Office of the
Privacy Commissioner
of Canada

AUDIT OF
SELECTED MORTGAGE BROKERS

Section 18 of the *Personal Information Protection and Electronic Documents Act*

FINAL REPORT

2010

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 947-1698, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190
Follow us on Twitter: @privacyprivee

Cat. No. IP54-32/2010
ISBN 978-1-100-51559-5

This publication is also available on our website at **www.priv.gc.ca**.

Table of Contents

Main Points

WHAT WE EXAMINED

From July to December 2008, 14 mortgage brokers notified the Office of the Privacy Commissioner of numerous breaches of personal information affecting hundreds of people. A privacy breach is the loss of, unauthorized access to, or disclosure of personal information as a result of a compromise of an organization's security safeguards. As all of these reported breaches occurred in Ontario, we audited five mortgage brokers based in that province. They were selected on the basis of the number of persons affected, the occurrence of multiple breaches or the nature of the breach.

We examined privacy policies and procedures that are in place and mortgage application forms in use. We conducted physical inspections of the mortgage brokers' offices, and evaluated measures in place to secure the brokers' physical premises. We examined the information technology systems as well as the controls around how credit reports are accessed from credit agencies by mortgage brokers.

WHY THIS ISSUE IS IMPORTANT

Mortgage brokers represent a large and growing segment of the mortgage industry in Canada. Brokers and their agents regularly obtain, use and disclose personal information during the course of their work. In order to assess creditworthiness and suitability for mortgage products, the industry relies on credit reports obtained from credit-reporting agencies via a web-based tool.

There were two common conditions surrounding the breaches that were reported to our Office. First, an individual, posing as a legitimate mortgage agent, was able to obtain employment at each of the mortgage brokerages we audited. Second, the fraudulent agent gained access to the web-based credit-reporting tool and obtained hundreds of credit reports unrelated to mortgage applications.

WHAT WE FOUND

We found that brokers have significantly strengthened their hiring processes in the wake of these breaches. As well, the mortgage brokers proactively reported the breaches to our Office. However, we found that mortgage brokers are unable to demonstrate that there are adequate security safeguards in place to protect the personal information under their control. Documents, including mortgage application files, credit reports and other sensitive material, were not always stored securely. We also found that mortgage brokers did not have adequate systems and tools in place to help ensure credit reports were not being accessed inappropriately.

Although most brokers we audited have privacy policies in place, they were not always detailed enough to clearly state their information-handling practices or indicate how they are meeting their privacy obligations under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), nor were the policies always accessible to their clients. We found that a client's consent is not always obtained prior to a credit report being obtained, and that some brokers used client's information for purposes other than that for which it was collected.

We found that mortgage brokers do not always dispose of unapproved mortgage application files in a timely and secure fashion. Furthermore, our audit revealed that mortgage brokers and their agents are not fully aware of their roles in protecting the personal information under their control, and they have not received adequate training on their privacy responsibilities. In the absence of comprehensive privacy policies and procedures, and clear accountability for their implementation, none of the brokers we audited fully meet their PIPEDA obligations to protect the personal information of their clients and others.

The four out of five brokers that we audited that are still in business have responded to and accepted all of our recommendations. Their responses are included in Appendix A.

Introduction

ABOUT MORTGAGE BROKERS

1. Mortgage brokers represent a large and growing segment of the mortgage industry in Canada. A survey commissioned by the Canada Mortgage and Housing Corporation revealed that in 2009, mortgage brokers accounted for 25% of all mortgage transactions and 44% of transactions undertaken by first-time homebuyers. Brokers and their agents offer products, rates and terms for individuals seeking mortgages, and act as intermediaries between individuals and lenders, including banks and credit unions.

2. Mortgage brokerages can be franchises affiliated with a head office while remaining independently owned and operated, employing agents who can work from the brokerage office or their homes. They can also be single, independent operations, unaffiliated with another brokerage. For the purposes of this audit, the term "mortgage broker" refers to the franchisee or principal broker. Mortgage brokers fall under the jurisdiction of the province in which they operate. In Ontario, both brokers and agents are authorized to provide mortgages. The *Mortgage Brokerages, Lenders and Administrators Act, 2006* prohibits agents from dealing in mortgages except under the supervision of a broker. As well, given that these Ontario-based mortgage brokers collect, use and disclose personal information in the course of commercial activities, they are subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

3. Brokers and agents collect personal information from individuals through the mortgage application process which can include, but is not limited to, name, address, telephone numbers, date of birth, Social Insurance Number (SIN), marital status, dependants, employment information, income, assets and liabilities. To assess an individual's eligibility for a mortgage, mortgage brokers and agents access a credit-reporting agency's database via a third-party provider's web-based tool. This tool allows mortgage brokers and their agents to manage the entire mortgage application process, to obtain credit reports, to send applications to lenders and to secure mortgage financing.

