ALBERTA
OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

Report of an Investigation into the Collection of Personal Information

February 16, 2010

Mark's Work Wearhouse Ltd.

Investigation Report P2010-IR-001

I. INTRODUCTION

[1] An individual ("the Complainant") had applied for a Sales Associate ("SA") position at one of Mark's Work Wearhouse Ltd.'s ("MWW" or "the Organization") corporate stores. During the Complainant's in-person interview with the Organization he was asked to sign a declaration of understanding and consent for a "security clearance check" and "credit check" which he did. The Complainant was advised that the Organization would contact him about his employment status.

[2] A few hours after the interview, the Complainant received a telephone call from a MWW Human Resources Representative ("Representative") for an explanation of the Complainant's credit rating and how he was resolving his credit issue. The Complainant told the Representative that in the past an error in processing his paper work between the federal government and his bank concerning his student loans had occurred. He stated that due to a lack of financial resources he could not resolve the matter.

[3] Subsequently, the Complainant submitted a complaint to the Office of the Information and Privacy Commissioner ("Commissioner") that the collection of his credit information was not reasonable given the job requirements of a MWW SA.

[4] In response to this complaint, the Commissioner elected to conduct an investigation to determine whether the Organization's activities represented a contravention of Alberta's *Personal Information Protection Act* ("PIPA" or "the Act"). I have now completed my investigation into this matter. This investigation report sets out my findings and recommendations.

II. JURISDICTION

[5] Section 36 of the Act empowers the Commissioner to conduct investigations to ensure compliance with any provision of PIPA and make recommendations to organizations regarding their obligations.

[6] PIPA applies to provincially-regulated private sector organizations operating in Alberta, including MWW, a wholly owned subsidiary of Canadian Tire Corporation, Limited ("CTC"). The Commissioner has jurisdiction in this case because MWW is an "organization", as defined in section 1(i) of the Act, and operates in Alberta.

[7] MWW engaged the services of Allison and Associates (2001) Inc. ("A & A"), a third party security consultant, to conduct pre-employment background checks for MWW. As such, section 5(2) of PIPA applies. This section states:

> *5(2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act.*

[8] Pursuant to section 5(2) of the Act, MWW is responsible for A & A's compliance with PIPA when A & A provides services on behalf of MWW that involve the collection, use or disclosure of personal information. Consequently, this business relationship requires both MWW and A & A to comply with the Act.

[9] Pursuant to section 49 of PIPA, the Commissioner authorized me to investigate this matter. This report outlines my findings and recommendations which may be made public according to section 38(6) of the Act.

III. INVESTIGATION

[10] In conducting this investigation, I spoke with the Complainant and reviewed the written complaint. I spoke with MWW's Privacy Advisor, as well as the Manager of Customer Service Safety and Security and the CTC Legal Counsel, Risk Management and Compliance Services. I reviewed MWW and CTC's written response to the Complainant's allegations. Their response included a copy of MWW's security clearance and credit check process instructions for store operators, the security clearance check form, the credit check form, the criminal check matrix, MWW's recruitment process flowchart, the applicant questionnaire-pre-screen application, the SA job description, and the Organization's security and crime prevention booklet.

CTC and MWW's Response to Complaint

[11] CTC acquired MWW in February 2002. MWW operates 339 stores across Canada under MWW and Work World brands, and the L'Equipeur brand in Quebec. Of these 339 stores, 290 are corporate stores which are operated and staffed by MWW employees, and 49 are franchise stores which are independently owned and operated. The MWW store where this complaint originated is a corporate store location which implements MWW's standard operating policies and procedures.

[12] In 1996/97 MWW implemented a "Security and Crime Prevention Program" ("the Program") in all its corporate store locations to enhance security measures and prevent in-store theft. The Program's procedures are outlined below.

- Employees are prohibited from processing their own sales, return or exchange transactions. All such transactions must be completed by the manager on duty (Store Operator, Assistant Store Operator or Key-Holder (Shift Leader);
- No unauthorized person is to be given access to any cash terminal;
- Small amounts of cash are to be kept in the cash terminals. To reduce potential losses, the manager on duty will transfer excess cash from the terminals to the store safe every 2.5 hours for high sales volume stores and every 4 hours for low sales volume stores.
- Employees who visit the store on days when they are not scheduled to work are not permitted to enter the back office or stock room areas. Further, the manager on duty must be notified when an off-duty employee is in the store;
- Cash desks must be kept tidy and clear at all times to ensure visibility throughout the store; and
- All waste disposal must be inspected by the manager on duty before it leaves the store. This process requires that all boxes must be flattened and includes a visual inspection of all bags.

