Catalogue no. 85-569-XIE

A Feasibility Report on Improving the Measurement of Fraud in Canada

2005

Statistics Canada Statistique Canada

Canada

How to obtain more information

Specific inquiries about this product and related statistics or services should be directed to: Canadian Centre for Justice Statistics, Statistics Canada, Ottawa, Ontario, K1A 0T6 (telephone: 1 800 387-2231 or (613) 951-9023).

For information on the wide range of data available from Statistics Canada, you can contact us by calling one of our toll-free numbers. You can also contact us by e-mail or by visiting our website.

National inquiries line	1 800 263-1136
National telecommunications device for the hearing impaired	1 800 363-7629
Depository Services Program inquiries	1 800 700-1033
Fax line for Depository Services Program	1 800 889-9734
E-mail inquiries	infostats@statcan.ca
Website	www.statcan.ca

Information to access the product

This product, catalogue no. 85-569-XIE, is available for free. To obtain a single issue, visit our website at www.statcan.ca and select Our Products and Services.

Standards of service to the public

Statistics Canada is committed to serving its clients in a prompt, reliable and courteous manner and in the official language of their choice. To this end, the Agency has developed standards of service that its employees observe in serving its clients. To obtain a copy of these service standards, please contact Statistics Canada toll free at 1 800 263-1136. The service standards are also published on www.statcan.ca under About Statistics Canada > Providing services to Canadians.

Statistics Canada

Canadian Centre for Justice Statistics

A Feasibility Report on Improving the Measurement of Fraud in Canada

2005

Published by authority of the Minister responsible for Statistics Canada

April 2006

Catalogue no. 85-569-XIE
ISBN 0-662-42984-2

Frequency: Occasional

Ottawa

Cette publication est disponible en français sur demande (nº 85-569-XIF au catalogue).

Note of appreciation

Canada owes the success of its statistical system to a long-standing partnership between Statistics Canada, the citizens of Canada, its businesses, governments and other institutions. Accurate and timely statistical information could not be produced without their continued cooperation and goodwill.

Table of contents

Acknowledgements

This feasibility work was conducted by the Canadian Centre for Justice Statistics with the assistance and guidance of Yves Gauthier of Small Business and Special Surveys Division at Statistics Canada. Recommendations regarding the methodology were provided by Lyne Guertin of Business Surveys Methodology Division at Statistics Canada. A portion of the study was funded by the Commercial Crime Branch of the Royal Canadian Mounted Police. The Centre for Justice Statistics is grateful to the members of the following two committees of the Canadian Association of Chiefs of Police for their support, guidance and participation in this project: the Police Information and Statistics Committee and the Private Sector Liaison Committee. Thank you to the representatives from the many businesses and the various government and law enforcement agencies that participated in the consultations and focus testing sessions conducted for this study, as well as to those who comprised the Advisory Committee for this study.

Abstract

This feasibility report provides a blueprint for improving data on fraud in Canada through a survey of businesses and through amendments to the Uniform Crime Reporting (UCR) Survey. Presently, national information on fraud is based on official crime statistics reported by police services to the UCR Survey. These data, however, do not reflect the true nature and extent of fraud in Canada due to under-reporting of fraud by individuals and businesses, and due to inconsistencies in the way frauds are counted within the UCR Survey. This feasibility report concludes that a better measurement of fraud in Canada could be obtained through a survey of businesses. The report presents the information priorities of government departments, law enforcement and the private sector with respect to the issue of fraud and makes recommendations on how a survey of businesses could help fulfill these information needs.

To respond to information priorities and to try to fill the gap in data on fraud, the study recommends surveying the following types of business establishments: banks, payment companies (i.e. credit card and debit card companies), selected retailers, property and casualty insurance carriers, health and disability insurance carriers and selected manufacturers. The report makes recommendations regarding survey methodology and questionnaire content, and provides estimates for timeframes and cost.

The report also recommends changes to the UCR Survey in order to improve the way in which incidents are counted and to render the data collected more relevant with respect to the information priorities raised by government, law enforcement and the private sector during the feasibility study.

Background

With globalization, the growing use of technology and the increased sophistication of certain criminal activities, the issue of fraud has become a growing concern for several countries, including Canada. Examples of initiatives indicating that fraud is a growing priority for Canada include bilateral work with the United States and other countries on telemarketing, mass-marketing fraud and identity theft (Bi-national Working Group on Cross-Border Mass Marketing Fraud, 2003 and 2004) and the establishment of Canada's Fraud Prevention Forum.[1] Further, in 2004, the government launched the *Anti-Spam Action Plan for Canada* which was overseen by a government-private sector Task Force on Spam and which resulted in a report containing 22 recommendations on possible action by government regarding the issue of spam (Task Force on Spam, 2005)[2]. Also in 2004, the United Nations' Economic and Social Council adopted a resolution on "international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes." That resolution included the establishment of an intergovernmental expert group to conduct a study of fraud and identity crimes, and the study is presently seeking data from Canada and other countries. Currently, however, there is little data that can be used to fully understand the nature and extent of fraud in Canada.

Presently, Canada relies on police-reported data for this type of information. This is problematic in that fraud is a crime that frequently does not get reported to the police by the individuals or businesses that fall victim. Incidents may not get reported to police for various reasons, such as private companies employing their own investigative personnel and individuals reporting incidents such as credit card fraud only to their financial institution. Data on the extent to which incidents are reported to the police are limited, yet the data that exist point to under-reporting. For instance, the 2000 International Crime Victimization Survey (ICVS) measured the number of victims of consumer fraud. The Canadian component of the ICVS found that of the 7.5% of Canadians that fell victim to consumer fraud in the 12 months prior to the survey, 13% had reported to the police and 20% had reported to an authoritative body other than the police (e.g. a consumer protection agency) (Van Kesteren et. al, 2000). In the United States, results from a 2003 survey by the Federal Trade Commission show that only 2.4% of victims of consumer fraud reported to either a consumer protection agency or local police and that victims were more likely to complain to the seller or manufacturer (53.7%), to a bank or financial institution (18.6%) or to no one at all (29.3%) (Anderson, 2004).[3] According to Pricewaterhouse Coopers' 2005 Global Economic Crime Survey, almost four-in-ten Canadian organizations surveyed did not report incidents of fraud to law enforcement agencies (2005).

The under-reporting of credit card fraud to the police is illustrated by the gap between Canadian police-reported data and data from the Canadian Bankers' Association (CBA). Police-reported data suggest there were 29,500 incidents of credit card and debit card fraud in 2004.[4] In contrast, the CBA indicates there were 177,000 Visa and Mastercard credit cards alone that were used fraudulently that year.[5]

In Canada, police-reported data on the incidence of fraud suggest that fraud has been decreasing in the past decade (Figure 1). This trend is more likely a reflection of the changing nature of fraud (i.e., the dramatic decrease in cheque fraud as shown in Figure 2) and, as suggested above, the non-reporting to police of current types of fraud, such as credit card fraud. The way Canadians do business is changing, with the use of cheques among consumers declining and the use of credit cards, debit cards and Internet transactions increasing. For instance, in 2004, there were 53.4 million Visa and Mastercard credit cards in circulation, almost double the number in circulation 10 years earlier and over eight and a half times

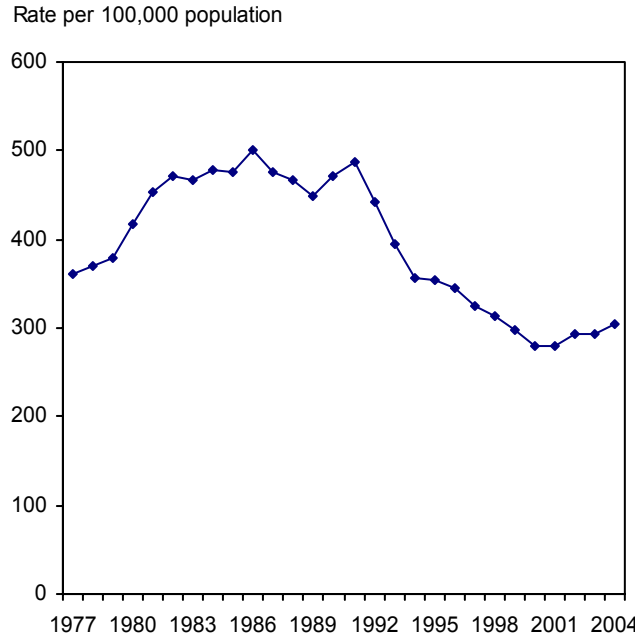
1. The Competition Bureau Canada chairs the Fraud Prevention Forum, a group of private sector firms, consumer and volunteer groups, government agencies and law enforcement organizations committed to fighting fraud aimed at consumers and businesses. Its mandate is to prevent Canadians from becoming victims of fraud through awareness and education, as well as to increase reporting when it occurs. The Fraud Prevention Forum grew out of the Deceptive Telemarketing Forum that was established in 1997.
2. Spam is considered any bulk commercial e-mail sent without the express consent of recipients. Spam is a concern with respect to its role as a mass-marketing vehicle that is used by some to defraud consumers and businesses through deceptive spam.
3. Total exceeds 100% due to multiple responses.
4. Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.
5. Statistics published by the Canadian Bankers' Association and are available at www.cba.ca. The 12-month reporting year for police-reported data ends December 31 whereas the reporting year for the data published by the Canadian Bankers' Association ends October 31.

more than in 1977.[6] Further, according to a survey conducted by the firm Strategic Council, 86% of Canadians have a banking card.[7] The CBA reported over 1.1 billion transactions at bank-owned Automatic Teller Machines in 2004, compared to almost 770 million in 1993.[8] According to a 2004 CBA Technology Survey, the proportion of Canadians who do their banking primarily through the Internet has almost tripled from 8% in 2000 to 23% in 2004 (Canadian Bankers Association, 2005).

The Internet is also becoming part of our daily lives and Canadians are increasingly using the Internet to make purchases and conduct sales. Overall, Internet use among Canadians has grown substantially since 1994 when about 18% of the population aged 15 and over was using the Internet compared to 53% in 2000 (Dryburgh, 2001). In 2004, six-in-ten Canadian households were connected to the Internet, up from just four-in-ten in 2000 (Statistics Canada, 2005a). According to Statistics Canada's 2003 Household Internet Use Survey, 64% of Canadian households had at least one member who was a regular Internet user in 2003, be it from home, work, school, or any other location. This represented a 5% increase from 2002 and more modest gains from the growth recorded in 2000 (+19%) and 2001 (+24%) (Statistics Canada, 2004a).

In 2003, Canadians spent just over $3.0 billion shopping on the Internet, a 25% increase over the $2.4 billion spent the year before (Statistics Canada, 2004b).[9] This growth in Internet purchases was driven by both a growth in the number of households that made purchases (from 2.8 million in 2002 to 3.2 million in 2003) and the total number of orders (from 16.6 million orders to 21.1 million). Despite these increases and the increase in payments over the Internet, Canadians remain wary of making purchases on-line. More than three-quarters of the 2.7 million households that paid for goods and services on-line indicated that they were either concerned or very concerned about the security of financial transactions over the Internet. From the business side, according to Statistics Canada's Survey of Electronic Commerce and Technology, on-line sales by private firms increased 46% in 2004, rising from $18.2 million in 2003 to $26.4 million (Statistics Canada, 2005b). The amount of on-line sales reported in 2004 was five times higher than in 2000.

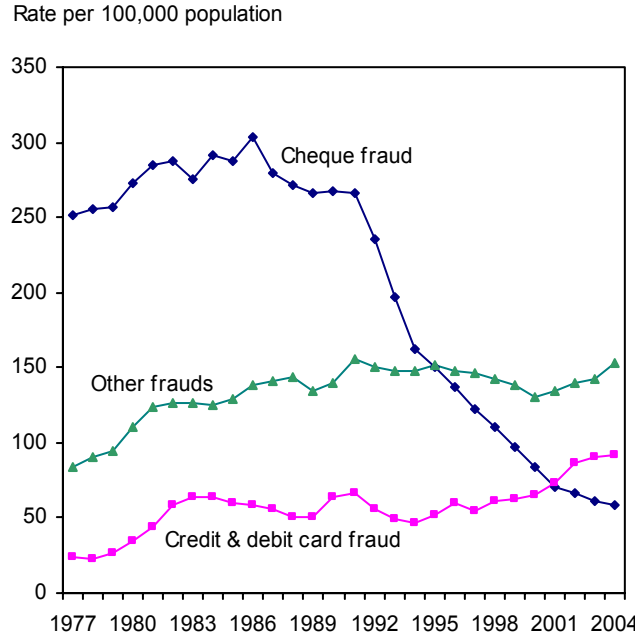
Figure 1. Police-reported data on fraud suggest fraud decreased substantially from 1991 to 2001



Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

6. Statistics published by the Canadian Bankers' Association and are available at www.cba.ca.
7. Among these, the survey found that 47% prefer to use Interac Direct Payment as their main method of paying for purchases, 29% prefer to use cash, about 20% prefer to use credit and less than 5% prefer to use cheques. Statistics available at www.interac.org.
8. Statistics published by the Canadian Bankers' Association and available at www.cba.ca.
9. Includes shopping on foreign web-sites.