HUNDREDS OF CREDIT REPORTS WERE INAPPROPRIATELY ACCESSED

4. From July to December 2008, 14 mortgage brokers in Ontario notified the Office of the Privacy Commissioner (OPC) of numerous breaches of personal information affecting hundreds of people. In all cases, an individual impersonating an experienced mortgage agent downloaded credit reports, using the third-party provider's web-based tool, for his own use. These breaches are the subject of ongoing police investigations.

5. The brokers discovered the suspected theft of credit reports in one of three ways:

   - when an individual consulted his/her credit report and subsequently alerted the broker;
   - when a mortgage broker received an unusually large invoice for credit reports; or
   - when credit-reporting agencies contacted the brokers to report suspicious activity.

6. Credit reports contain extensive personal information. These are attractive to criminals as they can be used to commit identity theft or identity fraud.

7. Under section 18 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the Privacy Commissioner of Canada has the power to audit an organization where the Commissioner has reasonable grounds to believe there is non-compliance with the *Act*. Accordingly, the Privacy Commissioner assessed the facts surrounding the privacy breaches and determined that reasonable grounds existed to undertake an audit of the personal information-handling practices of selected mortgage brokers.

FOCUS OF THE AUDIT

8. Five Ontario-based mortgage brokers were audited, as all the breaches occurred in that province. They were selected based on the number of persons affected, the occurrence of multiple breaches or the nature of the breach. The audit objective was to determine whether selected mortgage brokers in Ontario have developed and implemented policies and procedures to protect the personal information of their clients and others. Information on the scope, criteria and approach can be found in the **About the Audit** section of this report.

9. The audit does not focus on the management of personal information about mortgage brokers, mortgage agents or employees. It focuses on customer's, client's or other individual's information. In addition, credit-reporting agencies were not examined as part of this audit. As section 18.(1)(d) of PIPEDA precludes us from conducting audit activities in dwelling houses, we were unable to assess activities performed by agents who work out of their homes. Finally, we did not audit the third-party provider of the web-based credit-reporting tool.

Credit reports may contain

- name, address, date of birth and, possibly, Social Insurance Number;
- a listing of any organization that has requested a copy of the credit file within a specific amount of time;
- information on secured loans, bankruptcies and/or judgments;
- past and present debts, including those which have been forwarded to a collection agency; and
- a history of credit transactions and payments.

Observations and Recommendations

SAFEGUARDING PERSONAL INFORMATION

10. One of the main reasons why the breaches occurred at the mortgage brokers we audited was that there were inadequate systems and controls in place to ensure credit reports were not accessed inappropriately. Organizations subject to PIPEDA are required to protect personal information by implementing security safeguards that are proportionate with the sensitivity of the information held. Consequently, mortgage brokers must have sufficient physical, technical and administrative controls in place to safeguard the personal information of their clients and others.

11. We examined policies and procedures, agreements, process-flow documents and IT systems. We conducted physical inspections of the mortgage brokers' offices. We also tested the controls around how credit agencies' credit reports are accessed by mortgage brokers via a third-party provider's web-based tool.

Physical security of brokerages is at varying levels of sophistication

12. Given the sensitivity of the personal financial information used, we examined whether the mortgage brokers had undertaken to define threats, evaluate the associated risks, and recommend mitigating actions to address the identified vulnerabilities. None of the brokers we audited had undertaken these activities, which are also referred to collectively as a "Threat and Risk Assessment."

13. A Threat and Risk Assessment is used to identify and mitigate weaknesses in processes and systems. This type of assessment helps mortgage brokers determine an acceptable minimum level of security required to safeguard the information. We found varying levels of security among the five mortgage brokers we audited. For example:

    - not all mortgage brokers had alarm systems to protect their places of business. One broker who did not have an alarm system informed us that an adjacent business had been burgled;
    - the majority of brokerages we examined had solid, secure walls on the perimeters of the suites that ran from the ground to the floor above, although one did not; and,
    - none of the brokers we examined had solid walls on the interior of their premises. Rather, all brokerages had floor-to-ceiling interior walls that could expose them to unauthorized access from neighbouring offices via the crawlspace between the ceiling and the floor above.

14. Undertaking this type of assessment, and acting on the recommendations, can assist brokers in meeting their safeguarding obligations under PIPEDA. In the absence of a Threat and Risk Assessment, the mortgage brokers we audited were unable to demonstrate that they had identified and mitigated security risks.

Inconsistencies in document storage

15. According to the Generally Accepted Privacy Principles of the Canadian Institute of Chartered Accountants, physical safeguards may include the use of locked filing cabinets, card-access systems,

physical keys, sign-in logs and other techniques to control access to offices, data centres and other locations in which personal information is processed or stored.

16. As previously mentioned, mortgage application files contain sensitive personal information that should be stored securely. We found a mix of storage practices within brokerages. For example, some brokers we examined used secure filing cabinets while others stored files in unlocked cabinets or stacked files openly on the floor or on desks within accessible offices. We also noted that one broker had overflow storage in the unsecured parking arcade of the building in which the brokerage was located which could result in a breach of personal information. We noted that another broker had arranged to have all inactive/closed mortgage files stored off-site with a third-party document storage company accredited under the National Association for Information Destruction.

