Reviewing the Return Policies of the Liquor Control Board of Ontario

Privacy Investigation Report PC07-100

and

A Review of the Literature Relating to Fraudulent Returns: Practices Used by Retailers to Combat Fraud

January 15, 2009

Information and Privacy Commissioner of Ontario

Ann Cavoukian, Ph.D.
Commissioner

Table of Contents

Report

Addendum

Report

Introduction

This investigation report deals with the collection of personal information by a retailer from a customer who was returning a product. This is an issue that continues to trouble both customers and retailers alike. Retailers want to offer liberal return policies in order to encourage customer convenience and loyalty. Customers enjoy the advantages of such policies, but may object to providing retailers with additional personal information, as a condition of returning a product. Underlining this issue is the fact that the abuse of return policies and fraudulent activities results in significant financial losses for retailers. In 2007, it was estimated that the costs relating to fraudulent returns amounted to $10 billion in the United States.

This report will deal with a specific complaint filed with my office in Ontario. However, in recognition of the significance of this issue for consumers and retailers alike, we included an Addendum containing a review of the literature relating to fraudulent returns and practices used by retailers to combat the problem. The report culminates in recommended practices on how to attain the legitimate business objective of detecting and deterring fraud with respect to retail returns, while at the same time, protecting customers' privacy.

Summary of Complaint

The Office of the Information and Privacy Commissioner of Ontario (IPC) received a privacy complaint from an individual, involving the Liquor Control Board of Ontario (the LCBO). The complainant felt that the LCBO had improperly collected his personal information, in contravention of the provisions of the *Freedom of Information and Protection of Privacy Act* (the *Act*).

Specifically, the complainant advised that he went to one of the LCBO's retail stores in order to return an unopened bottle of spirits. He had a receipt for the product, which he had paid for in cash.

The complainant advised that he was asked by the store's manager to provide his name and address in order to receive the refund. The complainant reluctantly provided his name and address, but was of the view that he had been "forced" to do so. In addition, the complainant indicated that he was not told why his personal information was being collected, or what it would be used for, other than it was being collected for "his safety." In addition, he was not informed of the retention period to which his personal information would be subject.

The complainant advised that, "there seemed to be no reason for providing the name and address since the purchase was in cash, with the receipt." In addition, if the product was found to have been stolen, there would have been no method of tracing the product back to the purchaser given that the purchase was made in cash.

In summary, the complainant was of the view that the LCBO's collection of personal information was "in violation of privacy laws."

In Ontario, the *Liquor Control Act* authorizes a government agency, the LCBO, to operate retail stores, for the sale of liquor in the province.

The IPC conducted an investigation into the complaint, which involved obtaining information from both parties, both verbally and in writing. In addition, staff met with representatives from the LCBO to obtain further information. Both parties were given the opportunity to provide written representations to this office, which they both chose to do.

Issues Arising from the Investigation

I have identified the following issues arising from this investigation, each of which will be discussed in turn.

(A) Is the information "personal information" as defined in section 2(1) of the *Act*?

(B) Is the collection of the "personal information" by the LCBO in accordance with section 38(2) of the *Act*?

(C) Is the notice provided by the LCBO in accordance with section 39(2) of the *Act*?

(D) Is the use of the "personal information" in accordance with section 41(1) of the *Act*?

(E) Is the retention of personal information in accordance with section 40(1) of the *Act*?

Discussion

Issue A: Is the information "personal information" as defined in section 2(1) of the *Act*?

At issue in this complaint is the information that was collected by the LCBO, namely the complainant's name and home address. As a general rule, the LCBO collects an individual's name, residential address and telephone number when goods are returned for a refund. Accordingly, this investigation will focus on these three pieces of information.

The definition of "personal information" is set out in section 2(1) of the *Act*, which states in part:

> "personal information" means recorded information about an identifiable individual, including,
>
> …
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> …
>
> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Based on the above definition, I am satisfied that the information in question clearly qualifies as "personal information" under the *Act*. The parties do not dispute this conclusion.

Issue B: Is the collection of the "personal information" by the LCBO in accordance with section 38(2) of the *Act*?

The section of the *Act* that addresses the collection of personal information is section 38(2), which establishes a basic prohibition on the collection of personal information, but states that there are three circumstances under which the collection of personal information may take place. Section 38(2) states:

> No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

In order for a particular collection practice to be in accordance with the *Act*, it must be shown to satisfy at least one of the three conditions set out in section 38(2). In other words, the institution must show that the collection of personal information is either, (1) expressly authorized by statute, (2) used for the purposes of law enforcement, or (3) necessary to the proper administration of a lawfully authorized activity.

Representations of the Parties

The LCBO submits that the *Liquor Control Act* authorizes it to, among other things, operate government retail stores for the sale of liquor in Ontario. In particular, section 3(1) provides that the LCBO has the power to:

> (a) buy, import and have in its possession for sale, and to sell, liquor and other products containing alcohol and non-alcoholic beverages;

(b) control the sale, transportation and delivery of liquor;

(d) establish government stores for the sale of liquor to the public; and

(n) do all things necessary for the management and operation of the Board in the conduct of its business.

The LCBO submits that the collection of personal information in the context of a refund relates directly to its authorized sale of liquor and is necessary for the management and operation of the LCBO in the conduct of its retail business.

The LCBO provided the following information regarding the collection of personal information in the context of the return of a product for a refund. Customers may return, and in some cases exchange, products for the following reasons:

1. Over-purchase (including from special occasion permit functions such as weddings);
2. Wrong size/product type;
3. Customer changed his/her mind;
4. Customer doesn't drink alcohol;
5. Product recall; and
6. Customer complaint.

Returns for the first four reasons are considered routine refunds where the product is returned to the store inventory, while reasons five and six fall within the scope of quality control where the product is destroyed or forwarded to the LCBO's Quality Assurance department for further investigation.

Customers may return any product, excluding gift cards, sold by the LCBO to any LCBO store for a full refund, provided the product is unopened, in saleable condition, and the customer possesses the receipt for the purchase. Where there is no receipt, the return may be allowed at the discretion of the manager. Customers may exchange one product for another of equal value, and no personal information is required.

All returns where money is refunded require that a name, address and telephone number be entered on the Point of Sale (POS) system - the electronic cash register. The customer has the option of providing the personal information verbally or in writing. Where the customer does not have a receipt, the customer may be required to show a piece of photo identification, such as a driver's licence, so that the staff member can visually verify the customer's identity. The photo identification number is not, however, recorded, or retained.

The personal information entered on the POS system in individual stores is transferred onto the LCBO's mainframe, which is called the T-log, on a daily basis. Personal information, such as customer name, address and telephone number, once entered on the POS system, cannot be accessed by staff at the store level.

Once the customer has provided the above information, the money is refunded, and the customer is required to sign a "refund transaction" to confirm that they received the refund. This receipt also contains their name and address. I have been advised by the LCBO that this receipt will no longer contain any personal information, effective the end of February, 2009.

In the case of refunds involving large amounts of money (over $500 without a receipt, and over $2,000 with a receipt), the refund is provided via postal mail.

Where the product is returned for a quality control reason, the customer's personal information appears on a customer complaint screen, which is then forwarded to the Quality Assurance Department for possible investigation to manage health and safety concerns, mitigate product tampering incidents, and identify potential product quality issues. In addition, the customer may be contacted in order to resolve quality-related complaints.

In summary, the LCBO collects customers' personal information for three reasons: to reduce potential losses associated with fraudulent returns; to send refunds in the mail; and to manage quality assurance matters where a customer has lodged a complaint about a product.

With regard to the first reason, the LCBO is of the view that the collection of personal information plays a critical role in identifying fraud related to returned products, which is estimated to represent eight to ten per cent of returns, and has proved "extremely valuable in curtailing fraudulent returns." In addition, the LCBO submits that the collection of personal information relates directly to its authorized sale of liquor and is necessary for the management and operation of the LCBO in the conduct of its retail business.

In support of its position, the LCBO notes that it is an acceptable common practice for retail organizations to collect name and address information when processing return transactions for the purpose of preventing fraud.

The LCBO referred the IPC to a number of investigations conducted in other Canadian jurisdictions that upheld the collection of limited amounts of customer personal information by retail stores, when goods are returned. These cases will be discussed in detail below.

The complainant submits that the collection of personal information is an unnecessary invasion of an individual's privacy in "the sensitive field of alcohol." The complainant states:

> I have been referred to several cases in dealing with this matter and respectfully submit that they are wrong as far as the issue of whether or not retaining the name, address, phone number of a person returning an item in perfect condition with a cash receipt is concerned. The main argument is that the LCBO cannot control its employees to the extent that these employees are collecting the customer's receipts that they don't use and then stealing products and then having these items returned. It's respectfully

submitted that there are better and different methods of deterring this theft than asking innocent customers for personal information and then calling them up to see if they in fact returned the product. It is respectfully submitted if employees are engaging in this type of activity which would be obviously visible to the naked eye, it should be easy to prevent with other methods and also the LCBO has more to worry about than returned product.

Analysis

The collection of certain types of personal information has been considered by several other jurisdictions in Canada.

In 2005, the Office of the Information and Privacy Commissioner of British Columbia (OIPCBC) dealt with a complaint from an individual who had been asked to provide her name, address and telephone number upon returning merchandise to a Canadian Tire store. The issue in this case was whether British Columbia's *Personal Information Protection Act* (*PIPA*) permitted a retailer to require someone who was returning merchandise to provide identifying personal information, for the purpose of combating fraudulent returns of merchandise.

