE AND APPROACH

The OIPC is conducting an audit to address the Minister's request. ICBC initiated an investigation to determine whether the April 2009 incident was isolated or the extent to which this practice was being used by adjusters and defence counsel within ICBC's Claims division.

The year 2000 was selected as a starting point for this review because the Claims division implemented a new database system to record settlement and litigation information that year and this database provided the best and most practical way of identifying a complete population of jury trials. In addition, in 2000 the Litigation Management Strategy (LMS) was updated to include a reference prohibiting jury checking. The LMS outlines ICBC's expectations of its Claims staff and defence counsel with respect to handling litigated claims. ICBC expects all Claims staff and defence counsel to be familiar with its contents.

Therefore, ICBC's investigation focused on claims resolved by jury and settled after January 1, 2000 to June 2009.

ICBC committed to perform a thorough investigation of this and any other similar incidents. This entailed using multiple processes to identify prior jury cases and cross checking the accuracy of the information, as jury trials were not tracked prior to January 1, 2008. These processes involved:

- Review of all jury trials conducted by the law firm involved in the initial incident;
- Interviews of all current ICBC staff working on litigated files in the Claims division;
- Interviews of all current defence counsel who conducted jury trials in 2008 and 2009; and,
- Review of all identified claim files that involved jury trials from 2000 to June 2009.

CAS' review of the investigation included:

- Gathering documentation of the investigation process;
- Interviewing relevant staff about the process; and,
- Identifying areas for management to conduct further investigation and provide additional documentation.

CAS verified the accuracy of the investigation statistics reported and ensured that the investigation processes, including supporting documentation, were complete.

INVESTIGATION

To what extent did the law firm make jury checking requests?

The law firm provided ICBC with claim file numbers for six jury trials (other than the initial April 2009 incident) that they had conducted since 2000. Claims division management reviewed these files for documentation to indicate whether jury checking took place. Claims staff had already been interviewed. These procedures identified another incident of jury checking for a 2006 trial. The adjuster had been requested by the law firm to access the claims files of the eight jurors. Defence counsel had already been terminated as a result of the initial incident. No action was taken against the former employee who was not employed by ICBC at the time of the investigation. The OIPC confirmed that ICBC did not have to notify the jurors as there was no evidence that information was disclosed to defence counsel and access occurred after the trial ended.

To what extent was jury checking done by ICBC Claims staff?

On May 19, 2009 the VP Claims Field Services directed all Claims Centre Managers to interview Claims staff who handle litigated files. A total of 1037 interviews were completed; 14 interviews are outstanding for staff who are on long term or maternity leave. The interviews were conducted with scripted questions and identified three additional incidents that were subsequently confirmed. Two occurred in 2000 and one in 2006. In response, ICBC disciplined the Claims staff, terminated defence counsel contracts and issued notification letters to the jurors in one of the incidents. In the other two cases, the OIPC confirmed that ICBC did not have to issue letters to the jurors. In one instance it was not possible to determine if the information had been disclosed to defence counsel, and in the other instance it was not possible to obtain juror addresses.

To what extent were jury checking requests made by external defence counsel?

ICBC's Special Counsel department interviewed the 87 external defence counsel lawyers who had conducted jury trials on ICBC's behalf in 2008 and 2009. For consistency, scripted questions were used in all interviews. No additional incidents were identified.

For any litigated claims files that resulted in a jury trial (2000 to 2009), was jury checking done?

Concurrently with the Special Counsel department's interviews of defence counsel, several Claims managers reviewed the 70 litigated claims files that resulted in jury trials since 2008. The file reviews confirmed the results of the defence counsel interviews as no additional incidents were identified.

ICBC's Senior Legal Counsel examined 16 claims files identified from a manual file search of ICBC's Fraud Assessment Committee logs. No additional incidents were identified.