17. During our interviews with staff regarding security measures, we were informed that mortgage application files may be housed in a broker's home, and that agents may also retain in their homes copies of mortgage applications that had not been approved. The security of files outside the mortgage broker's premises could not be verified as some brokers/agents kept copies of files at their home offices, the examination of which falls outside the scope of this audit.

18. In addition to paper files, all brokers we examined keep copies of electronic files, including mortgage applications, credit reports and spreadsheets. Although the computer network systems we examined required users to log in and were using virus protection software, none had been tested for vulnerabilities to ensure that adequate protection was in place.

Access to credit reports is not adequately controlled

19. Mortgage brokers and agents use a web-based tool to obtain credit reports for the purpose of assessing creditworthiness for mortgage products. The breaches reported to the OPC occurred when mortgage agents downloaded hundreds of credit reports that were not required for mortgages. The breaches at issue involved someone impersonating a mortgage agent who downloaded an excessive number of credit reports that was well beyond the norm. This activity went unnoticed for some time. Had the mortgage brokers put in place adequate controls to prevent unauthorized use of the web-based tool, the risk of inappropriate access to credit reports could have been mitigated.

20. We tested the tool used to access credit reports and found that there are controls in place to authorize access to the credit-reporting system. Although the system was encrypted and required a login password, there is no capacity for mortgage brokers to proactively monitor and receive alerts when suspicious activity is occurring, or to place limits on how many credit reports can be downloaded.

21. These types of controls are used by a number of organizations including those that provide employees with corporate credit cards. They enable organizations to monitor purchases, set spending limits and track spending with customizable reports, thereby reducing the possibility of fraud.

22. Currently, the only way for mortgage brokers to become aware of inappropriate access to the credit-reporting system is to review computer log files, which record information on credit reports that are accessed by a specific login identifier. However, a log file review is a retrospective measure. Further, brokers do not have the capability to limit access to the number of credit reports that can be downloaded.

23. We also found during our testing that when a credit report is accessed, a duplicate of the credit report remains in the requesting computer's "temporary" folder. Unless the contents of this folder are deleted, the credit report will remain on the computer.

24. Although we were not made aware that this vulnerability had resulted in a breach of personal information, this could pose a serious risk if computers are shared, if credit reports are accessed on public computers (e.g., in an Internet café or public library), or if agents use shared home computers to run credit reports.

25. As well, when these computers are disposed of, unless hard drives are properly and adequately overwritten, the credit report data will remain intact and could be accessed by anyone who acquires the computer or hard drive.

26. RECOMMENDATION

The mortgage brokers we audited should ensure they have in place security safeguards appropriate to the sensitivity of personal information in their control. This includes, but is not limited to, ensuring that

- adequate physical measures are in place, such as alarms and lockable filing cabinets; and
- additional controls are put in place to safeguard credit reports and limit the number that can be downloaded.

IDENTIFYING PURPOSE, COLLECTION, CONSENT, USE, RETENTION AND DISCLOSURE

27. Organizations subject to PIPEDA are required to comply with the principles set out in Schedule 1 of PIPEDA regarding the collection, use and disclosure of personal information. Mortgage brokers are required to

    - clearly identify the purposes for the collection of personal information before or at the time of collection;
    - obtain consent for the collection, use and disclosure of personal information;
    - limit the information being collected to the minimum required to meet the identified purposes;
    - use and disclose the personal information only for the purpose for which it was collected; and
    - retain personal information only for as long as necessary.

28. To determine the extent to which mortgage brokers are meeting these obligations, we examined privacy policies to verify whether they addressed the appropriate privacy principles under Schedule 1 of PIPEDA. This includes whether they clearly listed the type of personal information collected, how it is used (including how it is safeguarded), with whom it is shared, when it is disposed of and who is responsible for ensuring the broker's privacy policy is followed. We conducted interviews with mortgage brokers and carried out site visits at their offices. We also examined mortgage applications and consent agreements for privacy protection clauses. Finally, we reviewed the procedures in place to see how privacy policies are implemented.

Privacy policies not always sufficiently detailed

29. Organizations subject to the *Act* are required to implement policies and practices based on the 10 privacy principles listed in Schedule 1 of PIPEDA. Two of the brokerage head offices we audited had very detailed privacy policies posted on their websites. These two policies covered the 10 privacy principles, addressed information management in some detail and included contact information for the Chief Privacy Officer, to whom questions could be addressed.

30. By contrast, another broker we examined had a privacy policy posted on its website, but it lacked sufficient detail for individuals to understand how the mortgage broker managed its personal information. For example, no mention was made of the 10 privacy principles, or how its client's personal information would be used. Although their policy states that the organization is "committed to keeping your personal information confidential," no specifics are included. Moreover, during the course of our audit, we noted that the link to the privacy policy from the broker's "terms of service" page did not function.