Figure 2. Police-reported data suggest rate of cheque fraud falling while credit and debit card and other fraud have increased slowly in recent years



Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

In response to the gap in information on the nature and extent of fraud in Canada, the Canadian Centre for Justice Statistics (CCJS) undertook a study in 2005 to assess the feasibility of improving the measurement of fraud in Canada by collecting data from other sources such as businesses and business associations. A second objective of the study was to make recommendations to improve the collection of police-reported data through the UCR survey. This study was undertaken with the endorsement of the Police Information and Statistics (POLIS) Committee and the Private Sector Liaison Committee (PSLC) of the Canadian Association of Chiefs of Police (CACP), and with the approval of the National Justice Statistics Initiative (NJSI). Funding contributions were provided by the Royal Canadian Mounted Police (RCMP). This report describes the feasibility project, its findings and recommendations.

Overview of the feasibility study

This feasibility study included two main phases.

Phase 1: Consultations

The first phase consisted of consultations with representatives in the areas of law enforcement, government and the private sector. The objective of the consultations was to determine information priorities regarding businesses as victims of fraud, whether or not this information is tracked by businesses or associations, and their ability or willingness to share the information with Statistics Canada. Those consulted were selected as a result of their representation on relevant committees and working groups and based on referrals by experts in the area of fraud regarding others to consult. Representatives from the following organizations agreed to take part in the consultations:

Public sector (excluding health)

- Public Safety and Emergency Preparedness Canada
- Canada Revenue Agency
- Justice Canada
- Competition Bureau Canada
- Manitoba Justice

Law enforcement

- Police Information and Statistics Committee of the Canadian Association of Chiefs of Police
- Private Sector Liaison Committee of the Canadian Association of Chiefs of Police
- Royal Canadian Mounted Police, Commercial Crime Branch
- Ontario Provincial Police, Anti-Rackets Investigation Section; PhoneBusters; Health Care Fraud Investigations Unit

Finance

- Bank of Canada
- Canadian Imperial Bank of Commerce (CIBC)
- Royal Bank of Canada (RBC)
- Visa Canada
- Mastercard Canada

Retail

- Retail Council of Canada
- Sears Canada
- Staples Business Depot

Property and casualty insurance

- Insurance Bureau of Canada
- The Economical Insurance Group
- The Cooperators Insurance Corp.
- TD Meloche Monnex Group
- Allstate Insurance Corp.

Health insurance[10]

- Ontario Workplace Safety and Insurance Board
- The Canadian Health Care Anti-Fraud Association
- ESI Canada
- Equitable Life
- ClaimSecure Inc.
- Workers Compensation Board, PEI
- Workers Compensation Board, NWT & Nunavut
- Emergis

10. Responses from the agencies listed from Equitable Life to The Empire Life Insurance Company were provided electronically through coordination by the Canadian Health Care Anti-Fraud Association while all other consultations for this and the other sectors were conducted face-to-face. This accounts for the greater number of responses from the health care sector.

- Department of Health, New Brunswick
- Department of Health, Alberta
- College of Dental Hygenists of Ontario
- Green Shield Canada
- The Empire Life Insurance Company

Manufacturing

- Celestica Inc.
- Motorola Canada Limited
- IBM
- Husky Injection Molding Systems Ltd.

Other

- Telus
- Canadian Federation of Independent Business

Based on the results of this consultation, the CCJS determined that there were no complete and comparable centralized sources of information, such as associations representing certain industry types. It was therefore felt that a national data collection strategy would require the collection of standard data directly from businesses.

Phase 2: Drafting a questionnaire

The second part of this project, therefore, involved drafting a questionnaire based on the information needs articulated during the consultation process and then testing the questionnaire with businesses that represented the types of industries that were of interest and the various sizes of businesses of interest. One-on-one interviews to test the questionnaire were held with 23 randomly selected businesses. In addition, two focus groups were held - one with representatives from the property and casualty insurance industry and one with representatives from the health insurance industry. Testing was conducted in Ottawa, Toronto and Montréal. This focus testing helped to improve understanding of the feasibility of data collection and to further refine the questionnaire. The following is a description of the types of organizations included in the testing of the draft questionnaire:

	Total sessions	Size of business		
		Small	Medium	Large
Banking	3	0	2	1
Insurance property & casualty: 1 focus group consisting of representatives from 6 medium to large organizations	1	…	…	…
Insurance (health): 1 focus group consisting of representatives from 5 medium to large organizations	1	…	…	…
Retail	10	4	5	1
Manufacturing	7	4	3	0
Telecommunications, Internet service providers, web search portals and data processing services	3	2	1	0
Total	**25**	**10**	**11**	**2**

… not applicable

This feasibility report presents the results of both phases of this project. Based on these results, the report presents recommendations, cost estimates and timeframes required for Statistics Canada to measure fraud according to data reported by businesses. Finally, this report includes an analysis of data reported by police to the Uniform Crime Reporting Survey and, based on the information priorities

expressed by those consulted, makes recommendations on how these data could be improved to better inform issues regarding fraud.

It should be noted that while a survey of businesses will improve the measurement of fraud in Canada, it will not provide a complete picture. First, this study does not address the utility of a household survey since this study began with the goal of investigating the feasibility of collecting data from other sources that may already be compiling or tracking information on fraud. It is important to recognize that a household survey on fraud would capture certain types of fraud to which the general public is more likely to fall victim than businesses, such as consumer and mass-marketing fraud. In addition to providing detailed information on the nature and extent of fraud experienced by Canadians at large, the micro-data collected through a household survey would provide information on factors that increase one's risk of victimization, monetary losses, non-monetary consequences and the extent to which incidents are reported to police or others. Second, the recommendations in this report are designed to respond to the information priorities of government, law enforcement and the private sector while balancing respondent burden and the feasibility of accurate responses. As such, within the vast variety of businesses and frauds that exist, the recommendations focus on surveying certain types of businesses and collecting data on certain types of fraud.

Findings

Data sources and data availability

One of the objectives of the consultation process was to find out if centralized sources for data exist. In other words, are there associations or other centralized agencies that already collect data on fraud from businesses? Another objective was to determine whether or not businesses were able and willing to provide data on frauds they experienced.

Consultations revealed that, in terms of the private sector, there are few centralized sources of data. Further, the centralized information that does exist is limited and not necessarily complete or comparable across businesses. For instance, the Retail Council of Canada conducts an annual voluntary survey of its members to measure fraud and other security and crime issues facing retailers. However, participants in the survey are a handful of Canada's largest retailers, therefore the data are not representative of the retail sector. Payment companies, on the other hand (i.e. credit card and debit card companies), are a robust source of information for all credit card and debit card frauds in Canada. The credit card companies interviewed indicated that they collect detailed information. It appears that their data definitions are complete and comparable across companies. The information from the credit card companies would therefore contribute significantly to our understanding of the nature and extent of credit card fraud in Canada. With respect to the three other types of industries that were of interest to those consulted (i.e., manufacturing, health insurance and property and casualty insurance), there are no centralized sources of data on fraud. However, representatives from these industries felt they could provide data through an analysis of their files and reports (Table 1).

Table 1: Types of information either currently tracked or could be tracked or calculated, by type of industry representatives consulted[1]

	Type of information						
Types of fraud	Basic count of incidents of fraud	Dollar amount lost	Identity theft information	Other details on method or source of fraud	By province	By other geographic boundaries	By merchant type
Credit card fraud - major credit cards	Major credits card companies; banks; major retailers	Major credits card companies; banks; major retailers	Major credits card companies	Major credits card companies	Major credits card companies; banks	Major credits card companies; banks; major retailers	Major credits card companies
Credit card fraud - private label	Major retailers	Major retailers	.	.	Major retailers	Major retailers	.
Bank card fraud[2]	Banks	Banks	Unknown if available	Unknown if available	Banks	Banks	Unknown if available
Fraudulent cheques	Banks; major retailers; manufacturers	Banks; major retailers; manufacturers	.	.	Banks; major retailers	Banks; major retailers	.
False applications	Major credits card companies; banks	Major credits card companies; banks	.	.	Major credits card companies	Major credits card companies	Major credits card companies
Mortgage fraud	May be available from some banks	.	May be available from some banks	...	May be available from some banks	May be available from some banks	...
Worthless deposits in Automatic Teller Machines	Banks	Banks	...	.	Banks	Banks	.
Account takeovers	Major credits card companies; banks	Major credits card companies; banks	.	.	Major credits card companies; banks	Major credits card companies; banks	Major credit card companies
Impersonations (general and not by type of transaction)	Banks	Banks	.	...	Banks	Banks	...
Counterfeit currency	Banks, major retailers	Banks	...	...	Banks, major retailers	Banks, major retailers	...
False billing	Major retailers; manufacturers	Unknown if available	...	Unknown if available	Major retailers; manufacturers	Major retailers; manufacturers	...
Internal fraud	Major retailers; banks	Major retailers; banks	.	Unknown if available	Major retailers; banks	Major retailers; banks	...
Insurance claim fraud (property and casualty)	Major private insurance companies	Major private insurance companies	.	Major private insurance companies	Major private insurance companies	Major private insurance companies	...
Insurance claim fraud (health and disability)	Major health and disability insurance companies; Workers' Compensation Boards	Major health and disability insurance companies; Workers' Compensation Boards	.	Major health and disability insurance companies; Workers' Compensation Boards	Major health and disability insurance companies; Workers' Compensation Boards	Major health and disability insurance companies; Workers' Compensation Boards	...
Product piracy/counterfeit goods	Manufacturers	Manufacturers	...	Unknown if available	Manufacturers	Unknown if available	...
Theft of intellectual property	Manufacturers	Manufacturers	...	Unknown if available	Unknown if available	Unknown if available	...

. not available for any reference period

... not applicable

1. Availability of data is based on responses of those consulted during the 2005 Study to Examine the Feasibility of Measuring Fraud Experienced by Businesses and not of industries as a whole. Data collected by OPP's National Anti-Fraud Centre and RCMP's RECOL are not included in this table as these data are considered police-reported data, which are under-reported, and are already being submitted to the UCR survey.

2. Although Interac was not consulted during this project, it is assumed information on basic counts of fraud are available based on newspaper reports.

The Royal Canadian Mounted Police (RCMP) and the Ontario Provincial Police (OPP) currently operate two separate initiatives that are centralized reporting vehicles for victims of fraud. The RCMP operates the web-based Reporting Economic Crime On-line (RECOL) and the OPP and the RCMP jointly operate PhoneBusters. In 2005, these two initiatives standardized the complaint information they collect, yet the two databases remain separate for now. Victims can report economic crimes to either initiative by phone, Internet, fax or e-mail. The PhoneBusters system adopted the technology of RECOL to perform

automated information analysis and distribution of this information to relevant investigative parties (upon consent by the victim).

The RECOL and PhoneBusters databases are valuable investigative tools and can provide statistics on the different types of frauds (such as advance fee schemes, identity fraud and health fraud). They can also provide statistics on dollar values lost, characteristics of the victim, and the geographic location of the incident. However, the information contained in these databases represents the incidents that are reported to these police initiatives. It is assumed that they are not representative of fraud in Canada, particularly fraud committed against businesses, due to low rates of reporting to police by businesses. Further, these initiatives do not necessarily represent all police-reported frauds in Canada as individuals and businesses that choose to report to police may report to their local police service rather than these larger initiatives.

Despite the lack of centralized sources of data, several large companies indicated that they track information on fraud. For those that do not currently track it, some have plans to collect it. Small to medium companies that did not track incidents of fraud indicated that they felt they had enough knowledge to be able to reliably report the number of incidents they experienced in the last year. Overall, the majority of companies consulted in the first phase of the project and those who participated in the second phase of the project (i.e. the testing of a draft questionnaire) saw value in such data collection and stated that they would be willing to participate.

With a few exceptions, the banking industry in general, including the Canadian Bankers' Association (CBA), declined participation in this feasibility study. The banks that participated indicated that they collect data on incidents of fraud, but felt that there would need to be some consensus across the industry with respect to reporting to Statistics Canada for the purpose of a national data collection strategy. While it is CCJS' understanding that the CBA regularly collects data on incidents of fraud from its members, meaning there exists a centralized source of data, the nature, coverage and quality of these data are unknown. Further, the quality of data from individual banks and the extent to which categories are standardized across banks requires further investigation. While the banking sector is an important component to measuring fraud against businesses, the lack of participation should not preclude a data gathering exercise from going forward, particularly if credit card and debit card companies are willing to take part.