Commissioner David Loukidelis considered the evidence submitted by Canadian Tire and the Retail Council of Canada (RCC). In Order P05-01, the Commissioner noted that:

> The RCC has periodically studied losses to retailers from theft, fraud, and other activities. Its 2003 Canadian Retail Security Report indicated that "the total retail sales lost due to theft were over $3 billion annually or $8 million each day"... The largest part of these losses stems from theft, but the RCC says these figures are relevant because stolen products are often returned fraudulently for refund …
>
> …
>
> … the RCC adds retailers have had to improve their procedures regarding returns while maintaining good customer service. This of necessity has required better information about returns and the individuals who make them.
>
> This information is used by many retailers, the RCC indicates, to analyze the risk that a particular return of goods may be fraudulent…the RCC says retailers have identified a number of 'strong indicators that a transaction may be an attempt to get money from a retailer fraudulently,' including these:
>
> - Frequent returns by the same customer;
> - Multiple refunds made to different individuals at the same address;
> - Returns of product unaccompanied by a receipt;
> - An unusually high level of returns without a receipt (may be a sign of employee collusion);

- Above-average returns of the same product (also useful as a warning of product performance and quality problems);
- A volume of returns that is excessive in relation to the volume sold;
- Returns of an unusual type of product such as a product that is purchased to be used immediately (e.g. consumable products); and
- The presentation of counterfeit receipts of credit or debit card slips along with stolen merchandise (this is typically gang-related activity).

Personal information is "essential," according to the RCC, to help a retailer decide whether a fraud is being attempted…The collection of personal information also deters fraud because …

> … criminals abhor visibility. Our members advise us that the mere request for personal information will cause some customers to refuse or leave the desk immediately. Our members recognize that some legitimate customers genuinely object to providing personal information. But it has also proven to be a strong indicator of fraud. Those retailers who ask for an address to which they can send a cheque reimbursing the customer are confident that a customer who refuses this information has a high likelihood of being a fraudster …

The material before me establishes that some individuals return stolen goods to retailers using receipts that they have obtained illegitimately. In other words, the fact that someone who is returning an item produces a receipt does not mean the item was not stolen or that the receipt genuinely relates to the item being returned.

To summarize, the material before me establishes that there is a real, not merely a perceived or minimal, problem with the fraudulent return of stolen goods by supposed customers, with or without sales receipts in hand. The organization has other loss prevention measures in place, but collection and use of identifying personal information is, it says, an important feature of its overall loss-reduction efforts.

Commissioner Loukidelis concluded that the collection of an individual's name, address and telephone number by Canadian Tire was "appropriate" and "necessary" under the applicable sections of *PIPA*. In doing so, the Commissioner considered the following factors in concluding that the personal information at issue is necessary for loss prevention purposes.

First, the Commissioner noted that the type of personal information at issue is generally available to the public and is generally not sensitive in nature. Second, the information is collected to implement a risk management strategy, i.e., to minimize monetary loss due to fraud, and not for the purpose of using it as an asset or turning it into a "collateral advantage." Third, Canadian Tire limits its requirement to basic identifying information that is directly related to, and minimally required for, achieving its legitimate purposes.

Following the OIPCBC's order, the Office of the Information and Privacy Commissioner of Alberta (OIPCA) initiated an investigation following a complaint that two Canadian Tire stores were collecting customers' personal information, including driver's licence numbers. Then-Director Elizabeth Denham noted that the complainants in this matter were not concerned with the collection of their names, addresses and telephone numbers, but were solely concerned with the collection, recording and retention of their driver's licence numbers. However, she commented on the issue of the collection of name, address and telephone number, stating:

> Because the complainants were not concerned with the collection and recording of their names, addresses and telephone numbers, I will consider only the collection, recording and retention of D/L [driver's licence] numbers in this context. I note that Commissioner Loukidelis in his recent order found that collecting names, addresses and telephone numbers to be acceptable under B.C.'s *PIPA*, but he did not address the recording of D/L numbers. His reasons for reaching that conclusion are persuasive in my view for the purposes of Alberta's *PIPA*.

Ms. Denham concluded that it was not reasonable for retailers to collect and retain customers' driver's licence numbers when merchandise is returned. She also found that it was reasonable in some cases to ask for photo identification to confirm identity, but not to record this information.

In February, 2007, the Office of the Privacy Commissioner of Canada (OPC) published a Case Summary[1] in which the OPC received a complaint from an individual who had been asked to provide his name, address and telephone number, and to show a form of photo identification to a retailer in order to receive a refund.

The OPC launched an investigation and found that it was appropriate for a retailer to verify the customer's identity by requiring that the customer produce photo identification, which is checked but not recorded, in the context of a refund or exchange of merchandise, as the loss of privacy to the customer, as a result of viewing the identification, was minimal. In addition, although the complainant was not concerned about the collection of his name, address, and telephone number by the retailer in processing his refund, the OPC's Assistant Commissioner, Heather Black, considered the issue, and determined that the collection of this information in the context of a refund or exchange resulted in a minimal loss of privacy to the customer and was, therefore, appropriate in the circumstances. The Assistant Commissioner concluded that any loss of privacy to the customer must be weighed against employee or customer fraud, which "means higher prices for all consumers."

In coming to the above conclusion, the Assistant Commissioner considered information provided by the RCC, who submitted that obtaining personal information, such as name, address and telephone number, is necessary to combat theft and fraud. The RCC provided examples of how such a purpose is met. They are:

1 PIPEDA Case Summary #361, 2007.

- Reduction of theft by employees. Employees can no longer claim that an item had been returned for refund by an unknown person. Information about the customer is now available so stores can verify the return.

- Identification of multiple returns made by the same person or persons who have different names but are connected with the same address or telephone number.

- Identification of buying patterns. For example, people may buy an item and then use half of it. They then return the unused portion and claim the item is defective or was not full upon purchase.

- Reduction of "receipt theft." This is the theft of items listed on receipts that people find outside a store or in a mall.

In September, 2007, the OPC initiated a joint investigation with the OIPCA after being notified by TJX Companies Inc. and Visa that TJX had suffered a network computer intrusion affecting the personal information of an estimated 45 million payment cards in Canada, the United States, Puerto Rico, the United Kingdom and Ireland. TJX is the parent company of Winners Merchant International L.P. (Winners).

The personal information that was accessed by the intruder(s) consisted primarily of credit card numbers used by customers who paid using that method of payment. Also accessed were the names, addresses and telephone numbers of customers as well as Canadian driver's licence numbers and other provincial identification numbers for unreceipted merchandise-return transactions. The latter set of personal information was collected for the purpose of preventing fraud.

One of the issues to be determined was whether TJX and Winners had a reasonable purpose for collecting the personal information affected by the intrusion. In making their determination, the OPC and the OIPCA applied section 5(3) of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), and section 2 of Alberta's *PIPA*. Both provisions state that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

The OPC and the OIPCA determined that the collection of customers' names and addresses for the purpose of deterring fraud during the return of goods was reasonable and appropriate in the circumstances, and was in compliance with their respective statutes. However, the report concluded that the recording of ID numbers, such as driver's licence numbers, was excessive and contrary to the two relevant statutes.[2]

More recently, on December 2, 2008, the Privacy Commissioner of Canada and the Information and Privacy Commissioners of British Columbia and Alberta released a guide to retailers on the collection of driver's licence numbers when processing customer returns. Consistent with the

2 After considering further submissions made by the retailer, the OPC and the OIPCA allowed the collection of driver's licence numbers on a temporary basis. The retailer devised an algorithm that would instantly convert the driver's licence number to a unique identifying number. It is important to note that the decision resulting from this joint investigation was in the context of the return of merchandise in the absence of a receipt.

jurisprudence of the three offices reviewed above, the guide discourages retailers from collecting a customer's driver's licence, in most situations. As noted in the guide, in most instances, asking to view a customer's licence in order to verify their name and address will be sufficient to meet the needs and legitimate purposes of the retailer.

As part of the present investigation, we decided to retain Ernst & Young to conduct a thorough review of industry practices regarding the collection of personal information from customers returning merchandise, and the related privacy considerations. We viewed this as an opportunity to address the issue of returning goods in Ontario, in an in-depth and comprehensive manner.

In their report, Ernst & Young confirmed that retailers collected personal information for a number of reasons, including the primary purpose of fraud control. The report describes the type of fraudulent activity that can take place:

> Criminals, rogue employees, and even some customers commit fraud by abusing return policies. Customers may buy products, apply for rebates, return the purchases, and then buy the items back at the returned-goods discount. Rogue employees may collect receipts left in the store by customers and then use them in different locations to return stolen goods for cash. Criminals return stolen goods for refunds as well – in some cases using counterfeit receipts and in other cases returning goods that were purchased with fraudulent or stolen tender. Other types of fraudulent activities include placing lower priced tags on merchandise with the intent to return the goods for the full retail price, and buying differently priced, similar-looking items and returning a less expensive item as a more expensive one.
>
> … the collection of personal information from individuals returning merchandise is intended to identify the perpetrators of fraud and to deter them. The identification of such perpetrators allows retailers to prevent the fraudulent return and, where appropriate, involve law enforcement.

The findings of the Ernst & Young report will be discussed in the Addendum to this report.

The issue I must determine is whether the LCBO's collection of personal information is in accordance with section 38(2) of the *Act*. As previously indicated, section 38(2) states:

> No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

In this case, the LCBO stated that the collection of personal information in the context of a refund relates directly to its authorized sale of liquor and is necessary for the management and operation of the LCBO in the conduct of its retail business.

Therefore, the LCBO has taken the position that its collection of personal information is "necessary to the proper administration of a lawfully authorized activity." The LCBO states that the lawfully authorized activity in question is the sale of liquor to the public via government stores, which includes, among other functions, providing refunds to customers.

In *Cash Converters Canada Inc. v. Oshawa (City)*[3], the Ontario Court of Appeal made reference to past decisions of the IPC in interpreting the necessity condition:

> In cases decided by the Commissioner's office, it has required that in order to meet the necessity condition, the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not "necessary" within the meaning of the Act. Similarly, where the purpose can be accomplished another way, the institution is obliged to choose the other route.