31. Only two of the brokers we audited had a formal privacy policy that addressed the 10 privacy principles included in their policies and procedures manuals; however, the policy was not posted on the brokers' websites, nor was it made available to clients. All of the brokers we audited used either a "privacy protection client consent" or "privacy agreement" form that their clients are required to sign acknowledging that they consent to the use of their personal information. For the three brokers that did not have formal privacy policies, the only reference to privacy and protection of personal information appeared in the "privacy protection client consent" or "privacy agreement" forms. However, these forms were not detailed enough to clearly state their information-handling practices or indicate how they meet their privacy obligations under the *Act*. Furthermore, when we reviewed the files at the companies in question, we found that brokers did not consistently use these forms.

Purpose of collection is clearly identified but not all information is required for a mortgage application

32. To fulfill their client-identification obligations under the *Mortgage Brokerages, Lenders and Administrators Act, 2006* mortgage brokers and agents in Ontario must collect personal information. Mortgage brokers require their clients to fill out mortgage application forms. These forms state that the personal information collected will be used to obtain a credit report and for securing mortgage financing.

33. We found that the types of information brokers collected to verify a potential client's identity may include a driver's license, birth certificate and Social Insurance Number (SIN). Mortgage brokers use other documents to assess a potential client's financial situation, including Canada Revenue Agency "T4" forms and bank statements. The lending institutions stipulate what documentation the brokers are required to obtain from the clients before a mortgage is funded.

34. The mortgage application forms did not state that the provision of the SIN is optional. We found that the SIN was consistently collected by all mortgage brokers and agents on these application forms. We found that the SIN is frequently used by agents and brokers to differentiate between clients with similar names. However, a SIN is not required to conduct a credit check. Further, there is no legislative requirement for the SIN to be collected for this purpose. The OPC is of the view that the SIN should not be used as a general identifier and organizations should restrict the collection, use and disclosure of the SIN to legislated purposes only.

Consent is not always obtained before personal information is collected

35. PIPEDA requires the knowledge and consent of individuals for the collection, use and disclosure of their personal information. In order for consent to be meaningful, PIPEDA requires that the purposes for the collection, use and disclosure of personal information be clearly stated to the individual. The form of consent can vary, but PIPEDA requires that express consent be sought when the information is sensitive.

36. Mortgage brokers should only collect what is required and obtain their client's express and meaningful consent prior to obtaining credit reports and providing personal information to potential lenders. We found that although brokers require their clients to give their written consent for brokers to access credit reports, in cases where transactions are not conducted face to face, agents obtain consent verbally and have clients provide written consent after the credit report has been accessed. However, in some cases we noted that credit reports were obtained prior to consent having been recorded, and in others, we found no record of consent ever having been obtained.

Clients cannot opt out of secondary uses of personal information

37. In order to obtain a mortgage for their clients, mortgage brokers and agents are required to disclose a client's personal information to credit-reporting agencies and to lenders. Any additional use of their information (such as for marketing purposes) should be clearly stated in the mortgage application and consent forms. In accordance with PIPEDA, mortgage brokers should obtain express (opt-in) consent when using personal information for marketing purposes.

38. We examined all broker's consent forms and found that they allow the brokers to use the personal information collected for marketing and other secondary purposes. Three mortgage brokers we audited informed us that some personal information (name and telephone number) may be shared with real estate agents, financial planners and other service providers as a "sales lead." We also found the consent forms allow all the mortgage brokers we audited to use the personal information collected from their clients for marketing purposes, which could include sending clients newsletters and mailing out birthday greetings. The consent forms we examined do not allow clients the clear choice of opting out of secondary uses of their personal information.

Unapproved mortgages should not be retained for longer than necessary

39. The *Mortgage Brokerages, Lenders and Administrators Act, 2006* requires mortgage brokers to retain all records related to a mortgage for at least six years after the expiry of the term of the mortgage. Since this obligation came into effect in 2006, the brokers we examined did not have any records which met this requirement.

40. We note, however, that mortgage consent forms frequently state that files may be kept for specific periods of time, even if a mortgage was not approved by a lender. We found that four of the audited brokers' Client Consent and Privacy Protection forms state that the agents "can retain and use" the applicant's personal information for seven years after the last application was made. One of these four brokers has a policy that requires it to destroy unapproved mortgage application within six months. We examined the files of this broker and found that this policy was not followed. The fifth audited broker's form states that the retention period is three years.

41. Mortgage brokers were unable to demonstrate why they needed to retain unapproved mortgage applications for such a long period of time. If brokers are retaining personal information in anticipation of a new use, PIPEDA requires that new consent be obtained.