Recommendation: Given the amount of data that businesses would be able to report, it is recommended that a survey of businesses be conducted to gather data to measure the nature and extent of fraud experienced by businesses. It is recommended that a pilot survey first be conducted prior to embarking on a national survey. These data would provide insight into frauds that are likely not reported to police as well as incidents of certain crimes that affect the general population such as credit card and debit card fraud. It is recommended that the CCJS continue efforts to liaise with the banking industry regarding this project.

Objectives for data collection

Those consulted were presented with five possible objectives for measuring fraud against businesses. The five objectives presented to those consulted were:

1) Improve public awareness regarding the nature, extent and impact of fraud regarding businesses, particularly new and emerging types of fraud.

2) Provide information to enhance the capacity of law enforcement, government, businesses and associations to develop and assess methods of detection and prevention.

3) Provide information for public administrators to make information-based decisions with respect to policy and legislation regarding fraud.

4) Improve the detection and reporting of fraud.

5) Work toward consistent data recording practices.

The majority found it difficult to rank these in terms of importance and found all to be worthwhile objectives. Through discussions of issues, many expressed that the data are needed to meet the objectives listed in 2) and 3). Another made the important point that without objective 5) being the most important, the other objectives would be difficult to fulfill. It should also be noted that several businesses mentioned that a national survey would help them with standardizing their data collection practices.

Industries to include in a national data collection strategy

According to the Statistics Canada Business Registry, there are about 2.2 million commercial establishments in Canada and among them there are approximately 1.2 million that are employers. Because each varies in terms of the products and services they offer, each would vary in terms of the nature and extent of fraud they experience. While it would be ideal to survey all types of businesses regarding their experiences as victims of fraud, this would be cost-prohibitive. As such, stakeholders were consulted regarding which sectors and industries they felt were most important to include in measuring fraud against businesses. The following sectors were either ranked highly or most frequently by stakeholders. Several participants, however, had difficulty identifying which specific types of businesses within the sectors should be included. The following sectors were identified primarily because it was felt they are targets or at risk of being defrauded and that it is important to track the nature and extent of victimization among these particular sectors:

1) Banking, including payment companies (i.e. credit card and debit card companies)
2) Insurance (i.e. property and casualty insurance, and health care insurance)
3) Retail
4) Manufacturing
5) Real estate, rental and leasing
6) Information industries (i.e. telecommunications, Internet services providers, Web search portals)

Banking

Inclusion of the banking industry was not only rated frequently, but highly in terms of importance. The credit card companies consulted were open to the idea of sharing data with Statistics Canada to produce national statistics. As mentioned earlier, however, there was little participation by banks in the consultation and focus testing exercises, and the extent to which banks would participate in a national survey needs to be further explored. However, it is the CCJS' understanding that data on fraud are tracked by banks.

Recommendation: Include payment companies (i.e. credit card and debit card companies) in a national data collection strategy. Re-assess the banking industry's interest in participating in a data collection exercise prior to conducting a pilot survey. Include banks in a pilot survey and evaluate their inclusion in a national survey based on results from the pilot test.

Insurance

Along with banking, this industry was ranked frequently and highly in terms of importance. The insurance sector is divided between "property and casualty" insurance and "health and life" insurance. Consultations revealed that these should be treated separately. However, consultations also revealed that many provincial health insurers do not track information on fraud, but that cases are reported to the police. Further, focus testing with representatives from the health insurance sector recommended that data collection focus on health and disability insurance and, for now, exclude life insurance as they did not consider fraud in this area as a pressing issue. As well, other stakeholders specifically identified the issue of health insurance, not life insurance, as an information priority. Focus testing further revealed that insurance brokers should be excluded from data collection activities to avoid double counting.

Recommendation: Include private and public property and casualty insurers. Include private health care insurers, workers' compensation boards and Blue Cross. Exclude public health insurers. Exclude insurance brokers.

Retail

Next to banking and insurance, the retail industry was rated frequently and highest. Respondents found it difficult to identify which types of retailers should be included. Rather, several suggested targeting either the largest companies, or ones that have broad spectrum of products (e.g. department stores, warehouse-type stores, electronic stores, etc.). While the representatives from retail selected certain types, they also felt that the larger companies would best be in a position to report data. Further, there was interest in stores that do sales over the Internet.

Recommendation: Given the vast variety of retailers, it is recommended that a data collection activity target those that deal in "big ticket" items or a variety of items, as per the listing under the section "Identification of priority industries according to their North American Industry Classification Standard (NAICS) codes". Specifically, it is recommended that establishments within the following industry classifications be included: Furniture and Home Furnishings Stores, Electronics and Appliance Stores, Building Material and Garden Equipment Suppliers and Dealers, Health and Personal Care Stores, Clothing and Clothing Accessories Stores, General Merchandise Stores, and Office Supplies, Stationary and Gift Stores.

Manufacturing

The manufacturing sector was rated frequently in terms of importance, but not necessarily highly. Regarding which types of manufacturers to include, stakeholders in manufacturing suggested to target those where intellectual property is a concern, such as innovative companies. They also suggested including those that are Canadian-based in order to understand the impact on Canadian businesses. Further, for several stakeholders consulted, the importance of manufacturers was raised in terms of the issue of product piracy and how counterfeit products can compromise public safety.

Recommendation: Include manufacturers of selected types of products, as per the listing under the section "Identification of priority industries according to their North American Industry Classification Standard (NAICS) codes". Specifically, it is recommended that establishments within the following industry classifications be included: Machinery Manufacturing, Computer & Electronic Product Manufacturing, Electrical Equipment, Appliance and Component Manufacturing, Transportation Equipment Manufacturing, and Medical Equipment and Supplies Manufacturing.

Real estate, rental and leasing

This sector was rated frequently, but not necessarily highly. Issues with respect to this industry related largely to the role of identity fraud in mortgage fraud and in the rental and leasing of vehicles. Also, one stakeholder raised the issue of real estate investment fraud as important. In such cases, victims could include banks and other financiers, contractors, and construction and trades people. The topic of investment fraud can become quite complicated and does not necessarily solely involve the real estate industry as the victims.

Recommendation: Exclude real estate, rental and leasing from a data collection activity. Attempt to measure mortgage fraud through the banking industry.

Information industries

This sector was raised a number of times and sometimes ranked highly. Within this sector, stakeholders identified companies providing telecommunications, Internet services and Web search portals as important because they felt these are targets for fraud. However, consultations and focus testing with these areas revealed that fraud is not an issue for them.

Telecommunications service providers do not consider themselves as targets of fraud since illegitimate calls made by a third party on a legitimate account holder's account are usually the responsibility of the account holder and are not tracked. Further, stores that sell telecommunications products and services

for a larger provider do not see themselves as the victim as any questionable account activity is dealt with by the provider.

Focus testing with Internet and Web service providers revealed that, although fraudulent transactions can take place over the Internet, these businesses are not the targets of fraudulent activity.

Recommendation: Exclude telecommunications, Internet and Web service providers from a data collection activity.

Based on findings from the consultation process and focus testing, it is recommended that the following types of businesses, identified according their North American Industry Classification Standard (NAICS) code, be included in a national data collection strategy:

Identification of priority industries according to their North American Industry Classification Standard (NAICS) codes

Manufacturing:

333 Machinery Manufacturing
334 Computer & Electronic Product Manufacturing
335 Electrical Equipment, Appliance and Component Manufacturing
336 Transportation Equipment Manufacturing
3391 Medical Equipment and Supplies Manufacturing

Retail:

442 Furniture and Home Furnishings Stores
443 Electronics and Appliance Stores
444 Building Material and Garden Equipment Suppliers And Dealers
446 Health and Personal Care Stores
448 Clothing and Clothing Accessories Stores
452 General Merchandise Stores
4532 Office Supplies, Stationary and Gift Stores

Banking:

5221 Depository Credit Intermediation

Payment companies (i.e. credit card and debit card companies):

5222 Non-Depository Credit Intermediation

Health insurance:

52411 Direct Life, Health and Medical Insurance Carriers

Property and casualty insurance:

52412 Direct Insurance Carriers (Except Life, Health and Medical)

Size of business

The size of a business can be classified in a number of ways, such as according to the number of employees or according to the size of financial assets or other financial indicators. The vast majority of those consulted agreed that, for the purpose of a Survey of Fraud Against Businesses, the number of employees should be used to classify businesses by size. At Statistics Canada, there are no standards

for defining small, medium and large businesses according to the number of employees. Industry Canada, however, defines small businesses as those having 1 to 100 employees[11], medium business as having 101 to 499 employees and large businesses as 500 or more employees (Industry Canada, July 2005). Within the range for small businesses, Industry Canada includes "micro businesses" which are defined as businesses having less than 5 employees.

Among the consultations where there was discussion regarding the size of businesses to include, the majority said that all sizes should be included and about one-third suggested collecting data from the largest businesses only. Those who wanted all sizes included felt that this would be more representative and would permit analysis of differences across business of different sizes. It was stated that this analysis is needed to improve targeting of awareness/education and investigation. Those who thought we should focus only on the largest businesses felt that we would obtain the vast majority of incidents in terms of volume and that the largest businesses would likely track data on fraud and have the resources to provide information.

Representatives from the Canadian Federation for Independent Business (CFIB), an organization that advocates for independent businesses that have employees ranging in numbers from about 6 to 100, indicated that their membership would only see value in participating in such a data collection activity if they would benefit directly from the results in a tangible way (e.g. education/prevention materials, changes in the laws, changes in law enforcement policies and procedures, etc.). In addition, representatives were unsure of their membership's ability to provide data.

Consultations and focus testing did not reveal any evidence to argue at this point that large businesses are in a better position to report incidents of fraud to a national survey than small businesses. Some large businesses tracked information while others did not. Because of their large operations, those that did not track the information would likely have to rely on information from accounting files to extract counts of fraud or would simply not be able to report counts. The small businesses included in the focus testing part of the feasibility study did not see fraud as a large issue for them, but did see the benefits of a national data collection strategy and said they would respond to such a questionnaire, a perspective which differs from that provided by the CFIB above. While most did not track the information in a systematic way, operations were small enough that they could recall any incidents that took place in the previous year.

Recommendation: Size ranges representing small, medium and large business should be included in the pilot survey. The delineation of size should be based on number of employees. It is recommended that businesses with less than 5 employees be excluded from a data collection exercise as these are subject to frequent start-up and closure and could affect response rates. For the purpose of a Survey of Fraud Against Businesses, businesses should be categorized by size as follows: small (5 to 100 employees), medium (101 to 499 employees), and large (500 or more employees).

For analytical and data quality assessment purposes, it is also recommended that the classification of "small" be further broken down into "very small" (i.e., 5 to 50 employees) and "somewhat small" (i.e., 51 to 100 employees). Small businesses comprise the vast majority of commercial establishments within Statistics Canada's Business Registry and there may be differences among the "very small" and "somewhat small" establishments that are worth examining.[12] The inclusion of a variety of size ranges would better respond to the objectives of the survey. Further, there is currently not enough evidence to argue that small businesses are in a lesser position to be able to report incidents of fraud than larger businesses. However, the inclusion of small businesses will increase the cost of a national survey which is why it will be important to use the results of a pilot survey to assess the benefits of including them in a national survey.

11. This is the range Industry Canada attributes to goods-producing firms. For service-producing firms, Industry Canada classifies small businesses as those with 1 to 50 employees.
12. Under the section "Survey frame and sampling units for a pilot survey," the report will discuss the use of the Business Register as the recommended survey frame and the statistical unit of "establishment" within the Business Register as the recommended sampling unit.

Types of fraud to measure

Those consulted were presented with a list of various types of fraud to which businesses can fall victim. Some types of fraud are specific to certain businesses (e.g. insurance claim fraud). Participants were asked to indicate which were most important to include in measuring fraud against businesses, based on the types of businesses they ranked as important to include. Businesses that participated in the consultation process and the focus testing were also asked about the feasibility of reporting counts by type of fraud.