Also, Claims management conducted an extensive data search on the ICBC's claims systems to identify the claims files with jury trials that occurred prior to January 2008. To validate the results of the search criteria, the search included all jury trials from 2000 to June 1, 2009. Claims files which had already been identified and reviewed through one of the previous processes were removed from this list. As a result of the data search, 786 claims files were identified as potential jury trials.

Managers from the Claims Quality Review Team reviewed these claims files which resulted in one additional confirmed case from 2007.

CONCLUSIONS

The Claims investigation was extensive to ensure that all possible approaches and methods were explored to identify ICBC's jury trials and therefore any potential additional instances of jury checking. While the various approaches did result in some overlap by identifying the same claims files, they also served to validate and ensure that, to the best of ICBC's ability, all jury trials were identified. We are satisfied that no additional steps could be carried out to capture any jury trials not already identified.

For the period of review, January 2000 to June 2009, Claims management identified approximately 500 claims resolved by jury trials. Five additional confirmed incidents from 2000 to 2007 were identified through the investigation. Therefore, for those jury trials conducted by ICBC for the period 2000 to 2009, the investigation revealed that the April 2009 incident was not an isolated event, however it also identified that the practice was not common across the Claims division.

Susan Lucas
Director Risk Management & Corporate Audit Services

Lynn Lewicki
Manager Corporate Audit Services

APPENDIX 3

ICBC Internal Investigation Report — Details Summary

Corporate Audit Services

REVIEW OF ICBC's INVESTIGATION INTO INAPPROPRIATE ACCESS OF JURY CLAIMS INFORMATION

Claims Investigation Detail Summary

Distribution:

David Loukidelis, Information and Privacy Commissioner for B.C.
James K. Burrows, Portfolio Officer, Office of the Independent Privacy Commissioner of BC

Prepared by: M. Burnett
Contact: L. Lewicki

2009-PAS

October 5, 2009

Claims Investigation Detail Summary **Date: October 5, 2009**

This document is the Detail Summary to the *Review of ICBC's Investigation into Inappropriate Access of Jury Claims Information* (Summary Report) that was provided to external readers under separate cover. The Detail Summary should be read with the Summary Report as it contains details on the scope, objectives and outcome of the investigation.

Claims Investigation Detail Summary

Claims Investigation
Overall Objective: To determine if the April 2009 incident was an isolated event or a common practice for claims files involving jury trials.

1. Initial Incident – April 2009 Objective: To document the circumstances relating to the first confirmed incident of jury checking.		
Incident Overview	Results	CAS Assessment
Incident facts: • Prior to trial commencing, Defence Counsel (DC) emailed the adjuster requesting background information on the 8 jurors in the trial and whether or not they had ICBC claims. The adjuster responded by email with information on all 8 jurors, 2 of which had prior ICBC claims. The adjuster accessed records for all 8 jurors on the ICBC database. • The incident was revealed through discussions at the claim centre between the adjuster, manager, and claims centre manager. • ICBC's Corporate Law department informed the court and Plaintiff's counsel. Appearances were made before the Honourable Mr. Justice Macaulay, who dismissed the jury. • After disclosing the issue to plaintiff's counsel a settlement was reached. • System access logs confirmed the nature of jurors' personal information that was accessed (e.g.: claims history).	Incident 1 (2009) • Notify and report to OIPC. • Contract with DC firm terminated. • All open files which were assigned to the law firm re-assigned to other DC. • Adjuster was disciplined. • Letters of notification/ apology sent to 6 of 8 jurors • Current address of 2 jurors could not be reasonably found. OIPC agreed that no further work was required to locate these jurors.	• No further work required.

Claims Investigation Detail Summary

2. Claims Employees
Objective: To identify and interview all Claims staff involved in litigated files to determine if they had accessed jurors' claims files.