Disposal practices need to be strengthened

42. We also assessed how brokers disposed of records that had not resulted in mortgages being issued. While we observed that all brokerages had shredders, with one exception they were all strip-cut shredders and as such, do not adequately destroy documents that contain personal information. We also did not find evidence that shredders were used consistently, nor could we confirm that brokers and agents who retained files in their homes disposed of them safely. The OPC has issued guidance regarding identity theft wherein we recommend the use of cross-cut shredders to destroy all documents with personal or financial information.

43. We noted one case where a broker had reused old mortgage applications that contained the personal information of another client. These applications were then fed into printers and new applications printed on their reverse sides. This practice could result in the personal information of a client being shared with someone who has no need to know.

44. RECOMMENDATION

The mortgage brokers we audited should

- not routinely collect and retain personal information, such as Social Insurance Numbers, unless necessary to fulfill a specific and specified purpose and/or in accordance with the law;
- be able to demonstrate that clients have consented to the collection of their personal information. Furthermore, brokers should make clients aware of all potential uses and disclosures of their personal information and seek express consent for secondary uses of their personal information; and
- develop and implement policies and procedures regarding the retention of personal information. These should specify that unapproved mortgage application files and other files that contain personal information should be securely destroyed within a reasonable amount of time.

RESPONSIBILITY AND ACCOUNTABILITY FOR PRIVACY

45. Organizations subject to PIPEDA are responsible for the personal information in their control. PIPEDA requires that organizations that collect personal information establish clear responsibility for privacy. To ensure these responsibilities are understood by brokers, agents and clients alike, mortgage brokers are required to have clearly defined who within their organization is responsible for protecting personal information and ensuring compliance with PIPEDA.

46. To assess compliance, we examined mortgage broker's privacy policies, documentation surrounding responsibility for privacy (where available) and assessed breach reporting practices. We looked at hiring practices for new agents, interviewed agents and consulted training material provided by broker's head offices and by the mortgage broker and agent-training providers.

Mortgage brokers lack awareness of privacy roles

47. We have noted that many institutions that handle personal information—including banks, insurance companies and service-based industries among others—have a Chief Privacy Officer (CPO) as a point of contact for all privacy-related matters. Given that personal financial information is collected by mortgage brokers, all brokers are required to have identified an individual responsible for

    - ensuring that they and their staff are adequately trained regarding their privacy obligations;
    - identifying and mitigating privacy risks;
    - implementing ongoing monitoring for compliance with PIPEDA; and
    - seeing that existing policies and procedures are adequate and functioning as intended.

48. While all brokers we examined had designated a CPO, we noted a lack of understanding of the responsibilities of the role, and that not all agents were aware of either who the CPO was, or to whom they should turn if they had privacy-related questions or experienced a breach of personal information.

49. For example, we found that one broker we audited has a CPO; however, the position is located at the head office, not at the franchise level. The head office's policy is quite clear that, since brokerages are independently owned and operated franchises, the company disclaims responsibility for the privacy practices of their brokers.

50. Another broker states in its privacy policy that they have appointed a CPO to ensure franchisee compliance with privacy responsibilities. However, when we interviewed this franchisee and asked who the CPO was, we were informed the CPO was located at the head office. However, an examination of the policy manual revealed that the CPO was, in fact, the broker/owner. We conclude from this that there is a lack of clarity regarding roles and responsibilities for privacy.

Brokers and agents are not trained on their privacy responsibilities

51. PIPEDA requires employees to be educated about privacy practices and policies. It also stipulates that employees must understand their roles in implementing such policies and be able to communicate them. The *Mortgage Brokers, Lenders and Administrators Act, 2006* requires mortgage brokers and agents to undertake specific training concerning the provision of mortgages. While we found that brokers and agents had undertaken this mortgage training, no agents from the mortgage broker companies that we audited had been provided with formal and ongoing training on company-specific privacy practices, or their responsibilities under PIPEDA.

Brokers proactively reported privacy breaches

52. A privacy breach is the loss of, unauthorized access to, or disclosure of, personal information as a result of a compromise of an organization's security safeguards pursuant to Schedule 1 of PIPEDA. Privacy breaches can happen when the personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed (e.g., a computer containing personal information is stolen or personal information is mistakenly sent to the wrong people). However, a privacy breach may also be a consequence of a faulty business procedure or operational breakdown. In this instance, the breaches were the suspected theft of hundreds of credit reports.

53. Although PIPEDA does not place any specific requirements on an organization with respect to privacy breaches, the OPC has issued guidance to organizations in this regard in which we note that breach notification demonstrates good privacy practices and builds trust in your brand. The guidance document outlines four steps to consider when responding to a breach or suspected breach: (1) breach containment and preliminary assessment; (2) evaluation of the risks associated with the breach; (3) notification of those affected; and (4) prevention of recurrence.

54. None of the mortgage brokers we audited had formal breach-reporting policies in place at the time of the suspected thefts. However, the mortgage brokers we audited were proactive and contacted our Office to determine how to contain and mitigate the breaches, and also notified those affected by the breach. During the course of our audit, one of these brokers developed a formalized breach-reporting policy.