The types of fraud that were identified most often as being important to measure were:

1) Identity theft/false applications (particularly mortgage fraud)
2) Fraudulent use of credit and debit (i.e. bank) cards
3) Fraudulent use of cheques
4) False billing
5) Insurance claim fraud

Identity theft

Information on identity theft was deemed very important. However, focus testing revealed that it would be difficult to capture this information through a Survey of Fraud Against Businesses since identity theft is an action that precedes and enables a fraud to occur. Often, businesses that are defrauded will not know if identity theft preceded or enabled the fraud to occur, or in their categorization of fraud incidents, they do not capture the element of identity theft. For instance, a bank may track the number of fraudulent applications for loans, but will not track how many of these are a result of the use stolen identity (e.g. a Social Insurance Number, driver's license information, etc. that belongs to someone else) versus the misrepresentation of information (e.g. lying about employment and annual salary). Perhaps the only exception would be the fraudulent use of credit card and debit card information since the unauthorized use of one's credit or debit card by a third party is essentially the result of either stealing the card information, or the use of one's personal information by a third party to apply for a credit card.

Fraudulent use of credit cards and debit cards

Regarding the fraudulent use of credit cards, the credit card companies consulted revealed that counts could be broken down by the type or source of the fraud and that these are fairly comparable across credit card companies. Categories are presented in question C1 of the draft questionnaire in Appendix 1. Whether debit card companies have comparable categories for type or source of debit card fraud remains to be determined. Information on fraudulent use of retail-specific credit cards (e.g. Sears card, HBC card, etc.) would need to come from the retailer, but frauds using major credit cards (e.g. Visa, Mastercard) can be obtained from the credit card companies. Credit card companies are also able to produce data according to their own classification of the type of business.

Cheque fraud

Despite the apparent decrease in cheque fraud, as indicated by police-reported data, consultations revealed that information on cheque fraud is still a priority. Consultations and focus testing suggested that such data could be easily provided by businesses.

False billing

False billing occurs when a business or an individual receives a bill for a product whereby the representation of the product by the promoter was either false or misleading, or whereby the products were either never ordered or received. According to investigative data, the issue of false billing of businesses for products such as paper, photocopy machine toner and business directories is an issue and was raised by those consulted. The representatives from businesses that participated in the

consultations and the focus testing sessions felt that this information would be available from office administrators and data availability would require the involvement of this area of their business.

Insurance claim fraud

Regarding insurance claim fraud, the categories and working definitions for the types of fraud were refined through two separate focus testing sessions - one with representatives from the property and casualty insurance industry and one with representatives from the health insurance industry. These appear in questions D1 and E1 of the draft questionnaire (see Appendix 1). It was agreed among the respective groups that these data would be feasible to gather and report. The questionnaire does not solicit a breakdown of insurance claim fraud by type, such as false billing, false applications and impersonations as some insurance companies felt they may not be able to provide this type of detail. However, it should be noted that these types of fraud would be specified within the overall definition of insurance claim fraud and that this definition will be included within a survey guidebook that will accompany the questionnaire.

Other types of fraud

In addition to the types of fraud discussed above, there were other types that were raised as pertinent issues. *Product piracy, counterfeit products and theft of intellectual property* were considered important in relation to the manufacturing and research and development sectors. As mentioned earlier, counterfeit products is a priority with respect to how it can impact public safety. Although not within the *Criminal Code* definition of fraud, the Bank of Canada is interested in statistics on *counterfeit currency*, particularly with respect to the experiences of retailers and banks.

Fraud committed by employees

Discussions with stakeholders revealed that counting fraud committed by employees was as important to include as fraud committed by parties external to the business. While stakeholders, including some representatives from the private sector, supported trying to obtain separate counts for internal fraudulent activities, such as asset misappropriation, focus testing revealed that this type of information may be difficult to collect. A number of businesses involved in focus testing indicated that these incidents are not always tracked and such questions could prove sensitive for some businesses and therefore could negatively affect response rates.

Volume of transactions as a context for counts of fraud

Counting the number of incidents of fraud in relation to a number that indicates the overall volume of transactions was also raised as important for providing context to the numbers and being able to calculate some type of rate. The insurance industry felt they could provide such a count and certain transaction counts (such as Automated Teller Machine (ATM), Direct Payment and credit card transactions) are tracked by the major banks and payment companies.

The importance of clear definitions

Several stakeholders from the private sector underscored the need to have at the outset of the questionnaire an explicit and clear definition of fraud in general, as well as for each type of fraud. Respondents will need direction to make the distinction between fraud and other types of economic crimes, such as incidents of straight theft that do not involve deceit.

Recommendations: It is recommended that a pilot survey attempt to collect the number of incidents of internal fraud and that the quality of these data and the effect of this question on response rates be assessed to determine whether or not these should be included in a national survey.

It is also recommended that, with the exception of the credit card companies, attempts to collect the number of fraud incidents as a result of identity theft be excluded from the pilot survey. Instead, data

could be collected on the use of false information in such things as applications, which does not require the respondent to have knowledge of whether or not the false information was obtained through theft of identity. Given the inability of businesses to provide counts of fraudulent incidents that transpired as a result of identity theft and that identity theft is a policy and enforcement priority, it is recommended that further consultations take place with stakeholders to assess which types of information beyond incident counts could prove useful in informing the issue. A newly developed question or set of questions should then be tested during the pilot survey phase.

With respect to the types of fraud to be measured, it is recommended that they be industry-specific. Examples of the types of fraud to be collected from each industry are presented in questions A1, A3, B1, C1, C2, D1, E1 and F1 of the draft questionnaire (see Appendix 1). The list of fraud types is based on information from participants regarding what is currently being collected and what is feasible to report. A clear definition of fraud and each type of fraud needs to be incorporated into the questionnaire. Based on results of a pilot survey, categories and definitions may require adjustment. Definitions need to be incorporated in the survey questionnaire or included in a survey guidebook that will accompany the questionnaire.

Other data requirements

The consultation process and the focus testing gathered input on other information priorities and the feasibility of reporting these data needs. This section presents the other information priorities that were raised.

Involvement of organized criminal groups

The involvement of organized criminal groups in fraud was raised during the consultations as a pressing issue. Despite the lack of comprehensive data on perpetrators, law enforcement has observed an increased involvement of organized criminal groups in the area of fraud not only to make money, but to use the proceeds to finance other criminal activities (Bi-national Working Group on Cross-Border Mass-Marketing Fraud, 2004 and 2003). Consultations revealed that data that could inform the extent of involvement of these groups in frauds perpetrated against businesses would be desirable and would inform the objectives of the survey. However, with the exception of the insurance industry, businesses indicated that they would be unaware of whether or not the incidents involved organized criminal groups and would therefore not be able to respond to such questions.

Due to the investigative work performed by the insurance industry, some information on this issue could be supplied by the health insurance industry and the property and casualty insurance industry. Within the survey, a criminal organization would be defined as it is in Section 467.1 of the *Criminal Code* of Canada.[13] The insurance industry frequently refers to organized criminal groups as “criminal rings” which fall within Canada’s definition of organized criminal groups. Questions D3, E2, E3 and E4 on the draft questionnaire are questions that were developed during focus groups with representatives from the respective insurance industries. These are based on what the respective industries felt they could reliably provide in terms of informing the issue of involvement of criminal rings/organized crime.

Recommendation: Include questions as presented in the draft questionnaire in a pilot survey and make revisions based on pilot test results.

International or domestic (Canadian-based) fraud

From a policy and law enforcement perspective, it is important to understand whether or not the frauds being committed in Canada are being perpetrated by individuals within or outside of Canadian borders.

13. Under Section 467.1 of the *Criminal Code of Canada*, “criminal organization” means a group, however organized, that (a) is composed of three or more persons inside or outside Canada; and (b) has as one of its main purposes or main activities the facilitation or commission of one or more serious offences that, if committed, would likely result in the direct or indirect receipt of a material benefit, including a financial benefit, by the group or by any of the persons who constitute the group. It does not include a group of persons that forms randomly for the immediate commission of a single offence.

With advancements in communication technology and globalization, the victimization of Canadians by Canadian-based fraudsters versus those from other countries is an issue that was raised during consultations and for which there is currently little data.

Results from focus testing reveal that many businesses would likely indicate that all incidents are perpetrated by a domestic source and that this conclusion would likely not be based on tracked information. The health insurance industry and the property and casualty industry did not feel this information could be tracked to provide counts and others involved in focus testing felt they would know if any incidents occurred, but would not be able to provide exact numbers.

Recommendation: Given the importance of this information for policy and law enforcement and the difficulty businesses would have in reporting reliable information, it is recommended that a question be included on the pilot survey asking respondents whether or not any of the incidents of fraud they experienced in the 12-month reference period were perpetrated by individuals residing outside of Canada (see questions A6, B5, C6 and F2 in Appendix 1). The response rate for this question can be assessed upon completion of the pilot survey.

Method by which fraud was committed

Information on how the fraud was committed, such as by Internet, e-mail, mail, phone, etc., was deemed important among those consulted. However, focus testing revealed that few businesses tracked the number of incidents of fraud according to how the fraud was committed. For some, the information could be gleaned from existing data categories. For instance, credit card companies have as one of their categories for fraudulent credit card incidents “card not present,” meaning purchases that were made over the phone or Internet whereby the credit card number, expiry date and name of cardholder were provided without a signature.

Recommendation: Given the importance of this information for policy and the difficulty businesses would have in reporting reliable counts, it is recommended that a question be included on the pilot survey to obtain an indication of whether fraud is committed more frequently through certain modes of contact than others (see questions A7, B6, C7, D4, E5 and F3 in Appendix 1). It is not recommended that the pilot survey attempt to gather counts of incidents in this respect.

Monetary impact of fraud

The monetary impact of fraud was raised as very important information among those consulted. Along with the number of incidents of fraud, the amount of money defrauded and not recovered is crucial to understanding the seriousness of fraud perpetrated against businesses. Comments were also received about the indirect financial costs of fraud to businesses, such as the need to invest in better security and detection measures and time spent in court.

During the focus testing, a few participants felt that this information would be sensitive and that businesses may be reluctant to reveal the direct monetary losses they incurred as a result of fraud. However, several did not see an issue with sharing this information provided there would be an opportunity to also indicate savings that were experienced as a result of fraud prevention and detection. During the focus testing phase, most participants indicated being more comfortable with reporting dollar ranges than exact dollar amounts.

Recommendation: Include questions to measure both the amount of dollars lost directly as a result of fraud and not recovered, and the estimated amount of dollar loss prevented as a result of fraud detection (see Questions G1 and G2 in Appendix 1). It should be noted at this time that all data provided by individual respondents, including financial information such as this, would be protected by the confidentiality provisions of the *Statistics Act*. It is also recommended to include a question to obtain an indication of areas where businesses incurred indirect financial losses as a result of fraud (see Question G3 in Appendix 1). Make revisions to the questions based on results of the pilot survey.

Non-monetary effects of fraud

The non-monetary effects of fraud can include effects on staff morale, business relationships, brand image and consumer confidence. During the consultation process, many indicated that this type of information was not as important relative to the number of incidents of fraud. Policy departments were more likely to see the value in these data than the private sector.

Recommendation: Include in a pilot survey a question to measure the non-monetary effects of fraud (see Question G4 in Appendix 1). Make revisions to the questions based on results of the pilot survey.

Fraud detection

During the consultation process, the ways in which fraudulent activity is detected by businesses was deemed very important to collect. It was felt that this would assist in understanding exposure to fraud and could inform education initiatives. Businesses saw this as an opportunity to compare themselves with their industry as a whole, with other industries and with businesses of different sizes. During the focus testing phase, these were viewed as questions that could reliably be answered and questions and response options were further refined as a result of the testing.

Recommendation: Include questions to identify measures that are in place that can detect fraud. See question H1 of the draft questionnaire (Appendix 1) for a draft question. Make revisions to the question based on results of the pilot survey.

Fraud prevention

The collection of information on the measures that business have in place that would prevent fraud was rated as important for the same reasons given for collecting data on fraud detection measures. During the focus testing phase, these were viewed as questions that could reliably be answered and questions and response options were further refined as a result of the testing.

Those consulted also saw value in including a question to assess businesses' opinions regarding new initiatives that could help in the prevention of fraud. This type of information would go a long way in policy decisions regarding prevention. Businesses included in the focus testing also saw this as a valuable question. However, a few were concerned that some respondents may not be familiar enough with various pieces of legislation to be able to rate their utility as a possible prevention measure.

Recommendation: Include questions to collect information on measures that businesses have in place that can prevent the occurrence of fraud. Also, include questions that can provide information on businesses' views of possible initiatives to combat fraud. See Section I of the draft questionnaire (Appendix 1) for draft questions. Make revisions to the questions based on results of the pilot survey.

Action taken when fraud is detected

An understanding of the actions taken by businesses when fraud is detected and the reasons for those actions was identified as very important information. This information would be used to understand the rate at which incidents are reported to the police, reasons for reporting or not reporting, and the extent to which incidents are reported to fraud-specific initiatives such as PhoneBusters or RECOL, or other agencies such as the Competition Bureau Canada or Better Business Bureaus, etc.