Accordingly, in order to demonstrate that a specific collection of personal information is permissible under the necessity condition set out in section 38(2) of the *Act*, the institution in question must show that the collection of each item or class of personal information is necessary to administer the lawfully authorized activity.

In applying the general rule to the facts of this investigation, the LCBO is required to demonstrate that the collection of each item or class of personal information is necessary to the prevention and detection of fraud in the context of the return of merchandise.

Based on the information provided by the LCBO, as well as my review of the current caselaw, the report produced by Ernst & Young and the guide to retailers issued by my federal and provincial colleagues on December 2, 2008, it is clear that the accepted industry standard is to collect personal information such as name, address and telephone number, in the context of a retail return.

In addition, there is significant evidence that the collection of an individual's name, address and telephone number is a necessary measure in preventing and detecting fraud. It is estimated that approximately eight to ten per cent of returns are fraudulent, and result in significant monetary losses to retailers. This is a legitimate business concern. I appreciate that the complainant feels that the collection of his personal information by the LCBO was intrusive and a breach of his privacy. However, it is important to note that any monetary losses suffered by a retailer as a result of fraudulent returns will be visited on customers in the form of higher prices.

It should be noted that this is not a case where the product is held under strict controls such that only internal theft would be possible. If that was the case, the collection of customers' personal information may not be necessary. However, the LCBO's products are clearly on display in their stores permitting easy, unobservable access by staff, customers and thieves alike.

Accordingly, I am satisfied that the collection of a customer's name, address and telephone number satisfy the necessity condition of section 38(2) of the *Act* and, therefore, that the collection of this type of personal information is in accordance with section 38(2).

---

3 (2007), O.J. No. 2613 (Ont. C.A.).

In addition, although in this case the complainant was not asked to produce any government issued photo identification, I am of the view that visually examining a piece of photo identification to verify a customer's identity is acceptable. However, consistent with the position taken by the above-noted Commissioners in other Canadian jurisdictions, the recording and retention of the identification number is not acceptable.

Issue C: Is the notice provided by the LCBO in accordance with section 39(2) of the *Act*?

Section 39(2) of the *Act* states:

> Where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of,
>
> (a) the legal authority for the collection;
>
> (b) the principal purposes for which the personal information is intended to be used; and
>
> (c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

In its representations, the LCBO states:

> On the LCBO Returns/Exchange receipt we include a notice that the customer's personal information is necessary for processing the transaction, and include a contact phone number for further inquiries. We recognize that this notice does not fully inform the customer that the information may be used to verify and investigate potential fraudulent returns …

The complainant submits that he was not informed of the purposes for which his personal information was collected, other than that it was for his "safety." In addition, the complainant indicates that he was not told he might be contacted in future by LCBO staff to verify the return.

I have reviewed the LCBO's internal and external policies on returning products, as well as its external privacy policy. I have also reviewed a typical receipt produced when a product is purchased, and the receipt that the customer must sign when given a refund.

The LCBO's policy on returning products is entitled *Returning Product to the LCBO*, and is available on their website. The policy describes the type of products that can be returned, including defective products and those that a customer feels caused illness. In general, however, an item must be unopened, in saleable condition, and the customer must have a receipt.

In the case of a return due to a defective product, the policy indicates that the product may be returned for a full refund without a receipt. The policy also states that the "pertinent information is forwarded to the LCBO's Quality Assurance Department."

However, the policy does not advise the reader that a customer's personal information, such as their name, address and telephone number, will be collected at the time of the return, and the purpose for this collection. In addition, the policy does not provide the customer with the contact information of a public official who can answer questions about the collection.

The LCBO's internal policies relating to returns are entitled *General Return to Stock and Head Office Issued Refunds*, and *Debit and Credit Returns*, and provide step-by-step instructions for staff members on how to process returns, including the collection of personal information. However, these policies contemplate the personal information being recorded in writing on a particular form, as opposed to being entered electronically into the POS system. In addition, staff members are not advised of the purpose of the collection, nor are they instructed to explain the purpose of the collection to the customer. I am advised by the LCBO that these policies and procedures are currently under review and will be updated within 3 months of receiving this report to incorporate the recommendations contained therein.

The LCBO's privacy policy is available on their website. It states that personal information is collected when individuals register to become a user on any LCBO website or when goods are purchased from the LCBO. It states "… therefore, all information is only collected when you voluntarily provide it to us." The policy also indicates that the LCBO may require the individual's name, address, email address and payment/credit card information. In addition, the policy states that the LCBO's collection of personal information is under the authority of the *Liquor Control Act*.

The privacy policy goes on to state that the LCBO collects personal information in order to better serve the customer and meet customer service expectations. The policy states that the LCBO uses personal information to:

- Process, verify and deliver orders;
- Better understand product preferences;
- Track and analyze trends and patterns;
- Administer the Air Miles® Rewards Program;
- Administer ballots for contests, draws and raffles;
- Conduct information and education programs such as tutored tastings; and
- Comply with any legal and regulatory requirements.

This policy fails to mention that the LCBO collects personal information in the context of refunds, nor does it state that the purpose of the collection is to prevent and detect fraud.

I have reviewed a sample of a typical receipt given to the customer at the time of purchase. The receipt states "… all returns require a receipt." I have also reviewed the receipt that customers sign upon receiving a refund. This receipt states "… your personal information is necessary for processing this transaction. For questions/information about its use, contact Customer Service at …"

While I appreciate the LCBO's attempts to provide customers with information by way of its privacy policy and returns policy, these policies fail to provide adequate notice about the collection of personal information in the context of a refund, as contemplated by section 39(2) of the *Act*.

Specifically, customers are not notified that their name, address and telephone number will be collected when returning a product and that the primary purpose of this collection is the prevention of fraud, both internal and on the part of customers.

In addition, I am of the view that the LCBO's privacy policy is not only incomplete, but inaccurate. The privacy policy states that personal information is only collected when the customer voluntarily provides it. However, that is not the case. The LCBO requires the customer to provide their name, address and telephone number in order to receive a refund. There is nothing optional about this requirement.

Further, while this information should be included in the privacy policy posted on its website, the LCBO should look for additional opportunities to provide customers with greater access to this information. For example, I note that some companies post their return policy in-store, at any counter where a return may take place. Other companies provide customers with the name and contact information of their Chief Privacy Officer, at the point of return, should the customer have any questions about the collection of their personal information during the return process.

The explanation for the collection of personal information that was given to the complainant in this case, namely that the information was collected for his "safety," is unacceptable. I had a similar experience when I recently returned products to my local LCBO store, and was asked to provide my personal information as part of the refund process. When I asked the customer service representative (who didn't know), and then the manager, why my personal information was being collected, I was emphatically advised that the purpose of the collection was to monitor possible incidences of product tampering. My staff was subsequently able to confirm with LCBO's head office that this was not, in fact, correct, and that the actual purpose of collecting personal information was to deter and detect fraud. These examples indicate a complete lack of understanding about the purpose of collecting customers' information during the return process. I decided to test this one more time at another liquor store, asking the customer service representative the reason why personal information was collected when processing a return. While she was very co-operative and helpful, she indicated that she honestly didn't know the reason behind the practice but simply followed the automatic prompts given by the cash register – requiring that personal information must be entered in order to complete the return transaction. When asked to "guess" the reason why, she said it was probably to prevent product tampering so that, for example, "coloured water couldn't be substituted for wine."

As noted, the LCBO's internal return policies are silent on the issue of the purpose of the collection of personal information. As a result, I am not confident that LCBO staff are aware of why they are collecting this information from customers, nor are they providing adequate explanations to their customers.

The inability of customers to obtain a clear and courteous explanation of why their personal information is being collected is, in my view, a significant reason for their resistance to providing that information. If informed that their name, address and phone number are only being collected for the purpose of preventing both internal and external fraud, and that this information will not be used for any other purpose, a number of concerns may be allayed. Taking the time to provide such an explanation would also be viewed by most as extending an additional courtesy to the customer.

Finally, the LCBO provided representations stating that customers who may object to verbally providing their personal information for fear of other customers overhearing them have the option of writing it down for staff. Based on his representations, the complainant was not offered this option. Again, staff need to be made aware that customers have this alternative to verbally providing their personal information.

Based on the above analysis, I conclude that notice to the individual was not provided in accordance with section 39(2) of the *Act*.

Providing notice to customers is not merely a matter of complying with a legislative requirement. The provision of proper, timely and comprehensible notice will, in my view, result in an informed consumer and reduce concerns regarding the collection and use of their personal information. As a result, in addition to addressing the issue of staff training in my recommendations, I urge the LCBO, and any other retailer, to ensure that the following steps are taken when a customer returns a product:

- The customer should be treated with courtesy and respect - not as if the mere act of returning a product is reason for suspicion;
- Staff should provide the customer with a clear explanation as to why a limited amount of their personal information is required; i.e., to prevent internal and external fraud;
- The customer should be assured that their personal information will be retained in a secure manner and will not be used for any other purpose; e.g. profiling customer activities for marketing purposes;
- Customers who may be concerned that their personal information will be overheard if provided verbally must be given the option of providing that information in writing; and
- Staff should be able to refer customers to an employee, such as the Chief Privacy Officer, who can answer any additional questions regarding the collection of personal information.

Issue D: Is the use of the "personal information" in accordance with section 41(1) of the *Act*?

Section 41(1) of the *Act* imposes a general prohibition on the use of personal information, but states that personal information may be used in a number of enumerated exceptional circumstances. Section 41(1) states:

An institution shall not use personal information in its custody or under its control except,

(a) where the person to whom the information relates has identified that information in particular and consented to its use;

(b) **for the purpose for which it was obtained or compiled or for a consistent purpose;**

(c) for a purpose for which the information may be disclosed to the institution under section 42 or under section 32 of the *Municipal Freedom of Information and Protection of Privacy Act*; or

(d) subject to subsection (2), an educational institution may use personal information in its alumni records for the purpose of its own fundraising activities, if the personal information is reasonably necessary for the fundraising activities.