Post-breach hiring processes are more stringent

55. We found that mortgage brokers have tightened up their hiring processes significantly following the breaches that were reported to our Office. As of July 1, 2008, the *Mortgage Brokerages, Lenders and Administrators Act, 2006* requires that all individuals and businesses that conduct mortgage-brokering activities in Ontario be licensed by the Financial Services Commission of Ontario (FSCO), the provincial agency responsible for overseeing the mortgage brokerage industry. To obtain a license, brokers and agents must take a course, pass an examination, undergo a criminal background check and fulfill certain other requirements established by the FSCO.

56. Prior to the breach, brokers informed us that they relied heavily on interviews, the applicant's knowledge of the business and references, and did not necessarily contact lenders with whom the applicant had dealings. One broker also informed us that it did not always confirm the applicant's FSCO licensing status.

57. After the breach, one brokerage implemented a practice of having a regional manager from the broker's headquarters meet all prospective employees and having a senior manager from headquarters approve all new hires. This same brokerage requires that all agents be members in good standing of the Canadian Association of Accredited Mortgage Professionals. Another broker informed us that it has implemented a practice of only hiring people whom staff know personally. Two brokers we audited are now verifying all references.

58. Many brokers also restrict access by new hires to credit-reporting software. One broker would not permit a new agent to access credit-reporting software until they have worked for the company for a minimum of 90 days; another confirmed that an agent's access to credit reports would be evaluated upon completion of five mortgage applications.

59. RECOMMENDATION

The mortgage brokers we audited should

- clearly establish who is responsible for privacy training and monitoring compliance with PIPEDA;
- develop and implement privacy policies and procedures to ensure compliance with PIPEDA principles, including developing information to explain the organization's information-handling policies and procedures;
- ensure their staff are trained on company-specific privacy policies and procedures, as well as on their responsibilities under PIPEDA; and
- ensure that mortgage brokers and clients are aware of and can readily access privacy policies.

Conclusion

60. Mortgage brokers make extensive use of personal information to provide mortgage products for their clients. PIPEDA requires that brokers be responsible for safeguarding the information collected and protecting against unauthorized access to it. These breaches came about as the result of mortgage brokers not fulfilling their obligations under PIPEDA. They did not put adequate controls in place to restrict access to credit reports and hiring processes were not sufficiently rigorous.

61. Since the breach occurred, mortgage brokers have significantly tightened their hiring practices. However, the mortgage brokers that we audited cannot demonstrate that the physical security of their premises or the controls surrounding access to credit reports is adequate.

62. We identified vulnerabilities in the web-based tool through which credit reports are obtained. The breaches reported to the OPC occurred when mortgage agents downloaded hundreds of credit reports that were not required for mortgages. We tested the tool used to access credit reports and found that while there are controls in place to authorize access to the credit-reporting system, there is no capacity for mortgage brokers to proactively monitor and receive alerts when suspicious activity is occurring, or to place limits on how many credit reports can be downloaded. Had these controls been in place to prevent unauthorized use of the web-based tool, the risk of inappropriate access to credit reports could have been mitigated.

63. We did not consistently find clear accountability for, training on, and knowledge of privacy at the brokers we audited. In the absence of comprehensive privacy policies and procedures, and clear accountability for their implementation, none of the brokers we audited fully meet their PIPDEA obligations to protect the personal information of their clients and others.

About the Audit

AUTHORITY

Section 18 of PIPEDA empowers the Privacy Commissioner to undertake an audit of the personal information- management practices of an organization if she has reasonable grounds to believe that a contravention of the *Act* is occurring.

OBJECTIVE

The audit objective was to determine whether selected mortgage brokers in Ontario have developed and implemented policies and procedures to protect the personal information of their clients and others.

CRITERIA

We expected the mortgage brokers we audited to have implemented policies and processes that comply with the requirements of the collection, use, retention and disclosure principles established under Schedule 1 of PIPEDA (A complete list of principles we considered while conducting this audit is included as Appendix B). Specifically, PIPEDA requires that

- the purpose of collection be identified at or before the time of collection;
- consent of the individual be obtained prior to collection, use or disclosure of personal information;
- the collection of personal information be limited to that which is necessary for the purposes identified by the broker;
- personal information be used and/or disclosed only for the purposes for which it was collected, except with the consent of the individual or as required by law; and
- personal information be retained only as long as necessary.

As per the requirements of the Safeguards Principle under PIPEDA, the mortgage brokers we audited are required to have appropriate measures in place to protect the personal information under their control.

Finally, in accordance with the Accountability Principle under PIPEDA, mortgage brokers are required to have

- developed and to regularly review privacy policies;
- developed and implemented a privacy breach reporting mechanism;
- defined roles and assigned responsibilities for privacy compliance throughout the organization, including privacy training; and
- established a means to monitor their compliance with PIPEDA.