Scope	Method	Results	CAS Assessment
• Interviews cover period from 2000 forward (the Litigation Management Strategy (LMS) with the prohibition on jury checking went into effect in Q4 2000). • Confined to existing claims employees who would be involved with litigated files • Some former claims staff came forward to self report. Limitations • Former claims staff still working for ICBC not interviewed. Through the HR system it's possible to identify staff that have held claims positions, however the HR system cannot identify if staff have worked on litigated files. • Limitations accepted as other processes in #5 & #6 below will identify individuals who did not come forward.	• Claims Management interviewed current Claims staff involved in litigated files to determine if they had accessed information with respect to a juror since 2000. • Scripted questions were used and each employee was provided with a copy of the Code of Ethics Use and Confidentiality of Information provision, a copy of the Corporate Policy on information disclosure (Release of Information Policy) and section 10.10.1 of the Litigation Management Strategy. • Results recorded on spreadsheet. • If employee disclosed potential incident, then: 1. Interview continued without script to obtain additional information for further investigation. 2. Information reported to Claims Management. 3. If Claims Management confirms incident: a. Privacy & Freedom of Information department (P&FOI) notified. b. P&FOI created case file for each incident, recorded incident and notified OIPC either through written incident report or by phone. Phone calls followed up with an incident report which may be for individual incidents or include more than one incident. c. System access logs run to confirm access for P&FOI review. d. Employee Relations notified. They participated in further interviews and recommended disciplinary action to Claims Management and the VP Claims.	• Employee interviews resulted in 3 confirmed incidents which were addressed as follows: Incident 2 (2006) • Adjuster & Manager disciplined. • External Defence Counsel's (DC) senior counsel terminated and all files assigned to DC were transferred out of firm. • External DC's junior counsel terminated with 90 days notice. All files assigned to junior counsel to be transferred within the firm. • Letter of apology/ notification sent to jurors. Incident 3 (2000) • Adjuster disciplined. • DC contract with external firm terminated with 3 months notice. • Jurors not notified – not possible to identify since file had been destroyed according to ICBC document retention policy. Incident 4 (2000) • Adjuster retired – no recourse. • Two Office Assistants disciplined. • No action against DC – no direct evidence that DC requested, received or used information. • Jurors not notified, not able to confirm data was disclosed. Decision confirmed with OIPC.	• No further work required.

Claims Investigation Detail Summary

3. Defence Counsel – 2008 – 2009 Jury Trials
Objective: To interview all defence counsel firms representing ICBC in 2008-2009 to determine if they had requested jury checking.

Scope	Method	Results	CAS Assessment
• All engagement lawyers (primary counsel) at defence counsel (DC) firms representing ICBC in jury trials in 2008 & 2009. • Secondary counsel at the same law firm was identified from other records and included in the scope. • Exception was made for one large law firm with most lawyers handling ICBC cases. All lawyers in the firm were interviewed. • DC were asked about all cases they conducted back to 2000 (or when they were hired) as many DC have worked for ICBC for many years. • Excluded lawyers from the initial law firm – addressed in #4 below.	• ICBC Special Counsel department interviewed, by phone, all engagement lawyers who conducted jury trials in 2008 and 2009 for ICBC. • Scripted questions were drafted and modeled after the questions used for claims employees. • Results recorded on a spreadsheet by Special Counsel. • If potential incident indicated, then: 1. Interview continued without script to obtain additional information for further investigation. 2. Information reported to Claims Management. 3. If incident confirmed: a. Privacy & Freedom of Information department (P&FOI) notified. b. P&FOI created case file for each incident, recorded incident and notified OIPC either through written incident report or by phone. Phone calls followed up with an incident report which may be for individual incidents or include more than one incident. c. System access logs run to confirm access for P&FOI review. d. Employee Relations notified. They participated in further interviews and recommended disciplinary action to Claims Management and the VP Claims.	• No additional incidents were identified.	• No further work required.

Claims Investigation Detail Summary

4. Review of all initial law firm files
Objective: To review all jury trials conducted by law firm involved in initial investigation on behalf of ICBC since 2000 to determine if there were other instances of jury checking.