[13] During the implementation phase of the Program, all corporate store employees were provided with a copy of the MWW Security and Crime Prevention Booklet, which outlines the program and procedures as described above.

[14] In 2003/04 MWW introduced a mandatory requirement that all new and existing employees read the MWW Security and Crime Prevention Booklet and sign an acknowledgement form confirming that they had read and understood its contents and agreed to abide by its terms.

[15] In April 2005, CTC launched a business conduct hotline and website reporting service for all MWW corporate stores for employees to use to anonymously report business conduct issues (including in-store thefts) that they witnessed or believe may have occurred.

[16] MWW installed closed circuit television cameras in 68% of its corporate store locations. The Organization's intent with these cameras was to prevent external theft; however, it was thought that their presence might also act as a deterrent against employee in-store theft.

[17] As a result of the Program, management gained more awareness of the occurrence of in-store theft and fraud. As part of this investigation MWW provided statistics concerning the number of in-store theft and fraud investigations conducted on an annual basis along with the total dollars lost since September 2003, when a formal log of employee theft and fraud was established. These statistics are:

Year	# of in-store thefts and fraud	Total $ lost as a result of in-store thefts and fraud
Sept 2003 – 2004	54	$98,400
Sept 2004 – 2005	60	$60,550
Sept 2005 – 2006	59	$61,552

[18] MWW stated that there was a decrease in the total dollars lost on an annual basis since the implementation of the Program; however, there was no significant decrease in the rate at which incidences were occurring. Consequently, MWW considered and implemented a pre-employment credit check process in September 2006, for all SA positions, in an effort to reduce in-store theft and fraud.

[19] MWW provided the following statement regarding the purpose of its pre-employment credit check.

> *Credit history information can provide insight into an applicant's tendency to meet financial obligations as well as his or her current financial pressures. The way in which individuals handle their own funds can often be a reflection of how they will handle the financial responsibilities and tasks associated with their employment duties. SAs at Mark's are often in a position to handle cash while completing merchandise transactions and depending on their level of hire may also have access to the store safe (which may contain 2 or 3 days worth of deposits), security codes, petty cash and the store*

itself during off hours. Performing credit checks at the pre-employment stage allows Mark's to ensure that applicants who may be under financial strain are not in a position to commit theft or fraud.

[20] MWW reported that since implementing the pre-employment credit check in September 2006, the Organization has completed 3,445 credit checks for corporate store SA applicants. The Organization has investigated a total of 53 cases related to credit and debit card fraud, theft of customer personal information, theft of deposits, and theft from fellow employees with a total dollar loss of approximately $43,000. Of those 53 cases investigated, two incidents involved employees who had completed and successfully proceeded through the credit check process. MWW noted that these two employees had both been flagged by the MWW Manager of Customer Service, Safety and Security as potential risks due to their credit rating scores. However, these employees performed well in their interview process and were cleared for hire based on the recommendations of the store operator.

[21] MWW advised that it engaged the services of A & A to conduct all pre-employment background checks. These background checks include a security clearance check and a review of an applicant's credit history. With respect to the credit check, A & A acquires the applicant's credit report from a credit reporting agency, and then provides the full credit report directly to the MWW Manager Customer Service, Safety and Security ("the Manager"). The credit reports received by the Manager include the North American Standard Account Ratings system which is a credit rating scale as outlined below:

RO – Too new to rate; approved but not used;
R1 – Pays (or paid) within 30 days of payment due date or not over one payment past due;
R2 – Pays (or paid) in more than 30 days from payment due date, but not more than 60 days, or not more than two payments past due;
R3 – Pays (or paid) in more than 60 days from payment due date, but not more than 90 days, or not more than three payments past due;
R4 – Pays (or paid) in more than 90 days from payment due date, but not more than 120 days, or not more than four payments past due;
R5 – Account is at least 120 days overdue, but is not yet rated "9";
R6 – This rating does not exist;
R7 – Making regular payments through a special arrangement or settle your debts re: O.P.D. or Proposal;
R8 – Repossession (voluntary or involuntary return of merchandise);

R9 – Bad debt; placed for collection; moved without new address, bankruptcy.

[22] MWW reported that applicants who have received a credit score of R7-R9 are classified as high risk and are required to have their credit history undergo a further review by the Manager to determine whether the applicant is an acceptable hire. The Manager reviews all factors which contribute to an applicant's overall credit score such as filing for bankruptcy, involvement with past collection agencies and patterns of bad debt. Upon completion of the review, the Manager advises the Store Operator or hiring Manager as to whether the applicant has been "cleared" or "not cleared" for hire. If the applicant has received a "not cleared" for hire rating, the Store Operator generally does not proceed with hiring the applicant; however, if the applicant scored well in the interview process, an MWW Staffing Specialist will ask the applicant to provide further explanation about his or her credit rating and the action taken to resolve the credit issue. MWW advised that this step provides further insight into the applicant's level of financial responsibility based on the steps that have been initiated by the applicant to correct his or her credit issue.