SCOPE AND APPROACH

The audit began with a survey of the practices and procedures of the mortgage broker industry across Canada. This included discussions with the Canadian Association of Accredited Mortgage Professionals and the Independent Mortgage Broker's Association, and a review of a sampling of files from the three mortgage brokers being audited that had reported a breach to our office.

Of the 14 mortgage brokers that reported a breach to our office, we examined the policies, systems, administrative controls and safeguards implemented by five mortgage broker franchises located in Ontario, as well as at national brokers' head offices located in Toronto and Vancouver. These brokers were selected on the basis of number of people affected, the nature of the breach and the type of brokerage. We interviewed staff and reviewed relevant policies and procedures, agreements, process-flow documents, records-retention documents, training materials, IT systems and a sampling of mortgage files from all brokers.

We met with representatives from the Financial Services Commission of Ontario to get a clearer idea of the regulatory environment in which mortgage brokers operate. We also met with a representative from the RCMP's Counterfeit and Identity Fraud, Commercial Crime Branch to obtain an overview of the circumstances in which the breaches arose. Finally, we held a teleconference with one of the instructors in charge of providing training for mortgage brokers and agents, and reviewed the course material.

The audit work was substantially completed on December 31, 2009.

STANDARDS

The audit work was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner, and followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants.

AUDIT TEAM

Director General: Steven Morgan

Leslie Fournier-Dupelle
Garth Cookshaw
Michael Fagan
Bill Wilson

Appendix A

RECOMMENDATIONS AND RESPONSES

RECOMMENDATION

The mortgage brokers we audited should ensure they have in place security safeguards appropriate to the sensitivity of the personal information in their control. This includes, but is not limited to, ensuring that

- adequate physical measures are in place, such as alarms and lockable filing cabinets; and
- additional controls are put in place to safeguard credit reports and limit the number that can be downloaded.

Mortgage Broker 1 has accepted this recommendation, and committed to storing all completed client files, whether approved and funded or not funded, in locking steel file cabinets. Agents have been advised that any files they are working on at home are to be stored in a secure location until returned to the office. In addition, agents do not have access to credit reports. Instead, they must request that the principal broker obtain the report for them after having obtained a signed client consent form. Finally, the broker has committed to advising all agents that viewing a credit report creates a new file in their temporary Internet files folder, and that this should be cleared after viewing a report.

Mortgage Broker 2 has accepted this recommendation, and will ensure that all files are stored in a locked cabinet located in a private office in the building with access limited to the principal broker only. In addition, the broker has centralized responsibility for credit reports so that only one person has access to the credit-reporting tool.

Mortgage Broker 3 has accepted this recommendation, and confirmed that its current offices have locks on all doors, along with a locked filing cabinet and locked desk cabinets where all files are stored. The broker intends to implement a "clean desk" policy. With respect to the credit-reporting tool, the broker confirmed that it monitors all agents by randomly checking their credit bureau "pulls" and tool-transaction history. New agents will not be allowed to download credit reports until they have worked for the company for 90 days and finalized four mortgage applications that have been supervised by the principal broker. Finally, all agents are being sent a supplementary form to be attached to the broker/agent contracts advising that they must empty their "temporary files" computer folders daily as they may contain private client information. This form will have to be signed and kept on file.

Mortgage Broker 4 has accepted this recommendation, and committed to ensuring that all files, once completed, will be secured in locked filing cabinets. In addition, the broker confirms that all computers are password protected and are set up to delete temporary files automatically. The broker stated that the building is monitored 24/7 by over 30 cameras. During non-business hours, the building is also monitored by security guards, and pass cards are required to access entrances and each floor of the building. The broker has also committed to installing cameras and an alarm system within the next six months that will be monitored off-site 24/7. Although all agents can download credit reports via the web-based tool,

the broker has implemented a policy restricting access for all new agents until they have worked for the company for a period of 90 days. Finally, the broker is currently reviewing the possibility of having a central person conduct credit checks.

RECOMMENDATION

The mortgage brokers we audited should

- not routinely collect and retain personal information such as Social Insurance Numbers unless necessary to fulfill a specific and specified purpose and/or in accordance with the law;
- be able to demonstrate that clients have consented to the collection of their personal information. Furthermore, brokers should make clients aware of all potential uses and disclosures of their personal information and seek express consent for secondary uses of their personal information; and
- develop and implement policies and procedures regarding the retention of personal information. These should specify that unapproved mortgage application files and other files that contain personal information should be securely destroyed within a reasonable amount of time.

Mortgage Broker 1 has accepted this recommendation, and acknowledges that it routinely collects personal information from applicants for the purpose of fulfilling their borrowing requests, which can include Social Insurance Numbers. The broker explained that the SIN is frequently requested by the lenders to ensure the credit report has been obtained on the correct person. In addition, the broker has confirmed the SIN is required by some lenders as part of the approval process to confirm whether the applicant is a non-permanent resident. With respect to the matter of consent, the broker confirms that all applicants sign a mortgage application which includes their consent to collecting personal information for the purpose of the application. The broker ensures that clients also consent to receiving periodic mortgage and real estate-related direct marketing materials. Finally, the broker committed to clarify its privacy guidelines to ensure that unapproved mortgage application files are securely destroyed within six months.