Scope	Method	Results	CAS Assessment
• 6 jury trials were identified by the law firm. • 2 paper files were destroyed in accordance with ICBC records retention policies as the trials occurred in 2001 and 2002 and were therefore unavailable for review. Reviews of the electronic files were conducted.	• Claim files were retrieved and reviewed for reference to a jury trial. • Files for two claims were reviewed online. • If potential incident indicated, then: 1. Claims Manager would interview staff involved. 2. Information reported to Claims Management. 3. If incident confirmed: a. Privacy & Freedom of Information department (P&FOI) notified. b. P&FOI created case file for each incident, recorded incident and notified OIPC either through written incident report or by phone. Phone calls followed up with an incident report which may be for individual incidents or include more than one incident. c. System access logs run to confirm access for P&FOI review. d. Employee Relations notified. They participated in further interviews and recommended disciplinary action to Claims Management and the VP Claims.	Incident 5 (2006). • Defence Counsel contract terminated as a result of initial incident. • Employee had already left ICBC. • Jurors not notified as no evidence information was disclosed to DC and access occurred after the trial. Decision confirmed with OIPC.	The law firm identified trials that ICBC's data run did not identify. These claims files did not meet the data extract search criteria. CAS is satisfied that these were uncommon practices and do not significantly affect the review results. No further work is required.

Claims Investigation Detail Summary

5. Claims Files – Jury Trials 2008 – 2009
Objective: To review all claims files that had a jury trial in 2008 and 2009 for reference to jury checking.

Scope	Method	Results	CAS Assessment
• Included jury trials in 2008/2009 based on the Provincial Trial Log (PTL) which was implemented January 1, 2008. Limitations • Entire claims files not reviewed as any documentation pertaining to a trial would appear around trial time at the end of the file documentation. • PTL may be incomplete as it relies on manual data entry. The Claims system does not have a field to capture whether a file goes to jury trial or not so unable to easily run a list of all jury trial files. System Accuracy Check • In order to determine the accuracy of the PTL, the Claims Managers reviewed each file listed in the PTL for their offices to ensure they were correctly identified as jury trials. Some errors were noted and corrected. • The corrected PTL was used to help refine the search criteria for the data extract in #6 below.	• Identify the 70 jury trials conducted in 2008/2009 based on the PTL. • Review the 70 claims file for reference to jury checking. Consisted of review of the paper file, electronic notes, correspondence & legal notes. • Files reviewed by a team of 8 Claims managers. • Each manager tracked results in a separate Excel spreadsheet. Completed spreadsheets consolidated and reviewed by Claims Management.	No additional incidents were identified from the file reviews.	• No further work required.

Claims Investigation Detail Summary

6. Data Extract – Jury Trials
Objective: To identify claims files with jury trials prior to June 1, 2009 and to review those claims files for references to jury checking.

Scope	Method	Results	CAS Assessment

Population
• All claim files with a jury trial prior to June 1, 2009. Includes ICBC as defendant and plaintiff.
 	
Sample
• Data search resulted in list of 1367 claims.
• The Claims Quality Review Team (CQRT) initially reviewed these files through electronic system notes to validate the search results and confirm which files had jury trials. Resulted in identification of claim files requiring further review.
• Head Office Claims (HOC) provided a list of 96 jury trials from their manual records that encompass trials from 1998 to 2009. The list of 70 claim file numbers on the Provincial Trial Log (PTL) was also added to the list.
• The combined list was sorted by claim number in order to remove any duplicate claim numbers and resulted in a list of 786 files requiring further review.
• Jury trials where ICBC is plaintiff were picked up by the data run, however there were a small number of files that were paid under a bulk payment and were not identified by the data run.
  o Bulk payments are for non claims specific payments for agencies such as BC Ambulance, lien searches, and the courts. Some of these cases would not have been attributed to a specific claim so would not have been paid through a claim.
  o A manual review of the trial logs identified 21 files where the trial was either trial by jury, or where billing records indicated that the matter may have involved a jury at some point in the course of proceedings. Five files on the list were identified as never involving a jury; these were excluded from the review.
  o The remaining 16 files were reviewed.
 	