During the focus testing phase, these were viewed as questions that could reliably be answered and questions and response options were further refined as a result of the testing. During focus testing, businesses also felt it was important to ask the extent to which cases are pursued in civil court.

Recommendation: Include questions to understand actions taken by businesses when fraud is detected and reasons for reporting and not reporting to the police. See Section H of the draft questionnaire (Appendix 1) for draft questions. Make revisions to the questions based on results of the pilot survey.

Levels of analysis

Results from the consultations reveal that it is important to provide data not only at a national level, but also by province. Understanding regional differences in the nature and prevalence of fraud would be useful for policy and law enforcement initiatives, particularly since the administration of justice is the responsibility of the provinces and territories. Generating reliable estimates for the 10 provinces, however, would require a very large sample which in turn increases the cost of conducting a survey.

With respect to the different types of fraud, it is evident that these are not homogenous across industry types. Further, there is value in understanding differences across industry types and sizes of business in order to direct public education initiatives as well as policy and law enforcement efforts.

Recommendation: In order to respond to the need for sub-national data and to contain the cost of conducting a survey, it is recommended that a national survey produce estimates not only for Canada, but also by region. The six regions would comprise the Atlantic Region (i.e., Newfoundland and Labrador, Prince Edward Island, Nova Scotia and New Brunswick), Quebec, Ontario, the Prairie Region (i.e., Manitoba, Saskatchewan and Alberta), British Columbia, and the Territories (Yukon Territory, Northwest Territories and Nunavut).

To respect the heterogeneity of the industry types regarding the types of fraud to which they may be subject and to increase the utility of the information, it is recommended that the data also be stratified by the six industry types identified as important (i.e., banking, payment companies, retail, property and casualty insurance, health and disability insurance, and manufacturing) and that the data be stratified by size of business.

The quality of the data and the response rate can affect the ability to produce estimates by sector and size for each region. Therefore, to respond to information priorities, a survey should aim to provide estimates by industry type for each region, and to provide analysis by industry type and size at the national level only.

Survey frame and sampling units

The Business Register at Statistics Canada is the main survey frame (i.e., database) from which businesses are selected to participate in surveys. The Business Register is a structured list of businesses engaged in the production of goods and services in Canada. For all industrial sectors of the economy, the Business Register includes the following economic entities: incorporated businesses, unincorporated businesses, commercial enterprises, non-profit organizations, religious organizations, government departments and government institutions. The Business Register provides Statistics Canada with a comprehensive quality survey frame in terms of coverage and a set of stratification variables such as geographical classification, industrial classification based on the North American Industrial Classification System (NAICS) code, business income, number of employees and total assets.

Recommendation: It is recommended that Statistics Canada Business Register be used to create the survey frame for the pilot Survey of Fraud Against Businesses. The NAICS code should be used to extract the businesses classified in the industrial sectors of interest.

One way in which businesses are organized within the Business Register is according to statistical entities. Statistical entities are organized as follows: enterprise, company, establishment and location. Each statistical entity is designated as such because of the type of statistical information it supplies to Statistics Canada. Large businesses often have a complex structure and include many units in all four statistical entities. The establishment level supplies information on revenues and expenditures to Statistics Canada. It is defined as:

> A production entity (i.e., a physical unit where the business operations are carried out and which has a civic address and dedicated labour) or the smallest grouping of production entities which:
>
> a) Produces a homogenous set of goods or services;
> b) Does not cross provincial boundaries; and
> c) Is an entity which can provide data on revenues and expenditures (Statistics Canada, 2005c).

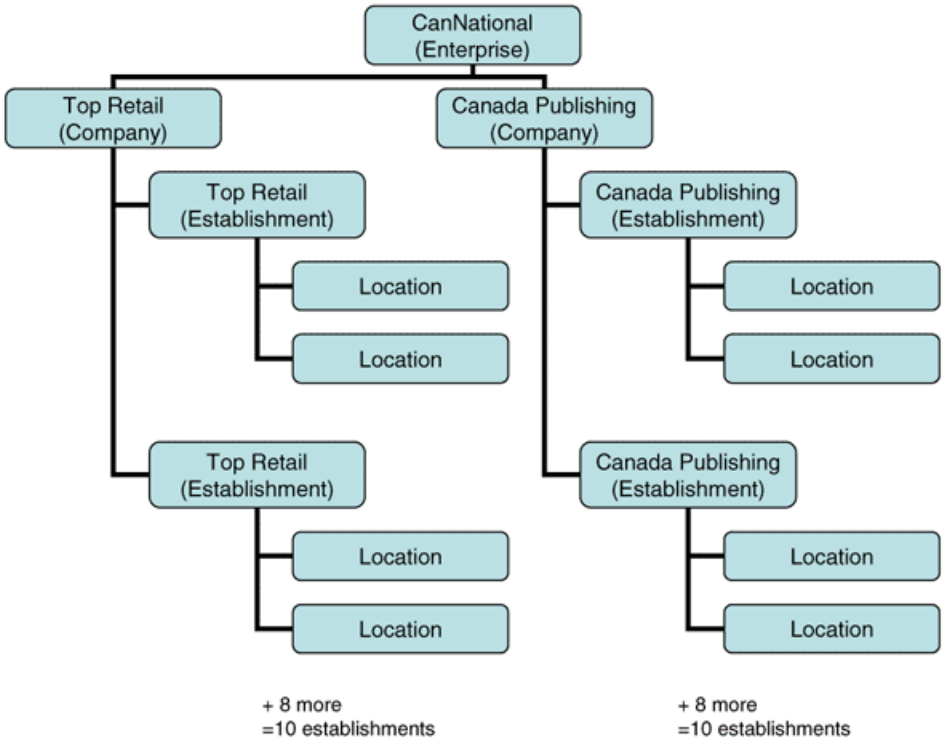
Recommendation: For the purpose of a Survey of Fraud Against Businesses, it is recommended that businesses be surveyed at the establishment level.

Surveying at the establishment level is recommended for three reasons. First, based on the feasibility work, it is anticipated that this will be the level at which information on fraud victimization will be available. Second, if it is not available at that establishment level but at a higher level, it is more useful analytically to be able to disaggregate the data to the establishment level. Third, the Business Register is undergoing a re-design which will be implemented in May 2008. The establishment level is a statistical entity which will be compatible with the new Business Register model. By choosing the establishment as the unit of count, it will not be affected by the upcoming changes to the Business Register's statistical units.

Statistical entities of the Business Register and challenges in surveying at the establishment level

It is important to understand the structure of statistical entities within the Business Register in order to appreciate some of the challenges that could be encountered with using the Business Register as the survey frame and the establishment as the survey unit. A common structure for a complex business is to have a number of companies of different NAICS codes under one enterprise. Under each company, there can be a number of establishments and under each establishment, there can be a number of locations. For simple businesses, the physical location represents all statistical units. In other words, there is usually a one-to-one relationship between each statistical unit.

To illustrate the complex structure of statistical entities under a large enterprise, the following fictitious example of an enterprise is provided. Under the business enterprise CanNational, there are two separate companies: Top Retail and Canada Publishing. Each of these companies has 1 establishment in each province amounting to 10 establishments nation-wide. Each of these establishments has a number of locations.



This example shows that there is not necessarily a one-to-one relationship between a store location and an establishment. An establishment, as defined by the Business Register, must be viewed as a statistical entity in terms of the fact that it is the source for revenue and expenditure information. For instance, in one province, there may be two Top Retail stores, but these are considered one establishment because the revenue and expenditure data are not available separately, but are combined at a higher level.

Consultations and focus testing revealed that, for larger businesses, data on incidents of fraud may be available at the individual location level only, or may be available at the national head office only. If the data being sought by a Survey of Fraud Against Businesses are not available at the establishment level (i.e., the business entity that received the survey questionnaire), the questionnaire could be filled out at a higher level in the organization. If this occurs, then Statistics Canada would need to disaggregate the data in order to create responses at the establishment level. Although the type of data being sought through a Survey of Fraud Against Businesses is new, the challenge of having to re-allocate data for complex businesses to the establishment level is not new to Statistics Canada.

We will use the fictitious establishment of Top Retail to illustrate some of the challenges of surveying the establishment level. For the purpose of a Survey of Fraud Against Businesses, only Top Retail is an industry we are interested in surveying because it is classified according to one of the North American Industrial Classification System codes we recommend surveying. Therefore, each of the ten establishments for Top Retail would receive a survey questionnaire. If each completes the questionnaire, the response pattern is clean. However, if the data on frauds are not kept at the establishment level, but are tracked by the head office for Top Retail (which, let's say in the Business Register represents the statistical entity of "company"), the 10 establishments may send their questionnaires to head office and head office may decide to complete just one questionnaire for all establishments. In such a case, Statistics Canada would need to follow-up with the head office and to try to re-allocate the data in order to come up with one response for each of the 10 establishments for Top Retail.

For some of Canada's largest enterprises, there exists an Enterprise Portfolio Manager (EPM) at Statistics Canada who liaises with a representative from the enterprise on all matters relating to Statistics Canada data collection activities. Where an establishment is selected for the Survey of Fraud Against

Businesses and it is located within an enterprise that has an EPM, Statistics Canada would respect the reporting arrangements that have already been established between the EPM and the enterprise for all Statistics Canada surveys.

The need for a pilot survey

Collecting data on incidents of fraud experienced by businesses has never been undertaken by Statistics Canada. While the consultations and focus testing conducted during the feasibility study provided much insight into the information priorities and some insight into data availability, the number of businesses involved in the feasibility study does not provide a full understanding of other issues that can be related to the outcome of a full national survey. These issues include the capability and willingness of establishments of different sizes and types to provide the data being collected and the possibility of double counting incidents (e.g. are instructions clear enough to ensure a retailer and a credit card company do not all report the same incidents of credit card fraud?). Further, a pilot survey would provide an opportunity to test the quality of the questionnaire and to make improvements or adjustments to the general survey process and methodology. Specifically, a pilot survey would have the following objectives:

- Test the quality of the questionnaire and help to further understand the feasibility of data collection, including:
    - Verify overall non-response rate and reasons for non-response, by size and industry type.
    - Test the flow of the questionnaire, the interpretability and comprehensiveness of instructions and definitions, and the extent of non-response for certain questions.
- Understand response issues that could be related to businesses with multiple establishments, or that could reside with industries of a particular type or size.
- Test survey procedures from the pre-contact stage to and including the Edit and Imputation stage. The pre-contact stage is performed prior to the mail out of the questionnaire to confirm contact information and whether or not the business is within the survey scope. The Edit and Imputation stage is one of the last cleaning stages of the data. A basic Edit and Imputation program will be required to assess the quality of the questionnaire and to create a clean file from which some cross-tabulations can be done to verify data quality.
- Recommend adjustments to a national level survey.

Sample design for a pilot survey

Based on previous recommendations regarding the inclusion of businesses of various sizes and industry types, all establishments of 5 employees or more would be considered in scope for the pilot survey if their main activity is classified within the NAICS codes listed previously in the section “Identification of priority industries according to their North American Industry Classification Standard (NAICS) codes”. There will be six industry groupings formed from these NAICS codes. These industry groupings are: retail, banking, payment companies, manufacturing, property and casualty insurance, and health and disability insurance.

In order to maintain a reasonable cost for the pilot test, it is proposed to consider analyzing the results of the pilot survey by industry and size classification only, and not by region. This results in the need for a smaller sample and therefore a lower cost. In addition, stratification by industry and size classification is sufficient to meet the objectives of a pilot test. The stratification of the frame and the sample allocation would therefore be done by industry and size. However, it is possible that the region and the NAICS could be taken into account in stratification when allocating the sample across Canada, but the region and NAICS will not play a role when determining the desired sample size by sector and size.

As mentioned previously, there are 6 different sectors of interest: retail, banking, payment companies, health and disability insurance, property and casualty insurance and manufacturing. The industry, derived from the NAICS, would be used as the first component of stratification.

There would be 4 size classes, derived by using the number of employees provided on the Business Register by establishment. The proposed size classes are the following:

Size Class	Number of employees
Very small	5 to 50
Somewhat small	51 to 100
Medium	101 to 499
Large	500+

Determining the sample size required for the pilot survey[1]	
Number of NAICS classes (industries):	6
Number of SIZE classes:	4
Number of contributors needed per domain (i.e., industry and size):	10
Expected response rate:	40%[2]

1. Based on the pilot survey being a mail out/mail back pen and paper questionnaire with a telephone pre-contact (to ensure the establishment is in scope and contact information is correct) and telephone follow-ups for non-respondents and data editing.
2. Forty percent represents the percentage of total records that are expected to be usable for analysis. This proportion is based on average response rates for business surveys in general.