[23] When applicants are hired, the results of the background check are forwarded to the MWW Human Resources Department for inclusion in the employee's personnel file. For applicants that are not hired, the Manager retains the records in a locked cabinet for three months after which time they are shredded.

[24] MWW advised that applicants with no credit history are categorized as low risk. For these applicants, MWW relies on the results of reference and criminal background checks, along with the applicant's personal interview and online profile assessment in determining suitability for employment.

[25] MWW maintained that the privacy concerns of its employees and customers are important to CTC and MWW and the pre-employment credit check was studied carefully by its Risk Management and Compliance Division, prior to implementation.

[26] The primary role of a MWW SA is to generate sales and includes various areas of responsibility including communication, product knowledge, merchandising, administrative support, housekeeping, and supervision. The job description describes two areas of responsibility that relate to handling monies:

- Administrative Support – The SA will be able to process all cash related transactions; process Business Account transactions; assist in transfer checks, look up information in the style file, and view the inventory of other stores, for the purpose of maximizing sales opportunities.

- Supervision – May be required to act as a shift supervisor opening and/or closing the store and providing leadership to the team ensuring that sales and customer service standards are met.

IV. ISSUES

[27] The issues to be examined in the remainder of this report are as follows:

1. *Is the information at issue "personal information" or "personal employee information"?*

2. *Did MWW collect the Complainant's personal information in compliance with section 11(1) of PIPA?*

V. ANALYSIS

1. Is the information at issue "personal information" or "personal employee information"?

[28] Personal information is defined in section 1(k) of PIPA to mean "information about an identifiable individual." The information at issue in this case is the Complainant's credit history information collected by MWW from a credit reporting agency. Typically this information can include an individual's occupation and current and past place of employment, past and present addresses, marital status, spouse or interdependent partner's name and age, number of dependents, education or professional qualifications, estimated income and assets, existing debts and paying habits, fines and restitution orders, cost of living responsibilities, and enquires made by others.[1]

[29] In this case, the information is about an identifiable individual – the Complainant. Therefore, I find that the information at issue is personal information as defined in section 1(k) of PIPA and the Act applies to this information.

[30] However, personal information may also qualify as personal employee information within an employment context. Personal employee information is a subset of personal information and is defined in section 1(j) of the Act to mean:

> *"Personal employee information" means, in respect of an individual who is an employee or a potential employee, personal*

[1] Consumer Tip Sheet: Your Credit Report, Service Alberta, Consumer Services Branch, February 2007 (http://www.servicealberta.gov.a.ca/tipsheets/credit_report.cfm)

information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating

(i) an employment relationship, or
(ii) a volunteer work relationship

between the organization and the individual but does not include personal information about the individual that is unrelated to that relationship

[31] In determining whether the information at issue is "personal employee information" under PIPA, I considered MWW's purposes for collecting the Complainant's personal credit information. That is, whether MWW's collection of the Complainant's personal credit information was reasonably required by the Organization solely for the purposes of establishing an employment relationship between MWW and the Complainant**.** Section 2 of PIPA states that when determining whether anything or any matter is reasonable or unreasonable, the standard to be applied is what a reasonable person would consider appropriate in the circumstances. It states:

Where in this Act anything or any matter

(a) is described, characterized or referred to as reasonable or unreasonable,

or

(b) is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner,

the standard to be applied under this Act in determining whether the thing or matter is reasonable or unreasonable, or has been carried out or otherwise dealt with reasonably or in a reasonable manner, is what a reasonable person would consider appropriate in the circumstances.

[32] MWW advanced two purposes for the collection of the Complainant's personal credit information as follows:

1. Assessment of how applicants will handle financial responsibilities and tasks associated with their employment duties as a SA.

2. Assessment of whether the applicants have a probable risk of in-store theft or fraud.

Assessment of financial responsibilities as a SA

[33] MWW advanced that the collection of a job applicant's personal credit information provides "insight" into how an individual will handle the financial responsibilities of a SA. The Organization stated:

> *The way in which individuals handle their own funds can often be a reflection of how they will handle the financial responsibilities and tasks associated with their employment duties. SAs at Mark's are often in a position to handle cash while completing merchandise transactions and depending on their level of hire may also have access to the store safe (which may contain 2 or 3 days worth of deposits), security codes, petty cash and the store itself during off hours.*

[34] Prior to his application to MWW, the Complainant in this matter had 7 years retail experience in a position similar to a MWW SA. He asserted that a MWW SA position does not have discretionary power over allocation of cash and all monies that would be handled in this position would be thoroughly documented and closely supervised by management and monitored through the Organization's point of sale system.