[emphasis added].

In order for a given use of personal information to be permissible under the *Act*, the institution in question must demonstrate that the use was in accordance with at least one of the exceptions in section 41(1).

In this instance, the LCBO has taken the position that its use of the complainant's personal information was in accordance with section 41(1)(b), (i.e., that the personal information was used for the original purpose for which it had been obtained or compiled, or for a purpose that was consistent with that original purpose).

In determining whether a given use of personal information is in accordance with section 41(1)(b), it is first necessary to determine the original purpose of the collection. Next, it is necessary to assess whether the use of this information can be properly characterized as being either for the original purpose of the collection, or for a purpose that is consistent with that original purpose.

The LCBO submits in its representations that the purpose of the collection of customers' personal information by the LCBO in the context of returns is to prevent and detect fraud. As previously indicated, the LCBO advises that the personal information collected during returns is downloaded daily and stored in a secure database called the T-log along, with all other daily transactional details from all LCBO stores. The Store and Winery Audit Department have audit software that flag potentially fraudulent returns based on a variety of parameters, which the LCBO provided to the IPC. The audit software is not run with the intent to profile customers in any way.

If suspicious patterns of returns are identified by the audit software, the Store and Winery auditors may verify if the names, and associated addresses and phone numbers, correspond to publicly available information. The auditors may then contact the customers in question to confirm whether they returned a product at a particular time. If there is a pattern of fraudulent activity

that has been verified, the matter is then turned over to the Resource Protection Department, who may, in turn, transfer the matter to the police.

Employee access to the return information, and any personal information collected as a result of efforts to identify fraud, is limited to the Store and Winery Audit Department and the Resource Protection Department.

Any personal information that is used by the Store and Winery Auditors and the Resource Protection Department is kept in the auditor's and investigator's working papers in individual files. It is important to note that these departments do not create or keep a database of customers' personal information. Therefore, neither department creates a list of "fraudulent" customers that could later be misused by the LCBO, perhaps for example, by providing it to other retailers.

The LCBO also indicates that the personal information collected in connection with refunds is not used for any other purposes such as marketing or mailing lists.

Based on the detailed information provided by the LCBO, I am satisfied that the use of personal information in the context of refunds is for the original purpose for which it was collected, which is the prevention and detection of fraud. There was no evidence that this information was used to profile customers; nor is it used to for marketing purposes or for the creation and distribution of mailing lists.

Having determined that the use of the personal information was for the original purpose for which it was collected, it is not necessary to determine if the collection was for a purpose that was consistent with the original purpose.

Therefore, I am satisfied that the personal information collected is used in accordance with section 41(1)(b) of the *Act*.

Issue E: Is the retention of personal information in accordance with Section 40(1) of the *Act*?

Section 40(1) of the *Act* states:

> Personal information that has been used by an institution shall be retained after use by the institution for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to that information.

Section 5(1) of Ontario Regulation 460 stipulates the retention period of personal information, as follows:

> Personal information that has been used by an institution shall be retained by the institution for at least one year after use unless the individual to whom the information relates consents to its earlier disposal.

The LCBO provided the following information regarding its retention period. The receipt signed by the customer at the time of the refund is kept for a two year period. As previously noted, the LCBO has advised the IPC that they are changing their practice such that personal information will no longer be recorded on this receipt, effective the end of February, 2009.

The personal information that is entered into the POS system (the electronic cash register) is transferred from the POS system to the LCBO's mainframe on a daily basis and stored in a secure database (the T-log). The personal information remains on the T-log for one year, unless it is used for investigating fraudulent returns, in which case it is retained for a minimum of one year after use.

In the usual course of business, after one year on the T-log, personal information is then transferred onto electronic tape and stored for seven years in secure storage. I am advised by the LCBO that this retention period is necessary as the T-log contains all the transactional information from all retail stores. The seven year retention period is required by Canada Customs and Revenue Agency (CCRA), pursuant to section 98 of the *Excise Tax Act* and by the Ministry of Finance pursuant to regulation 1012 of the provincial *Retail Sales Act*. In addition, the Ontario Government Common Record Schedule requires all provincial ministries and agencies to retain financial records for seven years.

If personal information is used by the Store and Winery Audit Department and the Resource Protection Department for the purpose of investigating potentially fraudulent returns, it is kept in individual files for a period of seven years.

The complainant submits that the LCBO's retention periods are too long.

The purpose of section 5(1) of Ontario Regulation 460 and section 40(1) of the *Act* is to stipulate the minimum period of time an institution must retain personal information, so that an individual has the opportunity to access their personal information. There is no maximum retention period set out in the Regulation. As the LCBO retains personal information for a minimum of one year after use, I am satisfied that the LCBO's retention period meets the requirements set out in Regulation 460.

While the *Act* and regulation set out a minimum retention period for personal information that has been used by an institution, it is a fundamental tenet of accepted privacy principles that personal information should not be retained longer than necessary to achieve its required purpose. I have therefore examined the LCBO's retention periods to determine if their lengths are justified.

While I am satisfied that the LCBO retains transactional information on the T-log for seven years in order to comply with the above stated statutory authorities, I am not convinced that customers' personal information, in the context of returned products, needs be retained for that length of time. I will address this issue in my recommendations.

I am satisfied that the retention period for the files created by the LCBO's auditors and investigators is reasonable, as that information may be required for possible future prosecutions. I note that this conclusion is based on the fact that this information is retained in discrete files and is not merged or amalgamated with any other personal information, to create lists of potentially problematic customers.

Therefore, I am satisfied that the LCBO's retention of personal information is in accordance with section 40(1) of the *Act*, subject to the outcome of my recommendation, below.

Conclusions

I have reached the following conclusions based on the results of my investigation:

- The information in question qualifies as "personal information" as defined in section 2(1) of the *Act*.
- The personal information was collected in accordance with section 38(2) of the *Act*.
- Notice to the individual was not provided in accordance with section 39(2) of the *Act*.
- The personal information was used in accordance with section 41(1) of the *Act*.
- The personal information was retained in accordance with section 40(1) of the *Act*, subject to the outcome of my recommendation, below.

Recommendations

In light of the above conclusions, I make the following recommendations:

1. That the LCBO review and revise its privacy and returns policies to clearly indicate the authority for collecting personal information, the type of personal information that is collected in the context of refunds, the purpose of the collection of the personal information, the use of the personal information, and the public official to whom customers can direct their inquiries.

2. That the LCBO develop a clear short notice to advise customers of the information set out in recommendation #1. Further, that the LCBO look for opportunities, in addition to their website and receipts, for making customers aware of the return policy, including what personal information is collected and why.

3. a) That the LCBO ensure that staff members who process returns are trained to advise the customer of the reasons why the collection of their personal information is required, for what purpose it may be used, and to provide the customer with the opportunity to give their personal information in a privacy protective manner.

   b) That the LCBO develop a prepared text to serve as the script for training staff members in providing customers with an explanation of the reasons why their personal information must be collected, and how it will be used. In addition, staff members should be trained to provide contact information for the LCBO's chief privacy officer to any customer who questions the need to provide personal information to process a return.

4. That the LCBO review its practices associated with the retention of personal information related to returned products and enter into discussions with the CCRA and the Ministry of Finance, to determine whether customers' contact information (name, address and telephone number) must be retained for seven years, in addition to the transactional information that is required to be retained.

By 3 months from the date of this report, the LCBO should provide the IPC with proof of compliance with the above recommendations.

Commissioner's Message

While generally considered to be a private sector issue, this is the third time that my office has been asked to investigate retailing practices relating to Ontario public sector organizations. In addition to the present investigation, my office has also reviewed the return policies of several other government organizations, starting with our provincial transit authority – GO Transit, with respect to the practice of returning purchased tickets. Similarly, my office has also worked with the Ontario Government Bookstore, which sells books and other goods to the public.

The question of what type of personal information may be collected when a customer returns a product is key for all retailers, whether they be in the public or private sector. There are numerous government organizations involved in the selling of goods and services, making their functions somewhat akin to private sector retailers, in this regard. As a result, I am adding an Addendum to this report that contains a review the literature in the area and examines current retail practices. Although the guidance provided is based on our public sector experience, it may also be of assistance to private sector retailers.

I am grateful to the Privacy Commissioner of Canada and the Information and Privacy Commissioners of Alberta and British Columbia for their "Guide for Retailers" jointly released on December 2, 2008. The recommendations contained in the present report and our Addendum are completely consistent with their approach.

Much of the concern that consumers have in providing their personal information when returning a product relates to the collection of their driver's licence number or other identifying information. Viewing the driver's licence, a provincial government-issued identification (ID),

is often the ID of choice and a practice that my federal and provincial counterparts agree is acceptable, as long as it is used only to verify a customer's name and address when processing a return, and no information from the licence is actually recorded. It should be noted that the LCBO follows this practice.

On a related matter, I should add that from time to time, a similar issue has arisen with regard to requests from retailers to view a customer's Ontario Health Insurance Plan (OHIP) card as a form of identification. In Ontario, the administration of health insurance and related services falls under the Ontario Ministry of Health and Long-Term Care. With respect to the collection of the OHIP number, the prohibition contained in the *Personal Health Information Protection Act* (*PHIPA*), is clear.

Under *PHIPA*, a retailer is prohibited from even requesting the production of an OHIP card, as well as prohibited from collecting, using or disclosing an OHIP number. A customer has the option, however, of voluntarily choosing to present his or her health card to a retailer for purposes of verifying identification. The retailer is prohibited, however, from collecting the OHIP number, which includes a prohibition against recording, taking note of, making a copy of the health card, or using and disclosing the number. It is critical that all retailers recognize the legal prohibition that *PHIPA* places on the production of OHIP numbers and on their collection, use and disclosure, as well as the guidance associated with not collecting or recording provincial driver's licence numbers.