Limitations:
• Jury trials in which plaintiff paid jury fees would not be captured by data search (these are rare).
• Excluded files previously identified in #5 above or as
	• Data was extracted from ICBC systems. Several data searches were executed and the criteria refined with each search.
	• The data search was first performed through the litigation system to select claims resolved by jury and settled after Jan 1/00. The search generated a list of claims with jury trials. The jury trials occurring in 2008 were compared to the list of jury trials occurring in 2008 per the PTL. This comparison showed that some files listed on the PTL were not included in the data extract.
	• The search was refined using the claims system database to filter for payments to the Minister of Finance (MOF). The resulting list was compared and reconciled to the PTL and based on the results of the reconciliation the search criteria was further refined to capture additional MOF payments under another payment code. Physical files were reviewed unless the file had been destroyed due to exceeding the retention period.
	• When paper files had been destroyed, review consisted of electronic notes only.
	• Related files that were identified in the course of the review were also reviewed with the results recorded in the record of the original file.
	• Results of reviews were recorded and compiled by the CQRT.
	• If potential incident indicated, then:
	  1. Information reported to Claims Management.
	  2. Privacy & Freedom of Information department (P&FOI) notified.
	  3. P&FOI created case file for each incident, recorded incident and notified OIPC either through written incident report or by phone. Phone calls followed up with an incident report which may be for individual incidents or include more than one incident.
	  4. System access logs run to confirm access for P&FOI review.
		• No incidents identified from the bulk payment files.
		• Data extract file reviews resulted in one confirmed incident:
		
		Incident 6 (2007)
		• Claims employee was disciplined.
		• Defence counsel no longer works on ICBC cases (DC did not participate in current ICBC contract with DC firms); therefore there is no recourse against the firm.
		• Jurors will not be notified since access occurred after jury was selected and no evidence that information provided,
			No further work required.

6. Data Extract – Jury Trials **Objective: To identify claims files with jury trials prior to June 1, 2009 and to review those claims files for references to jury checking.**			
Scope	Method	Results	CAS Assessment
confirmed incidents.	5. Employee Relations notified. They participated in further interviews and recommended disciplinary action to Claims Management and the VP Claims. • The data search resulted in one incident which was confirmed through the system access logs. 1. Employees interviewed using scripted questions. 2. ICBC Special Counsel department to interview Defence Counsel for any trials in which a jury list was provided and / or where the results of the employee interviews warrant further investigation. 3. Report results to Claims Management. 4. Employee Relations to participate in further interviews and recommend disciplinary action. • The bulk payment files were reviewed and results recorded in a spreadsheet 1. The review consisted of a review of the physical files, soft copies of documents, all email correspondence relating to each file, as well as counsel billings for each matter to determine if there was any reference to jury selection 2. The review focused on the time period just prior to and during the actual trial dates, rather than reviewing the entire file		

APPENDIX 4

ICBC's Response to Report Recommendations

building trust. driving confidence.

October 7, 2009

Mr. David Loukidelis
Information and Privacy Commissioner
3rd Floor - 756 Fort Street
POB 9038 Stn.Prov. Gov't
Victoria BC V8W 9A4

Dear Mr. Loukidelis:

Re: Investigation Report F09-01: Investigation into Disclosure of Jurors' Personal Information by the Insurance Corporation of British Columbia - October 2009

Thank you for providing us with a copy of your report. ICBC appreciates your thorough review of our privacy policies and procedures.

ICBC did not and does not condone the practice of jury checking. Although we had policies in place to prohibit jury checking, these isolated incidents did occur. ICBC immediately disclosed the policy breach when we became aware of it.

We have learned from this unfortunate situation and will improve our privacy practices because of it. We agree with your findings and conclusions and are implementing your recommendations for improvement.

Privacy will always continue to have a significant place in the governance of ICBC.

Yours truly,

Jon Schubert
President and CEO