[35] In reviewing this matter, I referred to Investigation Report #P2005-IR-008 published by this Office which involved a software company that conducted a credit check on an individual applying for a position as Administrative Assistant/Receptionist. One of the software company's purposes for the collection of the applicant's credit information in that case was to assess the applicant's suitability to manage petty cash, assuming that in most cases, an individual who can manage his or her own finances is better suited to manage the petty cash of the software company. [2]

[36] The investigator in the SAS Institute case found that the collection of the applicant's personal credit information was not reasonably required to determine the applicant's suitability to manage petty cash. She noted "that there may not necessarily be a correlation between an individual's ability to manage his or her own finances and an ability to do so on behalf of the organization". The investigator went on to say that an individual's personal credit problems could be "a result of factors beyond the individual's control" such as medical problems or periods of unemployment.

[2] SAS Institute (Canada) Inc. Investigation Report P2005-IR-008, Office of the Information and Privacy Commissioner of Alberta, available online at www.oipc.ab.ca

[37] Similarly, in this case, MWW asserted that the collection of the Complainant's personal credit information was reasonably required as an indicator of the applicant's ability to handle the financial responsibilities of a SA with the Organization. However, I am not persuaded that the Complainant's personal credit information is reasonably required for this purpose.

[38] An applicant's credit report, as pointed out by the investigator in P2005-IR-008, may be influenced by factors beyond the individual's control such as medical problems and periods of unemployment. An applicant may have the financial skills to perform a SA position with MWW, yet could be eliminated from the Organization's hiring process because of a negative credit rating beyond the applicant's control.

[39] Additionally, there are other factors which may create an inaccurate credit report unbeknownst to applicants who do not regularly review their credit report. Personal credit reports may be subject to inaccuracies submitted by creditors, identity theft, failure to correct errors and reinsertion of previously deleted credit information. These factors can create a credit report that is very damaging and, as a result, could eliminate a reliable and honest applicant from becoming a SA with MWW.

[40] Furthermore, in this case, there were less privacy intrusive means by which to assess the Complainant's abilities, such as making inquiries with his references about his skills and past performance in a related work environment and/or asking the Complainant, during an in-person interview, about his financial experience and responsibilities as a 7-year employee with a large retail organization.

[41] In a similar case involving the City of Vancouver & Canadian Union of Public Employees Local 15, Arbitrator Steeves analysed the collection and use of background checks for certain positions of the Union to determine whether the process was a reasonable collection and use of personal information.[3] The City of Vancouver's policy related to background checks stated that a "credit record check is used to determine whether an individual might be subject to outside financial pressures that could indicate an unacceptable risk in performing the duties of the designated position." With respect to criminal record checks, Arbitrator Steeves stated the following:

> I am not persuaded that, for example the *possibility* of outside financial pressures makes the collection of personal information through Police Record Checks necessary. A higher

[3] Arbitration Under the *Labour Relations Code*, R.S.B.C. 1996, City of Vancouver v. Canadian Union of Public Employees Local 15, November 12, 2007.

> standard than a possibility is required to demonstrate that the information is not being collected simply because it might be useful in the future or convenient. I appreciate that the Employer may well want to satisfy itself of the financial credentials of certain employees but information obtained from a police record is personal information protected by FOIPPA *(Freedom of Information and Protection of Privacy Act).* A direct relationship between the work and this personal information is required and I am unable to find that it is met by the Policy in this area.
>
> A related matter is that there may well be alternate, less intrusive and even more effective ways for the Employer to protect the risk of a breach of the financial trust they repose in some employees. I have in mind controls such as regular and/or random internal audits as well as reporting procedures and overall management responsibility. These controls may reasonably be part of an overall prevention policy in this area that includes a more focused policy on Policed Record Checks.

[42] I agree with Arbitrator Steeves' analysis that there must be a direct relationship between the duties and responsibilities of the position and the collection of personal information including personal credit information. In this case, it is my opinion that it is not reasonable to collect the Complainant's personal credit information to assess his ability to perform a job (SA) that requires day to day handling of monies, when the position is closely monitored by onsite supervision and the point of sale monitoring procedures prohibit employees from processing their own transactions. The type and amount of information in a personal credit report is not clearly and directly related to an individual's ability to handle financial responsibilities of a SA position, and there are other less privacy intrusive means available to assess an applicant's abilities.