While I have not ruled against the collection of a customer's name and address for the purpose of processing refunds for returned goods, let me be clear – the sole reason for this is because it serves as a strong deterrent to fraud. However, I would not have been aware of this fact had my office not been required to investigate this matter. I suspect that most people, likewise, would not be aware of it. For that reason (not to mention good customer service and courteous behaviour), all customers should be informed of this fact. Sales staff should lead by providing clear notice to customers of the reasons why they are required to ask for their personal information. If more retailers lead with notice instead of suspicion, when processing returned goods, they may encounter fewer difficulties in obtaining the information they seek.

January 15, 2009

Ann Cavoukian, Ph.D.
Commissioner

Date

A Review of the Literature Relating to Fraudulent Returns: Practices Used by Retailers to Combat Fraud

Addendum

to

Privacy Investigation Report:
Reviewing the Return Policies of the Liquor Control Board of Ontario

January 15, 2009

Introduction

On November 6, 2008, I gave a keynote address to the 2008 Privacy Invitational Forum, and mentioned in passing that my office was reviewing a privacy complaint regarding the collection of personal information in the context of returned goods. I was surprised at the high level of interest expressed by members of the audience after my speech. I was then approached by two senior executives from Canada's private sector – one from a large North American retailer and the other, a partner from a leading Canadian law firm – who encouraged me to examine the larger issue of return fraud. I agreed based on my understanding that this was a growing issue with significant implications to privacy and business.

Return fraud is a significant issue for consumers and retailers. In a report commissioned by my office, we asked Ernst & Young to delve into why personal information is often collected when goods are returned, and to identify the key privacy considerations for retailers.[1] Although the preceding privacy investigation report dealt with a specific complaint filed with my office, this Addendum reviews the issue of fraudulent returns and practices used by retailers to combat the problem. I hope that this review, based on my office's public sector experience and review of the literature, is helpful to other branches of government providing goods and services in similar contexts, and that it may also be of assistance to the private sector.

The Issue of Fraudulent Returns

Fraudulent returns fall under the larger umbrella of retail crime, which includes activities such as vandalism, burglary, and shoplifting. Retail crime is a serious problem for retailers around the world.[2] Unfortunately, the current economic downturn may serve to increase retail crime.[3] In 2006, 72 per cent of Canadian retailers said they experienced refund fraud in their stores[4]; in 2008, return fraud in the United States was estimated at $11.8 billion.[5]

Flexible return policies can contribute to a competitive business strategy. For example, J.C. Penney once changed their return policy to "no questions asked," even if the product did not come from their store. The policy was abused by some customers, with several staff refusing to give refunds despite the change in policy. It was later explained to staff that "… the policy generated more sales than losses due to customer abuse of it."[6] Therefore, lenient return policies

1 Ernst and Young. The Retail Perspective: Loss prevention, fraud control and privacy. (January, 2009) www.ey.com/privacy.

2 J. Shapland, "Preventing Retail-Sector Crimes" (1995) 19 Crime and Justice 263 at 292 citing results from an International Commercial Crime Survey conducted by the Netherlands.

3 "When a major electronics manufacturer opened a box of returned merchandise and found a tombstone instead of a television, the discovery did more than sound a grim warning for retailers in recession – it served as an omen of more brazen retail cons to come." J. Trop, "Businesses expect retail fraud to grow" *The Detroit News* (4 December 2008).

4 *2008 Retail Organized Crime Report* by the Retail Council of Canada and Brinks.

5 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's 2007-08 Customer Returns in the Retail Industry. Note, in this survey, the term "fraud" refers to "returns using counterfeit receipts, wardrobing (returns of used, non-defective merchandise), return of stolen merchandise, and return of merchandise purchased on fraudulent or stolen tender."

6 D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 27 at 28, 29.

can be a doubled-edged sword. Customer satisfaction goes up when returns are quick and easy, and, for that reason, customers may choose to shop at a particular store. On the other hand, return fraudsters can also exploit such return policies.

The Retail Perspective – A Report by Ernst & Young

At my Office's request, Ernst & Young researched the practice of retailers collecting personal information from customers wishing to return goods. They found that retailers collect personal information for purposes of fraud control and loss prevention, as well as identifying and categorizing customers. Retailers combating fraud collect personal information to identify and deter perpetrators which serves to prevent fraud, and can later involve law enforcement, if needed.

Ernst & Young found that the practices used by retailers are not uniform across the retail industry. They also found that when retailers ask for personal information, they may or may not document the personal information collected. Retailers who document personal information may limit the personal information being collected, and may or may not verify the personal information by asking to view identification.

Ernst & Young found that key components of return policies used by retailers included: limiting the time period a customer may return a product; restricting the types of products that may be returned; and restricting the condition of return items. As a result of such policies, customers may, for example, receive a partial refund, be charged a restocking fee, or be denied the refund.

Some key privacy considerations that Ernst & Young identified for retailers include stating in return policies if personal information is collected as part of the return process – in other words, giving clear notice. In addition, privacy considerations include limiting the amount of personal information collected, and ensuring the accuracy of any information, especially if used to take adverse action against individuals.

In summary, Ernst & Young confirmed that the practice of collecting the name, address and telephone number of customers returning goods is consistent with retail industry standards and is a recognized tool in addressing the significant problem of return fraud.

Categories of Return Customers

Return customers may fall into the following categories:

- **Fraudulent return customer:** The fraudulent return customer engages in conduct that is clearly against the law, such as asking for a refund for a stolen product or presenting a forged receipt. This return customer may or may not be part of an organized retail crime ring.

- **Abusive return customer**: The abusive return customer engages in conduct that is clearly unethical, such as asking for a refund for an item which was knowingly bought for a one-time use (known as "wardrobbing," "retail renting," or "deshopping").

- **Careless return customer**: The careless return customer makes purchases without careful thought or examination, such as failing to try on clothing, or purchasing an item and realizing one cannot afford it.

- **Typical return customer**: The typical return customer has a legitimate complaint regarding the purchased product, such as a defect or misrepresentation regarding the product.

- **Higher volume return customers**: The higher volume return customer is a customer who purchases more products than the average individual because of loyalty to the store, or because of their professional occupation, such as a wedding planner. Therefore, this type of customer will have more return items than the average customer.

Examples of fraudulent return activities

Return of stolen merchandise

The fraudulent return customer steals an item and requests a refund for the stolen item. This may be done by purchasing an item, and during or after the purchase, stealing an item of the same description and returning with the receipt to get a refund for one of the items.[7]

Return of merchandise purchased with a stolen credit or debit card

The fraudulent return customer purchases an item with a stolen credit or debit card and returns for a cash refund.

Phoney or altered receipts

The fraudulent return customer will show a phoney or altered receipt. "Well over half of the retailers are seeing fraudulent receipts used in committing return fraud."[8] Fifty-five per cent of retailers have identified fraudulent receipts forged on company receipt paper, and 67 per cent of retailers have identified fraudulent receipts forged on other receipt paper. In the organized retail crime context, "return gangs" will set up in parking lots with in-car printers and copiers.[9] An Australian parliamentary Crime Prevention Committee looked at the issue of return fraud and sheds additional light on forged receipt practices:

Offenders may purchase a small item at the start of the day from a store in order to obtain the code that relates to that day's trading. They will then go to their car and generate receipts for high value goods, such as televisions, using a portable laptop computer and printer. They then

7 Final Report of Australia's Parliament of Victoria Drugs and Crime Prevention Committee's inquiry into fraud and electronic commerce, January 2004, at 41.

8 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's *2007-08 Customer Returns in the Retail Industry*.

9 C. Timberlake, "Spider Wrap, Inks Arm Retailers Fighting Holiday Return Fraud" *Bloomberg.com* (13 November 2008).

return to the store, select a television, and take it to the counter with their manufactured receipt to claim a refund. [10]

As this example may suggest, "Organized retail fraud is more sophisticated; fraudulent receipts and other techniques are making traditional methods of return fraud prevention less effective."[11]

Use of legitimate receipts discarded by paying customers

The fraudulent return customer uses a receipt discarded by a paying customer, such as a receipt discarded in a parking lot.[12] In a practice called "shoplisting" the fraudulent returner will take items off the shelves that match the items on the receipt, and will present them for a refund.

Full price refund for discounted merchandise

The fraudulent return customer requests a full price refund for an item purchased at a discounted price by, for example, claiming a refund at a different store than the item was purchased. "Ticket switching" occurs when the offender alters the price tag of an item to show a lesser price than was originally attached to the goods.[13] "Offenders have also been known to make bar codes at home with computer equipment and place them over the real ones, leading to the item being scanned at a lower price. They then tear off the new bar code, and return it for full price."[14]

Return fraud assisted by a store employee

The fraudulent return customer is assisted by a staff member who processes a non-existent refund or a refund greater than the amount of the product. "The offender uses either proof of purchase documents from a previous sale, provides fictitious customer details in place of a receipt, or processes a refund without including a receipt."[15] Such a practice is called "sweethearting."

Wardrobbing

Some consumers engage in a return practice called "wardrobbing" (aka "retail renting," or "deshopping") by buying a product for one-time use, knowing they will return the item for a full refund.

---

10 Final Report of Australia's Parliament of Victoria Drugs and Crime Prevention Committee's inquiry into fraud and electronic commerce, January 2004, at 41.

11 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's *2007-08 Customer Returns in the Retail Industry.*

12 Final Report of Australia's Parliament of Victoria Drugs and Crime Prevention Committee's inquiry into fraud and electronic commerce, January 2004, at 41.

13 Final Report of Australia's Parliament of Victoria Drugs and Crime Prevention Committee's inquiry into fraud and electronic commerce, January 2004, at 41.

14 Final Report of Australia's Parliament of Victoria Drugs and Crime Prevention Committee's inquiry into fraud and electronic commerce, January 2004, at 42.