As there are 24 domains (i.e., 6x4=24), 600 units are required (i.e., (6x4x10)/0.4=600). The count of 10 is recommended for the number of domains of estimation given that the objectives of the pilot survey are to assess the quality of the questionnaire, test the survey procedures and obtain an idea of response rates rather than produce actual estimates.

Hence, **the recommended sample size for the pilot survey is 600 establishments**, allocated by industry and size classes. The exact allocation would be determined when work on the project begins. The sample selection would be done using the Generalized Sampling System (GSAM) of Statistics Canada and a stratified simple random sample of establishments would be selected.

Pilot survey: Activities, schedule, deliverables and costs estimates

The following schedule and cost estimates are based on the following assumptions:

- The survey will be conducted by Statistics Canada.
- Sample size is 600.
- A pre-contact will be made with all establishments in the sample to eliminate those that are out of scope and determine the recipient for the questionnaire.
- Survey is pen and paper questionnaire that is mailed out and mailed back.
- Total record length of questionnaire is 1,650 bytes.
- 40% response rate for methodological and analytical purposes (i.e., 40% of all questionnaires are complete enough to be used for estimates); 70% response rate for questionnaire processing purposes (i.e., 70% of questionnaires must be handled in some way by questionnaire processing).
- 45% verification to be performed by data capture.
- Manual “head-down” data capture.
- No public release of the pilot survey results through Statistics Canada’s *Daily.*

Should any specifications or start-up dates change, the cost profiles by fiscal year will also change.

Schedule for deliverables and key activities

Deliverables and key activities	Start date	End date
Questionnaire refinement	Jul 2006	Aug 2006
Design, build and test data capture and editing and imputation systems[1]	Sep 2006	Oct 2006
Pre-contacts	Sep 2006	Sep 2006
Mail out of questionnaire	Oct 2006	Oct 2006
Follow-up, data collection, processing and editing	Nov 2006	Feb 2007
Computation of response and non-response rates, and adjustment of weights	Feb 2007	Mar 2007
Creation of final file and weighted estimates	Mar 2007	Apr 2007
Analysis, including documentation and recommendations for a national survey[2]	Apr 2007	Jun 2007

1. Data capture system for the pilot will not comprise scanning and intelligent character recognition, but will be manual.
2. Assumption is made that the information will not be released through Statistics Canada *Daily* and will therefore not require dissemination procedures, such as report composition and the production of electronic tables.

Cost estimate

Activities	Costs (includes salary and non-salary costs) (dollars)
Questionnaire development, translation, design and printing	28,800
Design, build and test data capture and editing & imputation systems[1]	33,700
Preparation of frame and sample	9,600
Pre-contacts	6,000
Mail out of questionnaire, including postage	900
Follow-up	9,800
Data collection, data capture, processing and editing	60,600
Computation of response and non-response rates, and adjustment of weights	1,900
Creation of final file and weighted estimates	7,900
Analysis, including documentation and recommendations for a national survey[2]	19,800
Project management	35,100
Computer costs	1,400
Total	**215,400**

1. Data capture system for the pilot will not comprise scanning and intelligent character recognition, but will be manual.
2. Assumption is made that the information will not be released through Statistics Canada *Daily* and therefore will not incur costs associated with dissemination, such as composition and production of electronic tables.

otal cost estimate by fiscal year

Fiscal year	Cost estimate (dollars)
2006/07	151,100
2007/08	65,300
Total	**215,400**

Options for a national survey

This feasibility study is proposing two options for a first-time national survey, both of which would gather data to help fill the gap in information on fraud in Canada. Option 1 would target establishments with 5 or more employees (i.e., very small, somewhat small, medium and large establishments) and Option 2 would target establishments of 101 or more employees (i.e., medium and large establishments).[14]

Recommendation: Providing that there are no major changes required to the survey frame or target population as a result of the pilot survey and that the pilot survey demonstrates no major issues with data collection, Option 1 is being recommended. It is being recommended because, by including small businesses, it would best meet the overall objectives of a survey and would inform the data gap that exists with respect to understanding variations in fraud victimization, reporting, prevention and detection across small, medium and large businesses.

Option 2 is being presented in order to document survey methodology and cost and timeframe estimates in the event that the pilot survey reveals issues with the inclusion of small businesses, or if Option 1 proves cost prohibitive.

Option 1: Survey of small, medium and large establishments

The target population for Option 1 would be very small, somewhat small, medium and large businesses classified according to the NAICS codes previously listed in the section “Identification of priority industries according to their North American Industry Classification Standard (NAICS) codes”. The Business Register would serve as the survey frame.

The sample design for the first cycle of the survey would consist of a sample drawn from the roughly 50,000 small establishments representing the desired NAICS codes in the Business Registry and a census of the approximately 3,200 medium and large establishments. Because of the relatively small pool of establishments in Canada that are the target for several Statistics Canada surveys each year, business surveys are usually sample surveys rather than censuses. This reduces the burden upon businesses and avoids compromising response rates. However, this mix of sample and census based on size classification is being recommended because, to build a reliable sample, it must be known that incidents of fraud are similar between establishments. Based on the consultations and focus testing conducted during the feasibility study, it is understood that the incidence of fraud can vary greatly from one sector to another and from one size classification to another, which makes it difficult to build a reliable sample. With a pilot survey of 600, the information required to build a sample for the national survey would not be sufficient, which is why it is recommended to conduct a census of medium and large establishments for the first cycle of a national survey. This will help obtain an understanding of how the incidence of fraud differs across medium and large establishments and across different industry types. If the response rate for the current proposed cycle is high enough, it could provide the information needed to build a sample of medium and large establishments for subsequent survey cycles (if the survey were to become part of an ongoing data collection initiative). Due to the number of establishments within the small establishment classification, a census is simply not feasible which is why it is recommended to use a sample of small establishments.

14. These two options are discussed in detail as it is felt that these would best meet the information needs identified during the consultations held for the feasibility study. A number of other options also exist that would be less costly, yet would meet fewer of the information needs. For instance, the industry types surveyed could be reduced from six to perhaps only one or two industry types of high importance. Another option would be to produce estimates only at a national level rather than by region. These types of options would reduce the sample size and therefore the cost of conducting the survey, and would partially respond to the information priorities regarding fraud in Canada.

Option 1: Recommended sample size

Determining the sample size required under Option 1[1] for the very small and somewhat small establishments only	
Number of NAICS classes (industry):	6
Number of SIZE classes:	2
Number of geography classes (6 regions)	6
Number of contributors needed per domain: (industry x size x geography)	98[2]
Expected response rate:	40%[3]

1. Based on the survey being a mail out/mail back pen and paper questionnaire with a telephone pre-contact (to ensure the establishment is in scope and contact information is correct) and telephone follow-ups for non-respondents and data editing.
2. Since the proportion of businesses that experience fraud is unknown, this number is based on the assumption that 50% of businesses experience fraud. It is also based on a target coefficient of variation of 8% and a survey response rate of 40%. In other words, given all these expectations, 98 is the number of establishments per domain that need to be surveyed in order to produce reliable estimates.
3. Forty percent represents the percentage of total records that are expected to be usable for analysis. This proportion is based on average response rates for business surveys in general.

For the very small and somewhat small establishments, there are 72 domains (i.e., 6x2x6=72), meaning 7,056 sampling units would be needed (i.e., 72x98=7,056).[15] The sample size for very small and somewhat small establishments can therefore be set to 7,056. The proposal for a census of the medium and large establishments represents about 3,200 primary sampling units.

Hence, **the recommended sample size for Option 1 is 10,300 establishments**, allocated by sector, region and size classes across Canada. The exact allocation would be determined by Statistics Canada when work on the project begins. The sample selection would be done using the Generalized Sampling System (GSAM) of Statistics Canada and a stratified simple random sample of establishments would be selected for the very small and somewhat small establishments.

Option 1: Activities, schedule, deliverables and costs estimates

The following schedule and cost estimates are based on the following assumptions:

- The survey will be conducted by Statistics Canada.
- Sample size is 10,300.
- A pre-contact will be made with all establishments in the sample to eliminate those that are out of scope and determine the recipient for the questionnaire.
- Survey is pen and paper questionnaire that is mailed out and mailed back.
- Survey is voluntary.
- Total record length of questionnaire is 1,650 bytes.
- 40% response rate for methodological and analytical purposes (i.e., 40% of all questionnaires are complete enough to be used for estimates); 70% response rate for questionnaire processing purposes (i.e., 70% of questionnaires are returned and must be handled by data processing).
- 45% verification to be performed by data capture.
- Use of scanning and Intelligent Character Recognition for data capture, processing and on-line editing within a “Blaise” data processing system.
- Creation of approximately 40 standard output tables.
- Target coefficient of variation is 16% or less for estimates.
- Public release of the survey results via an analytical report and electronic data tables, and a release announcement through Statistics Canada’s *Daily*.

Should any specifications or start-up dates change, the cost profiles by fiscal year will also change.

15. The response rate of 40% is already factored into the count of 98, as per note 2 in the table “Determining the sample size required under Option 1 for the very small and somewhat small establishments only.”

Schedule for deliverables and key activities

Deliverables and key activities	Start date	End date
Questionnaire re-development	Jun 2007	Jul 2007
Design, building and testing of data capture and editing and imputation systems[1]	Jul 2007	Nov 2007
Pre-contacts	Nov 2007	Dec 2007
Mail out of questionnaire	Jan 2008	Jan 2008
Follow-up, data collection, processing and editing	Feb 2008	Oct 2008
Computation of response and non-response rates, and adjustment of weights	Oct 2008	Oct 2008
Creation of final file and weighted estimates	Nov 2008	Dec 2008
Analysis, report writing, report production, printing and postage; creation of public use electronic tables[2]	Dec 2008	Jul 2009
Release of analytical report and electronic tables	**July 2009**	

1. Data capture system for national survey will comprise scanning and Intelligent Character Recognition and will be a "Blaise" system.
2. Data must be released through Statistics Canada *Daily* and will therefore incur costs associated with dissemination such as composition and the production of electronic tables.

Cost estimate

The following cost estimate includes survey and system development costs associated with the first cycle of a survey. It is estimated that subsequent cycles would cost approximately $55,000 less.

Activities	Costs (includes salary and non-salary costs) (dollars)
Questionnaire re-development, translation, design and printing	36,700
Building and testing of data capture and editing & imputation systems[1]	103,100
Preparation of frame and sample	13,100
Pre-contacts	159,300
Mail out of questionnaire, including postage	2,400
Follow-up	153,100
Data collection, data capture, processing and editing	480,700
Computation of response and non-response rates, and adjustment of weights	2,000
Creation of final file and weighted estimates	14,700
Analysis, report writing, report production, printing and postage; creation of public use electronic tables[2]	106,700
Project management	115,800
Computer costs	4,000
Total	**1,191,600**

1. Data capture system for national survey will comprise scanning and Intelligent Character Recognition and will be a "Blaise" system.
2. Data must be released through Statistics Canada *Daily* and will therefore require translation, report production and electronic tables.

Total cost estimate by fiscal year

Fiscal year	Cost estimate (dollars)
2007/08	599,000
2008/09	536,800
2009/10	55,800
Total	**1,191,600**

Option 2: Survey of medium and large establishments

As mentioned earlier, Option 2 is being presented in order to document survey methodology, cost and timeframe estimates in the event that the pilot survey reveals issues with the inclusion of very small and somewhat small businesses. The target population for Option 2 would include medium and large businesses classified according to the NAICS codes previously listed in the section "Identification of priority industries according to their North American Industry Classification Standard (NAICS) codes". The Business Register would serve as the survey frame.

Based on the reasoning provided previously under the description of Option 1, the sample design for the first cycle of the survey according to Option 2 would consist of a census of the approximately 3,200 medium and large businesses. If the response rate for the current proposed cycle is high enough, it could provide the information needed to build a sample of medium and large establishments for subsequent survey cycles (if the survey were to become part of an ongoing data collection initiative).

Option 2: Activities, schedule, deliverables and costs estimates

The following schedule and cost estimates are based on the following assumptions:

- The survey will be conducted by Statistics Canada.
- Sample size is 3,200.
- A pre-contact will be made with all establishments in the sample to eliminate those that are out of scope and determine the recipient for the questionnaire.
- Survey is pen and paper questionnaire that is mailed out and mailed back.
- Survey is voluntary.
- Total record length of questionnaire is 1,650 bytes.
- 40% response rate for methodological and analytical purposes (i.e., 40% of all questionnaires are complete enough to be used for estimates); 70% response rate for questionnaire processing purposes (i.e., 70% of questionnaires are returned and must be handled by data processing).
- 45% verification by data capture.
- Use of scanning and Intelligent Character Recognition for data capture, processing and on-line editing within a "Blaise" data processing system.
- Creation of approximately 40 standard output tables.
- Target coefficient of variation of 16% or less for estimates.
- Public release of the survey results via an analytical report and electronic data tables, and a release announcement through Statistics Canada's *Daily*.