[43] As such, it is my opinion that the Complainant's personal credit information was not reasonably required to assess how applicants will handle financial responsibilities and tasks associated with their employment duties as a SA. Therefore, the personal credit information does not qualify as personal employee information for this purpose.

<u>Assessment of probable risk of in-store theft or fraud</u>

[44] MWW stated that "performing credit checks at the pre-employment stage allows Mark's to ensure that applicants who may be under financial strain are not in a position to commit theft or fraud". In other words, MWW maintained that the collection of this information is a way of minimizing the risk of theft or fraud at store level.

[45] MWW has provided evidence of a legitimate concern with respect to in-store theft and fraud, reporting 173 incidents of in-store theft and fraud over the course of 3 years; however, I am not persuaded that the collection of an applicant's personal credit information is reasonably required to evaluate a potential employee's likelihood to commit theft or fraud.

[46] Over the course of 3 years, prior to collection of personal credit information, the average number of in-store theft and fraud incidents was 57 compared to 53 cases since implementing the pre-employment credit check. This appears to be a minimal reduction in the number of incidents of in-store theft and fraud, suggesting that personal credit checks have not been effective in reducing the number of incidents. That is, the information is collected to screen out or deter individuals with criminal intentions; however, the Organization's statistics do not show that the practice has been effective in reducing the number of incidences of in-store theft or fraud.

[47] In my view, determining whether an applicant is likely to commit in-store theft or fraud requires a subjective assessment of the applicant's character. Personal credit history is not reasonably likely to provide the information necessary to make this assessment. Furthermore, the Organization did not provide evidence to show that its collection of personal credit information is effective for meeting this purpose.

[48] I conclude the information at issue is not reasonably required to assess the Complainant's ability to perform the duties of a SA, or to assess whether he might be likely to commit in-store theft or fraud.

[49] I therefore find that the information, in this case, does not qualify as personal employee information. Therefore, it is personal information for the purpose of PIPA.

2. Did MWW collect the Complainant's personal information in compliance with section 11(1) of PIPA?

[50] I have found that the Complainant's personal credit information in this case is personal information under PIPA; therefore, section 11(1) of the Act applies. Section 11(1) of the Act states:

> *(1) An organization may collect personal information only for purposes that are reasonable.*

[51] Section 11(1) of PIPA makes it clear that the purpose for collecting personal information must be reasonable. For example, reducing in-store theft

and fraud and making sound hiring decisions may be reasonable purposes in itself, but an organization must also establish that its collection of personal information in this case, the personal credit information of the Complainant is reasonably related to that purpose to meet the requirements of section 11 of PIPA.

[52] MWW maintained that the collection of Complainant's personal credit information was reasonably required to assess his ability to handle the financial responsibilities of the SA position and to consider whether he was a risk for committing in-store theft or fraud. From my review of whether the information at issue is personal information or personal employee information, I have already determined that the personal credit information of the Complainant is not directly related to the Organization's stated purposes for collecting such information.

[53] That is, the Organization has failed to establish any reasonable connection between collecting personal credit information and its stated purposes for collecting the information. I am therefore unable to conclude that the Organization met the requirements of section 11 of PIPA when it collected the Complainant's personal credit information.

[54] For these reasons, I find that MWW did not meet the requirements of section 11(1) of PIPA when it collected the personal credit information of the Complainant, as its collection of personal information is not reasonably related to its purposes.

VI. SUMMARY & RECOMMENDATION:

[55] In this investigation, I determined that MWW's collection of the Complainant's personal credit information was not reasonably required to assess the Complainant's ability to perform the duties of a SA, or to assess whether he might have a tendency towards committing in-store theft or fraud. Therefore, MWW did not meet the requirements of section 11(1) of the Act which requires that organizations collect personal information only for purposes that are reasonable.

[56] In response to my findings, I recommended that MWW take the following action to resolve improper collection of personal credit information:

- Cease collecting personal credit information of Sales Associate applicants as part of the Organization's hiring process.

[57] The Organization accepted the findings in this report and implemented the recommendation. The Complainant considered his complaint under PIPA to be resolved. This matter is therefore closed.

VII. CONCLUSION:

[58] This case illustrates the need for organizations to only collect personal information from prospective employees that is specific to the requirements of the position to be filled, while at the same time respecting their privacy rights set out in the Act.

Linda Sasaki
Portfolio Officer, *Personal Information Protection Act*
Office of the Information and Privacy Commissioner