15 Final Report of Australia's Parliament of Victoria Drugs and Crime Prevention Committee's inquiry into fraud and electronic commerce, January 2004, at 41.

Wardrobbing costs retailers[16] significantly. To address such return abuse, some retailers try to stem their losses via, for example, imposing a restocking fee – Circuit City introduced a 15 per cent restocking fee for returns of non-defective merchandise.[17] This, however, penalizes legitimate returns made by honest customers, who may then take their business elsewhere. Other retailers place tags in visible places on clothing, for example, and require that they be on the garment when returning an item.

Examples of practices used by retailers to combat the problem of return fraud

According to one survey, "Retailers continue to use a variety of methods, both manual and automated, in order to identify "bad returners" and stop the attempted return transaction. Tools employed include abuser lists, exception reports, real-time fraud detection systems, video analysis, and more."[18] Almost half of all retailers (49%) say that reducing fraudulent returns is a very high priority.

I have examined three employed practices in depth: tightening return policies; employing technology; and the collection of personal information and confirmation of identity.

Tightening return policies

According to a major survey conducted by the Retail Council of Canada and Price WaterhouseCoopers, 100 per cent of Canadian retailers surveyed have a formal policy for returns.[19] Retailers have responded to return fraud and abuse by tightening their return policies.[20]

In Australia, lenient return policies have worked against retailers trying to recoup money lost due to return fraud. For example, a Chief Magistrate of the State of Western Australia refused to order a fraudster to repay the money acquired from refunding stolen goods. The magistrate did so on the grounds that the "proudly advertised" refund policy "… encouraged people in difficult financial circumstances to steal."[21] Another magistrate in the State of Victoria refused to require a woman to repay $7,000 to a department store. "He claimed the store had to 'wear the consequences' of its negligence in letting the woman repeatedly get refunds for stolen merchandise." He said the store made it "… far too simple for people to go into the store, steal

16 "Previous research indicates that deshopping is widespread and is substantially affecting retailers' profits. Indeed, reducing the behaviour could add up 10 per cent or more to profitability ([9], [13] King, 1999, 2004)." T. King, C. Dennis, "Unethical consumers: Deshopping behaviour using the qualitative analysis of theory of planned behaviour and accompanied (de)shopping" (2006) 9:3 Qualitative Market Research 282.

17 J. Bilzi, "Circuit City applauded for new returns policy" (Nov. 17, 1997) 12:27 TWICE 1, 59.

18 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's *2007-08 Customer Returns in the Retail Industry*.

19 Retail Council of Canada and PriceWaterhouseCoopers' *Canadian Retail Security Survey 2007*.

20 S. Barlyn, "Cranky Consumer: Putting Return Policies to the Test; With Rising Fraud, Retailers Get Tough; 'No' to Washed Item" Wall Street Journal (Eastern Edition) (22 February 2007).

21 D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 27 at 28.

property and ask for a refund," adding that "… the store needs to learn a lesson as well as the accused."[22] It is perhaps views such as this that discourage retailers from offering lenient return policies.

Limit time period after which a customer can make a return

Some retailers choose to limit the time period after which a customer can make a return, or limit the number of returns a customer can make within a certain period of time. For example, Costco changed its return policy regarding electronic products. Previously, a customer could return the product at any time. The policy was changed so that customers had to return their electronic purchases within 90 days, with an exception for computers.[23] Seventy-one per cent of retailers have a date limit for allowing returns, exchanges or refunds.[24] The age of the receipt when processing returns matters 61 per cent of the time, and ranges from "as low as 5 days to as high as 90 days, with 30 and 90 days being the two most common time periods, at 40 % each."[25]

Taking into account the price of an item

Retailers will take into account the price of an item in determining whether the return will be accepted 30 per cent of the time in non-receipted situations, and 21 per cent in receipted situations.[26] Target Stores in the United States changed their return policy in this manner. Previously, customers could obtain a full refund without a receipt for purchases up to $100. Now the limit is $20 for returns without a receipt, with an exception for credit card purchases.[27]

Receipted vs. non-receipted

Eighty-one per cent of retailers require a receipt or proof of purchase to process returns, exchanges or refunds.[28] Retail and loss prevention groups in the United States have expressed concern that retailers are "… overly focused and more successful in stopping return fraud and abuse on transactions where receipts are not provided," adding:

> The majority of retailers' current processes and systems for reducing return fraud continue to focus on non-receipted versus receipted returns. At the same time, well over half of those surveyed have found forged receipts used in committing return fraud,

22 D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 27 at 28.

23 T. Sowa, "Privacy put on hold; As retailers try to cut down on fraudulent returns, consumers are asked to give up personal information" Spokesman Review (11 November 2007) E1.

24 Retail Council of Canada and PriceWaterhouseCoopers' Canadian Retail Security Survey 2007.

25 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's 2007-08 Customer Returns in the Retail Industry.

26 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's 2007-08 Customer Returns in the Retail Industry.

27 T. Sowa, "Privacy put on hold; As retailers try to cut down on fraudulent returns, consumers are asked to give up personal information" Spokesman Review (11 November 2007) E1.

28 The Retail Council of Canada and PriceWaterhouseCoopers' Canadian Retail Security Survey 2007.

which may indicate a growing trend and result in closer attention to the vulnerability of receipted returns.[29]

Requiring manager approval for returns

Sixty-two per cent of all retailers require manager approval prior to any return, exchange or refund.[30] For example, "Wal-Mart announced in 2004 that it began using its return-tracking system to alert cashiers to customers who bring back more than three items without receipts within 45 days. Those customers must get a manager to approve their returns."[31]

Refraining from providing cash refunds

Businesses attempt to prevent refund fraud by refraining from giving cash refunds, and instead only allowing an exchange of goods. Some businesses offer colour-coded refund credit notes, others with individual barcodes. Nevertheless, "Although such strategies could be circumvented by the onselling of credit notes or refund vouchers, this would limit some of the more obvious risks of refund fraud."[32]

Collection of personal information

Seventy per cent of retailers require that customers show some ID for non-receipted returns, and 21 per cent of retailers require customer to show ID for receipted returns. Sixty-eight per cent enter customer name, address or telephone number into a point-of-sale return system for non-receipted returns, and 49 per cent for receipted returns.[33]

Employing technology

Hard to forge receipts

Retailers may employ special paper to create hard to forge receipts. For example, one company produces receipt paper that changes colour when scratched.[34]

29 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's 2007-08 Customer Returns in the Retail Industry.

30 Retail Council of Canada and PriceWaterhouseCoopers' Canadian Retail Security Survey 2007.

31 "Returns: Prepare to be challenged" Consumerreports.org (December 2006).

32 Final Report of Australia's Parliament of Victoria Drugs and Crime Prevention Committee's inquiry into fraud and electronic commerce, January 2004, (available online at <http://www.parliament.vic.gov.au/dcpc/Reports/DCPC_FraudElectronicCommerce_05-01-2004.pdf) at 168.

33 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's 2007-08 Customer Returns in the Retail Industry report.

34 For example, see "Scratch and Secure" receipt <http://www.nashua.com/ESol/NashuaCom/CIS_ProductList.aspx?Selected=ESol>.

Point-of-sale receipt and goods tracking

Forty-two per cent of retailers use automated electronic return authorization systems.[35] Seventy per cent of retailers tie receipted returns to the original receipt value via an automated process.[36] Sixty-seven per cent of retailers tie receipted returns to the original item on the original receipt by looking up both the item (sku) and item purchase price (dollar value).[37] For example, one company that helps businesses keep track of goods such as TVs and DVD players employs a tracking system that works by assigning a unique "fingerprint" to each product sold in relation to the product's UPC code and serial number on the box:[38]

> In one example, someone may purchase a computer printer and then walk into the store, grab another unit and return it using the original receipt. Because [the company's system] prints both the UPC and the serial number on the receipt, the clerk would know immediately whether that was a fraudulent return … [the company's system] does not collect personal data about the customer; only the serial number and the UPC code, as well as the date and location of the transaction.[39]

Collection of personal information and confirmation of identity

It is a widely held view that collection of personal information and confirmation of identity detects and deters fraud. Accordingly, retailers commonly collect personal information as a means to reduce fraud, employing a variety of approaches depending on their fraud and loss prevention strategies as well as the availability of technology and resources.[40] The Federal, Alberta and British Columbia privacy commissioners have stated that the collection of personal information is "… used to detect and deter fraudulent returns of goods as part of its overall loss-reduction strategy," and that photo identification may be requested, but not recorded, in order to verify that the information provided by the customer is accurate. [41] I fully agree with my colleagues. Our research confirms the benefits of reducing fraud by collecting personal information and confirming identity.

35 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's 2007-08 Customer Returns in the Retail Industry.

36 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's 2007-08 Customer Returns in the Retail Industry.

37 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's 2007-08 Customer Returns in the Retail Industry.

38 The company has assisted retailers such as Wal-Mart, Target, Kmart, Toys "R" Us, Circuit City and Best Buy. Nintendo first used the system and saw a reduction in overall returns by 72 per cent. A. Gilroy, "Audiovox Taps SIRAS Tracking" (April 21 2008) 23:9 TWICE 30.

39 B. Ploskina "Reducing Returns, 50:7 Dealerscope (July 2008).

40 Ernst & Young, "The Retail Perspective: loss prevention, fraud control and privacy," (2008) at 4.

41 Photo Identification Guidance, Sept. 19, 2007. In Order P05-01, British Columbia Information and Privacy Commissioner David Loukidelis accepted representations from the Retail Council of Canada that personal information is essential in detecting and deterring fraud: "…criminals abhor visibility. Our members advise us that the mere request for personal information will cause some customers to refuse or leave the desk immediately. Our members recognize that some legitimate customers genuinely object to providing personal information. But it has also proven to be a strong indicator of fraud. Those retailers who ask for an address to which they can send a cheque reimbursing the customer are confident that a customer who refuses this information has a high likelihood of being a fraudster. The normal business response is simply to decline to accept a return of the product."