Should any specifications or start-up dates change, the cost profiles by fiscal year will also change.

Schedule for deliverables and key activities

Deliverables and key activities	Start date	End date
Questionnaire re-development	Jun 2007	Jul 2007
Design, building and testing of data capture and editing and imputation systems[1]	Jul 2007	Nov 2007
Pre-contacts	Nov 2007	Dec 2007
Mail out of questionnaire	Jan 2008	Jan 2008
Follow-up, data collection, processing and editing	Feb 2008	Aug 2008
Computation of response and non-response rates, and adjustment of weights	Sep 2008	Oct 2008
Creation of final file and weighted estimates	Oct 2008	Oct 2008
Analysis, report writing, report production, printing and postage; creation of public use electronic tables[2]	Nov 2008	Jun 2009
Release of analytical report and electronic tables	**June 2009**	

1. Data capture system for national survey will comprise scanning and Intelligent Character Recognition and will be a "Blaise" system.
2. Data must be released through Statistics Canada *Daily* and will therefore require translation, report production and electronic tables.

Cost estimate

The following cost estimate includes survey and system development costs associated with the first cycle of a survey. It is estimated that subsequent cycles would cost approximately $55,000 less..

Activities	Costs (includes salary and non-salary costs) (dollars)
Questionnaire re-development, translation, design and printing	31,700
Building and testing of data capture and editing and imputation systems[1]	103,100
Preparation of frame and sample	6,500
Pre-contacts	50,900
Mail out of questionnaire, including postage	1,400
Follow-up	54,000
Data collection, data capture, processing and editing	189,900
Computation of response and non-response rates, and adjustment of weights	2,000
Creation of final file and weighted estimates	10,000
Analysis, report writing, report production, printing and postage; creation of public use electronic tables[2]	99,800
Project management	73,300
Computer costs	4,000
Total	**626,600**

1. Data capture system for national survey will comprise scanning and Intelligent Character Recognition and will be a "Blaise" system.
2. Data must be released through Statistics Canada *Daily* and therefore will incur costs associated with dissemination, such as composition and the production of electronic tables.

Total cost estimate by fiscal year

Fiscal year	Cost estimate (dollars)
2007/08	322,500
2008/09	254,900
2009/10	49,200
Total	**626,600**

Analysis of UCR data and recommendations for improvement

One of the objectives of the fraud feasibility work was to examine police-reported data from the Uniform Crime Reporting (UCR) Survey in light of the findings from the consultations and make recommendations for improvements to the survey. In addition to having to keep up with demands to capture the changing nature of fraud, policing services have also grappled with how to score fraud incidents within the UCR Survey. This section of the report will provide a description of the UCR survey, an overview of the survey rules for counting frauds, and will present a description of the data available in context with the findings from the feasibility study.

A number of recommendations to improve the survey to respond to information priorities will also be made with the caveat that police will need to be consulted regarding the feasibility of reporting the new information to the CCJS. In addition, it should be noted that changes to the UCR Survey are implemented at set intervals because of the heavy burden on police departments to make such amendments. Because data are collected from every police service in Canada in a standardized fashion by interfacing with each police service's Records Management System (RMS) which is linked to the information collected on their occurrence reports, implementing any changes to the UCR national data requirements or scoring rules represents a large undertaking by the police service or their RMS vendor. As a number of amendments to the UCR Survey were implemented in 2005, the next round of changes is scheduled for 2010.

Overview of the Uniform Crime Reporting (UCR) Survey

The Uniform Crime Reporting Survey was developed by Statistics Canada with the co-operation and assistance of the Canadian Association of Chiefs of Police. The survey, which became operational in 1962, collects crime and traffic statistics reported by all police services in Canada. The data reflect reported crime that has been substantiated through police investigation. Currently, there are two levels of detail collected by the UCR Survey: aggregate statistics and incident-based statistics. The aggregate UCR survey records the number of substantiated offences, as well as aggregate counts of the number of offences cleared by charge or cleared otherwise, persons charged (according to their sex and whether or not they are an adult or a youth) and those not charged. It does not provide victim characteristics.

Incident-based statistics are collected through the Incident-based UCR Survey, also known as the UCR2 survey. This survey captures detailed information on individual incidents that are reported to police, including characteristics of the victim and accused persons. This detailed survey was implemented in the early 1980s. Police services have been switching from the aggregate survey to the incident-based survey as their records management systems have evolved to become capable of providing this level of detail. In 2004, 120 police services in 8 regions supplied data for the complete year to the UCR2 Survey. These data represent 58% of the national volume of crime.

Unlike the aggregate survey, the UCR2 survey is more flexible and allows for the addition of new data elements and scoring categories as information priorities evolve. Examples of the newest variables added to the survey include data elements to measure the involvement of organized crime and street gangs in criminal incidents, and data elements to measure hate-motivated crimes and cyber-crime.

Because the transition from the aggregate survey to the UCR2 survey has been incremental among police services, it is difficult to present trend data based on the UCR2 survey. In response to a need for some trend analysis, a UCR2 Trend Database was established. Presently, the Trend Database contains historical data for 69 police services that have consistently been reporting UCR2 data since 1998. These respondents accounted for 45% of the national volume of crime in 2004.

Overview of how fraud is counted according to the UCR survey

The UCR aggregate survey, which continues to be the standard for reporting national data to the public, counts crime according to the number of offences, and rules are provided on how to determine what constitutes an offence. In general, the number of violent offences equals the number of victims, while for non-violent offences, such as fraud, the number of offences equals the number of incidents. An incident is determined by a standard definition. An incident is a set of connected events which usually constitutes a police occurrence report and is generally defined as an event which has occurred at the same time, at the same place and under the same set of circumstances. Due to the varying nature of some crimes, there are additional counting rules that apply to specific offences. Fraud is one of those offences for which specific counting rules apply.

The UCR scoring manual acknowledges that when it comes to fraud, "scoring of these offences often presents difficulty relating to the definition of a separate or distinct set of events… All the various circumstances which arise cannot be covered by examples."[16] In an effort to provide some standards to scoring frauds, the UCR survey provides the following types of examples:

Cheques

A man enters a store and knowingly issues 3 bad cheques and subsequently enters another store and passes 2 bad cheques. Under the UCR aggregate survey, these would be counted as 2 separate incidents. Under the UCR2 survey, these would also be submitted as 2 separate incidents since there are two complainants, but the first would have a "fraud counter" of 3 and the second would have a "fraud counter" of 2 to indicate the number of bad cheques passed in each store. This additional field of "fraud counter" in the UCR2 survey, therefore, can provide a more complete picture of the extent of fraud.

The UCR survey specifies that an incident of cheque fraud is a series of cheque frauds that take place in one location on the same day. If they occur in this same location on two separate days, then two incidents would have taken place.

Credit cards

Both the UCR and UCR2 surveys base the incident count on the number of credit cards (or transaction cards) and not the number of times it was used over a period of time. For example, a woman enters a shopping centre and uses a stolen credit card in 3 different stores. Under the UCR aggregate and the UCR2 surveys, this would be counted as 1 incident because the rules specify the incident to be associated with the card. Under the UCR2 survey, a counter of 3 would be specified. It should be clarified that if 2 separate stolen credit cards were used over a period of time, under both the UCR aggregate and UCR2 surveys, these would be counted as 2 separate incidents and, under the UCR2 survey, the counter for each incident would equal the number of times each card was used.

Other fraud

A health/fitness club sells lifetime memberships to two hundred customers and the club never opens. Under the UCR aggregate and UCR2 surveys, this would be counted as 1 incident and, under the UCR2 survey, a counter of 200 would apply.

16. The Aggregate Uniform Crime Reporting Manual is available at http://www.statcan.ca/english/sdds/document/3302_D7_T1_V1_E.pdf. The Incident-based Uniform Crime Reporting (UCR2) Manual is available at http://www.statcan.ca/english/sdds/instrument/3302_Q7_V1_E.pdf.

While the aggregate UCR manual does not deal with many examples of what constitutes an incident with respect to "other" types of fraud, the UCR2 manual does indicate that for "other" types of fraud, the counter should equal the number of times the same fraudulent action was perpetrated over a period of time.

While both the UCR and UCR2 surveys count the number of "incidents" consistently, it is easy to see how counting frauds based on the "incident" under-estimates fraudulent activity in Canada. By counting according to the "incident", the situation where 200 customers were defrauded by the fraudulent health/fitness club, as per the example above, would be reflected in the official crime statistics as 1 incident of fraud. Not only does the "incident" count under-estimate the prevalence of fraud in Canada, the different rules for defining an incident of cheque fraud versus credit card fraud and other types of fraud creates an inconsistency in how fraud incidents are counted. These inadequacies with the incident count were identified a number of years ago and are what prompted the inclusion of a "fraud counter" in the UCR2 survey. It also prompted the exclusion of analysis of fraud data in the annual crime statistics report by the Canadian Centre for Justice Statistics.

The use of a "fraud counter" allows police to indicate in a consistent manner the extent of the fraud without having to divide incidents by time and place. Because of the incremental move by police services to the UCR2 survey from the aggregate survey and the need to maintain comparable historical trends, fraud data have always been counted according to the incident. Recently, however, the last two major police services remaining to convert to the UCR2 survey have made the transition. This means that as of 2006, incident-based data will account for about 85% of the national volume of substantiated crimes against the *Criminal Code*. As such, at their September 2004 meeting, the Police Information and Statistics (POLIS) Committee of the Canadian Association of Chiefs of Police (CACP) approved the proposal that the "fraud counter" be used as the basis for counting fraud in Canada.

Recommendation: It is recommended that the CCJS build a program to produce aggregate counts of fraud based on the fraud counter. It is further recommended that trend analysis at a level higher than the police service be restricted to statistics available on the UCR2 Trend Database since the conversion of police services to the UCR2 survey has been incremental and this gradual conversion will influence the trend in fraud counts that are based on the UCR2 fraud counter.

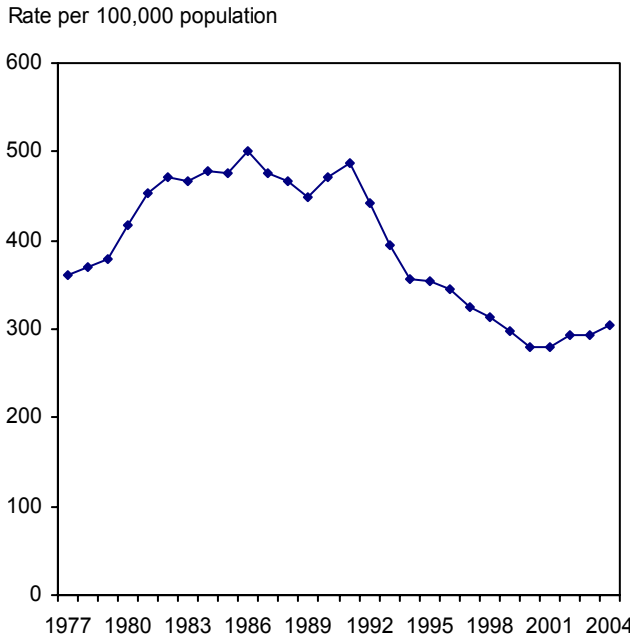
Overview of police-reported fraud in Canada

According to aggregate crime statistics, which are considered an under-estimate of fraud based on the issues outlined in the section above, there were 97,091 *Criminal Code* incidents of fraud reported by police in 2004. Since 1991, the rate of fraud has dropped 38%, falling from 488 to 304 incidents per 100,000 population (Figure 1). This decrease has been driven by the 77% decrease in cheque fraud. Prior to the drop that began after 1991, cheque fraud typically accounted for between 5 in 10 and 7 in 10 frauds in Canada. In 2004, cheque fraud accounted for just 2 in 10 incidents of fraud. Despite being an undercount of incidents of fraud overall, the drop in cheque fraud is likely real and is not surprising given that, as indicated in the Background section of this report, cheques are no longer a popular method of payment for purchases among consumers and are being replaced by the use of direct payment and credit cards.