Mortgage Broker 2 has accepted this recommendation, and stated that these requirements have been implemented since the audit examination work was conducted. The broker stated that although it is using the standard consent forms from the credit-reporting tool, it will look into providing the capacity to "opt out" of secondary uses of personal information. Once these practices are implemented, the broker has committed to ensure that training will be ongoing, and that files will be reviewed weekly for accuracy and to ensure compliance with policies.

Mortgage Broker 3 has accepted this recommendation, and will ensure that the mortgage application form is amended to reflect that the collection of the SIN is optional. When applications are taken over the phone, the broker committed to verbally informing clients that it is optional to provide the SIN. The broker has committed to ensuring that this policy is included in all training forms distributed to agents. The broker has implemented a policy whereby all unapproved mortgage files are shredded within a week, and all other files are secured in a locked steel filing cabinet. In terms of consent, the broker stated that their software program has the ability to document the date, time and method of consent (e.g., verbal) given by the client. When obtaining verbal consent for credit reports, the broker will ensure that all clients sign a consent form after the fact confirming that they did give consent to access their credit report.

Mortgage Broker 4 has accepted this recommendation, although with respect to the SIN, it confirms that it is the safest way to ensure that the correct credit report is accessed. Before a credit report is obtained, the broker commits to ensuring that all clients sign

consent forms that clearly indicate how personal information will be used, and with whom it will be shared. This form will be updated to include a clear "opt in" function giving clients more control regarding secondary disclosures. The broker confirms that all unapproved or withdrawn paper applications are now shredded within 30 days, and all paper files older than three years are securely destroyed. Finally, the broker stated that it no longer reuses mortgage applications as scrap paper.

RECOMMENDATION

The mortgage brokers we audited should

- clearly establish who is responsible for privacy training and monitoring compliance with PIPEDA;
- develop and implement privacy policies and procedures to ensure compliance with PIPEDA principles, including developing information to explain the organization's information-handling policies and procedures;
- ensure their staff are trained on company-specific privacy policies and procedures, as well as on their responsibilities under PIPEDA; and
- ensure that mortgage brokers and clients are aware of and can readily access privacy policies.

Mortgage Broker 1 has accepted this recommendation, and confirms that the broker is responsible for the company's privacy policies, training and compliance. The broker stated that the policies and procedures manual, which is provided to and reviewed with each agent, includes guidelines to protect the privacy of client information. The broker confirmed these guidelines were fully discussed with each agent, and that privacy compliance is regularly emphasized in the course of business. The broker committed to reviewing and updating these guidelines within 30 days to reflect the recommendations in this report. Specifically, the broker committed to broadening agent training to provide more clarity regarding personal privacy responsibilities. To do so, the broker stated they will use the resources on the Office of the Privacy Commissioner's website, and will require each agent to acknowledge that they are aware of both the company's privacy guidelines and their personal responsibilities.

Mortgage Broker 2 has accepted this recommendation, and has recently hired a training and compliance officer to train staff on their privacy responsibilities. The broker has committed to working diligently to ensure proper privacy procedures are followed at all times.

Mortgage Broker 3 has accepted this recommendation, and will take responsibility for privacy training and monitoring compliance with PIPEDA. The broker committed to being available to all agents and clients for any privacy questions or concerns, and to developing a privacy policy and procedures manual to ensure compliance with PIPEDA. This manual will be made available to agents, who will be required to agree to follow the procedures outlined in it. In addition, the procedures manual and privacy policy will be posted on the broker's website, and a print version will be made available to clients.

Mortgage Broker 4 has accepted this recommendation, and committed to ensuring that all agents are trained on privacy compliance and are monitored on an ongoing basis. The broker is in the process of developing a manual for all agents outlining their responsibilities under PIPEDA. The brokerage privacy policy is posted on its website. Finally, the broker stated that it is in the process of updating policies and procedures to reflect the recommendations in this report and this will be completed within six months.

Appendix B

PRINCIPLES UNDER SCHEDULE 1 OF PIPEDA CONSIDERED DURING THIS AUDIT

4.1 PRINCIPLE 1 — ACCOUNTABILITY

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

(a) implementing procedures to protect personal information;

(b) establishing procedures to receive and respond to complaints and inquiries;

(c) training staff and communicating to staff information about the organization's policies and practices; and

(d) developing information to explain the organization's policies and procedures.

4.2 PRINCIPLE 2 — IDENTIFYING PURPOSES

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1

The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 PRINCIPLE 3 — CONSENT

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 PRINCIPLE 4 — LIMITING COLLECTION

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 PRINCIPLE 5 — LIMITING USE, DISCLOSURE, AND RETENTION

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

4.5.1

Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.7 PRINCIPLE 7 — SAFEGUARDS

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).