It is well-known that a higher risk of detection and fear of apprehension lowers criminal behaviour:

> Researchers have explored the negative association between the illegal behaviour and the perceived chance of being caught. Such studies demonstrate that the fear of punishment deters people from partaking in behaviour, and a person is more likely to partake in criminal behaviour if there is low risk of detection ([3] Cole, 1989.).[42]

A combined approach (tightening of the return policy and collecting personal information) led to a reduction in fraudulent returns at Australia's leading retail company, Coles Myer Ltd., which at the time of the study had 1700 retail stores and $17 billion in yearly sales.[43] Coles Myer Ltd. tightened its refunds policy following the release of a model refund policy developed by the Retailers Council of Australia in 1993.[44] The revised policy provided that customers returning items without a receipt could exchange the item or obtain a credit voucher. With a receipt, a customer could be provided with a refund. In addition, cash refunds were permitted where the original purchase was made in cash, but not for credit card sales.[45] The company implemented a "refunder's database" which "… highlights frequent refunders to allow legitimate customers to be fast-tracked but also causes suspect refunders to be identified."[46] In an extensive review of the impact of the new policy, information was collected from 500 supermarkets, 391 discount stores and 70 department stores owned by Coles Myer Ltd. over a two year period. The results of the study, "… clearly show a marked reduction in fraudulent refund activity after introduction of the policy." During the peak months of the study, 600 fraudsters were detected.[47] In one example, a woman was identified, who in an 8-week period, visited three different store locations on 10 different occasions, seeking refunds without a receipt for computer games and toys. Overall, she obtained close to $3,000 for fraudulently refunding merchandise that she had not purchased.[48]

According to another study, confirmation of identity was shown to drastically reduce cheque fraud in Sweden.[49] The city of Stockholm faced an increasing problem with cheque fraud in the 1960s and 1970s. In 1965, instances of cheque fraud were 2,663, which rose dramatically to

---

42T. King, C. Dennis, "Unethical consumers: Deshopping behaviour using the qualitative analysis of theory of planned behaviour and accompanied (de)shopping" (2006) 9:3 Qualitative Market Research 282.

43 D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 27.

44 The model policy included the following elements: 1. Inform customers that proof of purchase is required for later refund (by signage or warning printed on register docket). 2. Require presentation of proof of purchase when refund requested. 3. If no proof of purchase is provided when refund is requested – (a) proof of identity must be seen; (b) the customer should provide a signed statement in their own handwriting detailing their identity, address, and details of the purchase; (c) a cash refund should not exceed a specified value set by the retailer and greater amounts should be paid by check; and (d) if the purchase had been made with a check, a refund should not be processed until the check is cleared. D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 31.

45 D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 27 at 31.

46 D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 27 at 34.

47 D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 27 at 31.

48 D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 27 at 34.

49 J. Knutsson, E. Kuhlhorn, "Macro-measures Against Crime: The Example of Check Forgeries" Chapter 7 in Situational Crime Prevention: Successful Case Studies Second Edition, ed. Ronald V. Clarke, (Guilderland, New York: Harrow and Heston, 1997).

15,817 in 1970. Criminals would steal cheque books and use cheques for payment in stores, or to obtain cash at a bank. At the time, stores did not have an incentive to ask for identification as banks indemnified cheques under 300 Swedish kronors, and the average amount for fraudulent cheques was also 300 Swedish kronors. Swedish law enforcement worked with banks and retailers to remove the bank guarantee and require that all cheque users show identification, which began July 1, 1971. Following the 15,817 peak in 1970, the cheque crime figures for Stockholm dropped steadily to a reported low of 2,066 in 1978 (1971 – 7,835 instances of cheque fraud; 1972 – 2,198; 1973 – 1,668; 1974 – 1,496; 1975 – 1,867; 1976 – 2,548; 1977 – 3,107; 1978 – 2,066 instances of cheque fraud). The researchers concluded that: "There is little doubt that the measures taken – the elimination of the bank guarantee and the introduction of identification requirements – were effective." They also note that unfortunately, "The measures meant that everyone who used checks was affected. The great majority of legal checking account users had to put up with increased restrictions so as to make it possible to cope with the abuses of a relatively small group."[50]

Another researcher found a 90 per cent reduction of credit card fraud losses during a 17 month period after the introduction of a computerised personal identification system used at an appliance chain store in New York.[51] Also in the context of cheque and credit card fraud, in New Zealand "Trustcard N.Z. ran an experiment for 18 months and found [photo cards] not cost-effective, though it did reduce fraud."[52] In the plastic and cheque fraud context, it is known that "Identity checking and matching with known previous frauds continues to cut fraudulent applications."[53] In the United Kingdom, the Credit Industry Fraud Avoidance System (CIFAS)

> … co-ordinates data on names and addresses involved in verified fraud. During 1999, 36,316 frauds were identified and reported to CIFAS in the banking sector, saving an estimated £47 million, while 25,948 frauds were reported in the retail credit (including store cards) sector, saving an estimated £9 million. In addition 17,608 frauds were identified as 'first party fraud' in which the cardholders themselves were implicated.[54]

When a CIFAS member identifies fraud, they file the name, address and other details with the CIFAS. When another member receives an application with, for example, the same address, that member will undertake a thorough investigation to determine if it is a fraudulent application. Such a flag on an address does not mean it is blacklisted, and members are not permitted to

50 J. Knutsson, E. Kuhlhorn, "Macro-measures Against Crime: The Example of Check Forgeries" Chapter 7 in Situational Crime Prevention: Successful Case Studies Second Edition, ed. Ronald V. Clarke, (Guilderland, New York: Harrow and Heston, 1997).

51 R. Smith, "Best Practice in Fraud Prevention" (Paper submitted to the National Outlook Symposium on Crime in Australia, 22-23 March 1999) 8, referencing research by Barry Masuda.

52 M. Levi, P. Bissell, T. Richardson, "The Prevention of Cheque and Credit Card Fraud" Crime Prevention Unit Paper No. 26, (1991) London Home Office at 39.

53 M. Levi, The Prevention of Plastic and Cheque Fraud: A Briefing Paper (School of Social Sciences, University of Cardiff School, 2000 [Prepared for Home Office Research, Development and Statistics Directorate] at 4.

54 M. Levi, The Prevention of Plastic and Cheque Fraud: A Briefing Paper (School of Social Sciences, University of Cardiff School, 2000 [Prepared for Home Office Research, Development and Statistics Directorate] at 4.

automatically refuse an application based on such a flag. In 2007, CIFAS identified 185,003 fraud cases which avoided losses equal to £987,829,077 (approximately $1.8 billion CAD).[55]

When personal information is collected, statistical fraud analysis may be performed to alert one to "… the fact that an observation is anomalous, or more likely to be fraudulent than others, so that it can then be investigated in more detail."[56] This type of statistical analysis returns a score – the higher the score, the more likely it is that fraud is taking place. These scores "… can be computed for each record in the database (for each customer with a bank account or credit card, for each owner of a mobile phone, for each desktop computer and so on), and these [are] updated as time progresses."[57] By creating a model of a baseline distribution that mirrors normal behaviour, statistical fraud analysis attempts to detect instances that exhibit the greatest departure from the norm.[58] To detect credit card fraud, for example, statistical fraud analysis scores are used to "… detect whether an account has been compromised" which is "… based on models of individual customers' previous usage patterns, standard expected usage patterns, particular partners which are known to be often associated with fraud, and on supervised models." Sudden jumps in transaction or expenditure rates may be further investigated. [59]

Between 2002 and 2004, Australia's Parliament of Victoria Drugs and Crime Prevention Committee conducted an extensive review of fraud and electronic commerce. Their final report, over 400 pages in length, includes information from various testimony and hundreds of sources. Regarding confirmation of identity, the Committee reports:

> Identity-related fraud takes place when an offender defeats the user authentication strategies of a system, whatever they may be, and successfully identifies himself or herself as someone else, whether in the guise of a real other person or under cover of a totally fabricated identity. Where user authentication procedures are circumvented, the offender can avoid responsibility for his or her actions. **One way in which to address this problem is to improve the methods by which people are identified, or authenticate their identity, so that people who attempt to use false identities are likely to be detected.** This is seen to be essential to fraud prevention: 'Fundamental to this whole problem of commerce and crime, particularly e-commerce, is knowing who you are dealing with.' "[60] [*emphasis added*]

Checking the identity of customers is especially important in the context of deterring and detecting certain fraudulent activities, such as money laundering. According to a 2007 European

55 http://www.cifas.org.uk.

56 R. Bolton, D. Hand, "Statistical Fraud Detection: A Review" 17:3 Statistical Science 235 at 236.

57 R. Bolton, D. Hand, "Statistical Fraud Detection: A Review" 17:3 Statistical Science 235 at 236.

58 R. Bolton, D. Hand, "Statistical Fraud Detection: A Review" 17:3 Statistical Science 235 at 237.

59 R. Bolton, D. Hand, "Statistical Fraud Detection: A Review" 17:3 Statistical Science 235 at 239.

60 Final Report of Australia's Parliament of Victoria Drugs and Crime Prevention Committee's inquiry into fraud and electronic commerce, January 2004, at 156.

Commission report, requiring identification for fraud prevention in this context is legitimate and helps merchants "… avoid being liable for fraudulent transactions."[61]

According to the U.S.-based National Retail Federation, Loss Prevention Research Council, and The Retail Equation's *2007-08 Customer Returns in the Retail Industry*:

> Whether with a manual or automated system, a retailer's approach to managing returns should be keyed on identifying all return customers (receipted and non-receipted) and acting on their purchase and return histories). Implementing the right technology, combined with employee training that encourages diligent attention to the issue at the store level, will help combat the growth of forged receipts and result in reduced return fraud and abuse – leading to lower return rates, increased net sales, higher profits, and improved customer satisfaction.

Protecting customers' privacy, while at the same time attaining the legitimate business objective of detecting and preventing fraud, should be the goal.

Return fraud strategies should not come at the expense of courteous customer service

"I'll never shop here again" are words a retailer never wants to hear. The unintended consequences of tightening return policies, employing various technologies, and collecting personal information to identify return fraud is the unintentional targeting of, for example, the typical and higher volume customer described previously. Technology that monitors return information to spot potentially fraudulent returns is far from fool-proof. Statistical fraud analysis experts provide a caution in this regard:

> Fraudsters adapt to new prevention and detection measures, so fraud detection needs to be adaptive and evolve over time. However, legitimate account users may gradually change their behaviour over a longer period of time and it is important to avoid spurious alarms. Models can be updated at fixed time points or continuously over time.[62]

The nightmare scenario of targeting innocent customers is something that retailers will want to avoid at all costs. For example, a retired woman accidentally gave the wrong address on a refund slip when returning some nail clippers. The identification she offered did not list the address provided. As a result, she was arrested and spent 44 days in jail because she could not afford the fines for providing a false address.[63] While this example is extreme, it serves to demonstrate the point.

---

61 Working Party 4 Final Report titled "Study of user identification methods in card payments, mobile payments and e-payments of the European Commission: Analysis of the possible regulatory and contractual barriers to the use of available or prospective best technologies" MARKT/2006/08/F/WP 4 at 47.

62 R. Bolton, D. Hand, "Statistical Fraud Detection: A Review" 17:3 Statistical Science 235 at 237, 238.

63 M. Curriden, "Expensive refund" (1993) 79 ABA Journal 42.

Sixty-one per cent of retailers would consider giving an incentive at the point of return to their best customers, and 3 per cent say they already do. "Other studies have shown that incentives such as this can add incremental sales."[64] In this regard, retailers will need effective systems in place to ensure they are targeting the right individuals.

Explain that your losses arise from fraudulent returns

Retailers must be prepared to answer customer questions regarding their return policy. According to an Ipsos Reid survey commissioned by the Federal Privacy Commissioner of Canada, "Half of respondents (52%) have asked a store why they need this information when asked for their name, phone number, or postal code, while close to half (45%) have refused to provide such information upon request."[65] First, you must ensure that your losses are in fact due to fraudulent returns as opposed to other types of retail losses ("shrinkage"). Other losses that can occur relate to product damage, accounting and data errors, physical loss such as waste and spoilage, pure cash loss due to theft or error, or simple variances in the value of stock such as pricing changes.[66] The types of criminal activity faced by retailers is wide-ranging and includes employee theft (95%), customer theft (95%), credit card fraud (90%), break and enter (81%), counterfeit bank notes (76%), merchandise theft from organized groups (76%), gift card fraud (62%), acts of violence (57%), debit card fraud (57%), PIN pad tampering (38%), cheque fraud (33%), customer information theft (29%), armed robbery (29%), and vendor/contractor fraud (29%).[67]

In 2008, the Retail Council of Canada and the Royal Bank of Canada produced a tool – the *Retail Business Security Self Assessment,* to help retailers identify and prevent losses from all forms of retail crime, such as theft by employees, armed robbery, cash handling losses, credit card fraud, theft from stores, etc.[68] In addition, retailers may wish to ask the following questions as part of their overall loss prevention strategy to understand their vulnerabilities:[69]

1. What is the total impact of theft to the retail organization? What are the direct (loss of product, cost of replacing goods) and indirect costs (time spent investigating thefts, damage to brand image)?

2. Where are the losses coming from? Are losses internal or external? Where can the organization make investments in training, staffing, hardware and software to offset these losses?

64 The National Retail Federation, Loss Prevention Research Council, and The Retail Equation's 2007-08 Customer Returns in the Retail Industry.

65 Ipsos Reid, Final Report "The Personal Information Canadians Give to Retailers" (Submitted to Office of the Privacy Commissioner, 4 January 2008) at 5.

66 A. Beck, C. Peacock, "Redefining Shrinkage – Four New Buckets of Loss" Loss Prevention Magazine (1 July 2006).

67 Retail Council of Canada and PriceWaterhouseCoopers' Canadian Retail Security Survey 2007.

68 See also, "Chapter 10: Loss Prevention" Winning Retail (Industry Canada/The Graff Retail Group) available at < http://www.retailcouncil.org/storeops/graff_report/winning_retail/Chapter10.pdf>. In addition, see R. Price, "Loss prevention dos and don'ts" 3:5 Retailer's Guide, Loss Prevention 1.

69 2008 Retail Organized Crime Report by the Retail Council of Canada and Brinks.

3. Who is responsible for understanding the organization's losses? Does the company's structure provide loss prevention the ability to get the answers they need from all departments?

4. What is the history of loss in the organization? What historical measures exist? Do measurements use consistent methodologies?

It goes without saying that customers will expect their personal information to be collected for the purpose of detecting and deterring return fraud, and not used for secondary purposes, such as identifying less profitable customers.

Customers should be made aware why their personal information is being collected. Retail organizations should look for different opportunities to provide customers with greater access to this information. For example, I note that some companies post their return policy on their websites, as well as in-store, at any counter where a return may take place. Other companies provide customers with the name and contact information of their Chief Privacy Officer, at the point of return, should the customer have any questions about the collection of their personal information during the return process.

None of these fraud detection practices should come at the expense of customers' privacy. The reality, however, is that they often do. For this reason, not to mention providing good customer service, a sales attendant should lead with an explanation of the reasons why a customer's name and address (and any other information) are required in order to process the return. Staff should be trained in advance with a prepared text that may be rehearsed in advance of processing returns. If this sounds excessive, then retailers should take the role of their customers, who, like me, have tried to innocently return an item within a reasonable period of time, only to be treated like a criminal and given the third degree. This is no way to treat your customers.

Employ a variety of strategies, not just collection of personal information

In addition, retailers should employ a variety of strategies, along with the collection of customers' personal information, to tackle the problem of return fraud, such as theft prevention. Research suggests that there is a relationship between the amount of fraudulent returns and thefts that a store may experience:

> A further success of Target's crime prevention approach to refund fraud is a diffusion of benefits in that there has been 'a reduction in crimes not directly addressed by the preventive measure' (Clarke, 1992, p. 25). In particular, theft of stock has decreased apparently because there were a number of offenders who were stealing from stores simply so they could then effect a fraudulent refund. With the refund option cut off, theft became pointless (or insufficiently rewarding) for them.[70]

70 D. Challinger, "Refund fraud in retail stores" (1996) 7 Security Journal 27 at 35.

For example, retailers will be well aware of measures that can be taken to prevent theft that may lead to the return of stolen items, such as:[71]

- tight supervision of goods and adequate security in the store to prevent fraudsters walking out with merchandise;
- adequate customer access control to high-end goods, such as putting high-end goods in cabinets;
- tagging of items;
- use of dummy goods and empty boxes for display purposes;
- goods in place;
- adjusting the store layout;
- warning notices about the consequence of theft;
- alarm systems;
- observation mirrors; and
- fitting room attendants.

Interestingly, identifying store items as ones that are frequently stolen by shoplifters, via placing a notice and red star on the item, significantly reduces the theft of those items.[72]

Retailers will also want to employ strategies to cut down on internal theft. Canadian retailers leverage simple control measures to reduce risk of losses due to internal sources such as pre-employment screening, rotating employees' duties where possible, avoiding having employees work alone in stores, providing training and training materials to employees on store policies specifically related to theft prevention. To prevent vendor and supplier fraud, retailers should also conduct routine reference checks prior to selecting a supplier, as well as tracking supplier delivery compliance to stores, and reconciling cheques to suppliers, on a regular basis.[73]

Having efficient processes in place will also minimize the impact that returned products have on retailers, such as reusing and reselling returned products (referred to as "reverse supply chain" or

71 J. Shapland, "Preventing Retail-Sector Crimes" (1995) 19 Crime and Justice 263 at 320.

72 J. Shapland, "Preventing Retail-Sector Crimes" (1995) 19 Crime and Justice 263 at 321.

73 Retail Council of Canada and PriceWaterhouseCoopers' Canadian Retail Security Survey 2007.

"reverse logistics").[74] For example, Estée Lauder has a $250 million product line from returned cosmetics that are sold to seconds stores and retailers in developing countries.[75]

Conclusion

Much of the annoyance that customers feel upon attempting to return an item to a retail store arises from how they are treated – poorly. Having reviewed the literature in this area, I now appreciate the high levels of fraud associated with the return of goods – in the vicinity of 10%. However, there is no reason to expect most customers to be aware of that fact. Nor is that an acceptable reason to treat the roughly 90% of honest customers with derision and suspicion. Leading with a polite explanation of the reasons why a customer's name and address (and any other information) are required, and, dare I say it, a smile, would go a long way to obtaining the necessary information and having a satisfied customer. Fraudulent returns are the retailer's problem, not the innocent customers', who nonetheless most often pay the price. Providing proper notice and courteous service achieves the retailer's need to obtain the necessary information and allows the customer to leave with their dignity intact – a win/win, positive-sum solution for both retailers and consumers alike.

74 V. Daniel, R. Guide Jr., L. Van Wassenhove, "The Reverse Supply Chain" Harvard Business Review (1 February 2002); J. Stock, T. Speh, H. Shear, "Many Happy (Product) Returns" Harvard Business Review (1 July 2002); S. Mukhopadhyay, R. Setaputra, "The role of 4PL as the reverse logistics integrator: Optimal pricing and return policies" (2006) 36:9 International Journal of Physical Distribution & Logistics Management 716.

75 A. O'Connell, "Improve Your Return on Returns" Harvard Business Review (1 November 2007).

Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario CANADA M4W 1A8
416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Email: info@ipc.on.ca