In 2004, official crime statistics suggest there were 29,533 incidents of credit card fraud (which includes all types of transaction cards) reported to the police and 48,817 incidents involving types other than cheque or credit card fraud (e.g. telemarketing fraud, securities fraud, false claims, etc.). The rate of credit card fraud began to rise in 1995, growing from a rate of 52 incidents per 100,000 that year to a rate of 92 in 2004 (Figure 2). Other frauds have seen consistent growth only since 2002, inching up from a rate of 135 that year to 153 in 2004. The growth in these types of fraud is likely much higher given the undercounting through the use of the "incident" as the unit of count, as indicated in the section above. Data from the UCR2 Survey indicate that the number of incidents based on the "fraud counter" is on average 1.8 time higher than the count based on the traditional method of counting fraud within the UCR Survey (Table 2). In addition, data from the UCR2 Trend Database show that while the direction of change from one year to the other for total frauds does not differ between the two methods of counting,

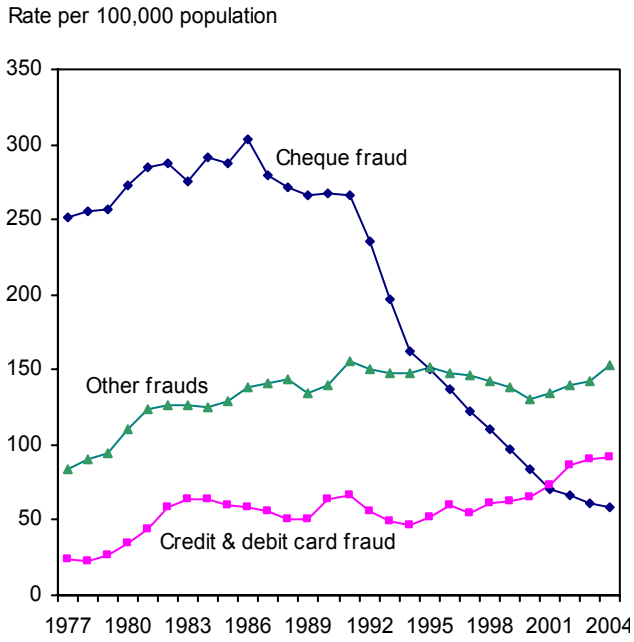
the size of change is greater when using the “fraud counter”. When examining the specific types of fraud, the direction of change at times differs according to the method used to count incidents.

Figure 1. Police-reported data on fraud suggest fraud decreased substantially from 1991 to 2001



Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

Figure 2. Police-reported data suggest rate of cheque fraud falling while credit and debit card and other fraud have increased slowly in recent years



Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

Table 2. Number of incidents of fraud, by type, using the traditional method of counting incidents versus using the fraud counter, selected police services, 2004[1]

	Incidents based on traditional counting method	Incidents based on use of the fraud counter	Difference	
	Number	Number	Number	Percentage
Total fraud	**66,618**	**117,561**	**50,943**	**76**
Cheque fraud	13,532	23,203	9,671	71
Computer fraud	840	1,319	479	57
Fraudulent insurance claims[2]	64	136	72	113
Fraudulent claims against a government department[3]	491	652	161	33
Financial or securities fraud	707	1,180	473	67
Telemarketing fraud	338	402	64	19
Transaction card fraud	21,905	49,999	28,094	128
Other fraud[4]	28,741	40,670	11,929	42

1. Data are not nationally representative. Based on data from 120 police departments active as of December 31, 2004 representing 58% of the national volume of crime.
2. Any fraud that involves providing false information to receive benefit from a private or public insurance agency.
3. Any fraud that involves providing false information to receive benefit from any federal, provincial/territorial, regional or municipal government department.
4. Includes other types of fraud not otherwise listed, such as price fixing, patent infringement, kickbacks, etc.

Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting (UCR2) Survey.

Almost 4 in 10 incidents of all frauds in 2004 were cleared, or solved, by police. The clearance rate for cheque fraud was 48% with clearance rates being lower for credit card fraud (30%) and other types of fraud (40%). As with other types of property crimes, the rate at which fraud incidents are solved has been decreasing since the mid-1990s.

Analysis of the UCR2 data in relation to information needs

During the consultations, certain issues and information priorities were raised. This section will address how, with amendments, the UCR2 survey can respond to these information priorities.

Type of fraud

During the consultations, the following types of fraud were raised as a priority for data collection: identify theft/false applications (particularly mortgage fraud); fraudulent use of credit and bank cards; fraudulent use of cheques; false billing, and; insurance claim fraud. Under the UCR2 survey, information is collected regarding the type of fraud and the response categories are: cheques, transaction card, telemarketing, securities/financial, false claims – insurance, false claims – government, computer, and other. Table 3 shows the distribution of incidents of fraud reported by all UCR2 respondents in 2004.

The category *transaction card* is generic and it would be useful to be able to monitor trends in terms of types of transaction card frauds being perpetrated. The utility of collecting data on different types of cards has also been an ongoing discussion with the CACP's Police Information and Statistics Committee for the last few years. In fact, at their September 2004 meeting, the committee agreed that **the category "transaction card" be disaggregated to the following categories: debit/ATM, credit card (financial institution), other credit card (retail), and other transaction cards (e.g. telephone)**. This feasibility study also concurs with that recommendation.

Table 3. Number and percent of incidents of fraud by type, selected police services, 2004[1]

	Number	Percent
Total fraud	**66,618**	**100**
Cheque fraud	13,532	20
Computer fraud	840	1
Fraudulent insurance claims[2]	64	0
Fraudulent claims against a government department[3]	491	1
Financial or securities fraud	707	1
Telemarketing fraud	338	1
Transaction card fraud	21,905	33
Other[4]	28,741	43

1. Based on data from 120 police services in 8 regions that supplied data for the complete year to the UCR2 Survey. These data represent 58% of the national volume of crime.

2. Any fraud that involves providing false information to receive benefit from a private or public insurance agency.

3. Any fraud that involves providing false information to receive benefit from any federal, provincial/territorial, regional or municipal government department.

4. Includes other types of fraud not otherwise listed, such as price fixing, patent infringement, kickbacks, etc.

Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting (UCR2) Survey.

Under the UCR2 survey, *insurance claim fraud* includes frauds against both private and public insurers of all types of insurance. As with other types of fraud, the number of incidents of insurance fraud reported to the police is likely an undercount because private insurers have their own investigators and are likely to avoid police involvement, particularly in less serious incidents. However, the health care sector and the property and casualty sector face different issues making it worthwhile to collect separate counts for each.

Recommendation: It is recommended that the scoring option of "false claims – insurance" be divided into "false claims – property & casualty insurance", "false claims – health, life and disability insurance" and "false claims – other insurance."

Telemarketing fraud is not a type of fraud, but a method by which fraud is committed. Various types of fraud, such as investment fraud and advance fee schemes, can be solicited using telemarketing techniques, or other mass marketing vehicles such as mail, e-mail or newspaper advertisements. Although telemarketing is not a type of fraud *per se*, information on how the fraud was committed, such as by Internet, mail, e-mail, phone, etc., was deemed important among those consulted as this would assist in understanding mass-marketing fraud activity.

Recommendation: It is recommended that the category "telemarketing" be removed from the data element "fraud type" and that a new data element called "mass marketing" be added to the UCR2 survey. Under this new data element, police services would first indicate whether or not this fraud was a result of mass marketing (with the scoring options of "yes" or "no") and the more detailed scoring options of "telephone", "postal mail", "e-mail", "Internet" and "other" would be available to indicate the nature of the mass marketing approach.

With respect to the pressing issue of *identity theft* and its role as an enabler to commit fraud, there is currently no information on the UCR2 survey that can inform this issue. Part of the dilemma lies in the fact that having someone else's personal identity information in your possession, regardless of how it was obtained, is presently not a criminal offence. The criminal offence occurs only when that identity information is stolen (i.e. theft) or is used to commit a crime, such as fraud. In addition, there is currently no consensus on the definition of identity theft or identity fraud. If and when a new offence under the *Criminal Code* is created that classifies "identity theft" or "identity fraud" as a separate criminal offence, this offence will be captured under the UCR2 survey.

Recommendation: The CCJS is to continue to monitor the definition of identity theft. If this activity is deemed a new, separate criminal offence, then it will automatically be captured by the UCR2 survey and should receive its own unique violation code under the UCR2 survey (as opposed to being included in a general code such as "other fraud"). If Canada reaches an agreement as to the definition of this type of activity before 2010 when the next round of changes are scheduled for the UCR2 Survey, but does not create a separate criminal offence for it, then the CCJS should consult with police services regarding the feasibility of adding a new data element of "identity theft" to the UCR2 survey. This data element could be scored by police officers to indicate that the commission of the offence involved the use of stolen or illegitimately obtained personal identification. This characteristic could therefore be examined in relation to the various types of fraud.

The category *other fraud* comprises a large proportion of all frauds reported to the UCR2 Survey. It would be useful to be able to break these down to provide more detail. Other types of fraud that were raised as issues during consultations included: advance fee schemes, mortgage fraud, and property fraud.

Recommendation: It is recommended that the categories of advance fee schemes, mortgage fraud and property fraud be added to the data element "fraud type" and that definitions be established to ensure there is no overlap between "mortgage fraud" and the existing scoring option of "financial/securities fraud".

Involvement of organized criminal groups

The UCR2 survey has recently been updated to capture information on whether or not the criminal incident was committed or suspected to have been committed by a criminal organization or street gang. This data element can be coded for any violation, including fraud. Because this data element was just added in 2005, no data are currently available and it may be a few years before enough police services are reporting to be able to perform some analysis on the information.

The insurance industry is subject to activities of groups they refer to as "rings" which can be defined as a group of people working toward the same goal of financial gain from illegal activity. Both the Insurance Bureau of Canada's definition of a criminal "ring" and the UCR2 Survey's definition of a criminal organization are based on the *Criminal Code of Canada*'s definition of a criminal organization. According to the UCR2 scoring manual, "a criminal organization consists of a static or fluid group of (2 or more) individuals who communicate, co-operate and conspire with an ongoing collective network; and has one of its main purposes or activities the facilitation or commission of offences undertaken or planned to generate material benefits or financial gains." As such, the UCR2 Survey already has the capacity to collect information on whether or not a fraud involved criminal rings or criminal organizations and requires no further changes to respond to this information need.

Method by which fraud was committed

As mentioned earlier, information on how the fraud was committed, such as by Internet, mail, e-mail, phone, etc., was deemed important among those consulted. The addition of the data element "mass marketing" will help to fulfill this data need. In addition, the data element of "cyber-crime" was added to the UCR2 survey in 2005. Within this data element, police can indicate whether a computer or the Internet was used as a tool to commit fraud (or any other criminal offence). This will allow the identification of all frauds committed through a computer, and the "mass marketing" data element will allow these occurrences to be further broken down as frauds which resulted from mass marketing or not.

Monetary impact of fraud

The monetary losses as a result of fraud is feasible to collect in a survey of businesses or individuals; however, past experience has proven that monetary loss for property crimes is difficult to collect through the UCR2 Survey. The original version of the incident-based survey contained a data element that captured the dollar value of property stolen or lost as a result of fraud. Due to the complexity of some

incidents and the effort required to determine dollar values, police frequently left this field blank. Due to non-reporting and data quality issues, this field was removed from the incident-based survey in the late 1990s. As such, **there is no recommendation to attempt to collect this information through the UCR2 survey.**

Conclusion

Currently, data on fraud in Canada are available piece-meal from various sources reporting various counts, none of which together can provide a complete picture of the nature and extent of fraud in Canada. Canada's main source for crime statistics, police-reported data from the Uniform Crime Reporting Survey, represents an under-reporting of this crime to police and also has limitations in terms of how incidents of fraud are counted. Other countries have begun trying to quantify the nature and extent of fraud through business and general population surveys. These include Australia's 1999 Survey of Crimes Against Small Businesses (Perrone, 2000); the British Crime Survey which is a national population survey and which added questions regarding credit card/debit card fraud and Internet fraud to its 2002/03 survey cycle (Allen et. al.) ; and, the United States Federal Trade Commission Survey of 2003 (Anderson, 2004).

This present feasibility study was undertaken by the CCJS to attempt to find a way to help bridge the gap in information on fraud in Canada. Results of consultations and focus testing with stakeholders and various businesses indicate that a national survey of businesses in Canada is a feasible approach to compiling more comprehensive, standard data on fraud in Canada. This report has provided the groundwork necessary to proceed with a Survey of Fraud Against Businesses and to improve the police-reported data collected through the Incident-based Uniform Crime Reporting (UCR2) Survey. The first cycle of a Survey of Fraud Against Businesses would generate baseline data; further value of the survey lies in generating trend data by repeating the survey every two to three years. The business survey data would also help to further analyze the quality of the UCR2 Survey data by, for instance, demonstrating which types of frauds are seriously under-reported. The UCR2 Survey would continue to collect data on incidents of fraud reported by the police and the CCJS would continue to assess the quality of these data.

A business survey would go far in responding to information priorities on fraud, but certain types of fraud, such as consumer and mass-marketing fraud, are issues that are best informed by data collected through a general population survey. A general population survey would also shed light on who is at risk and how the general population is affected by fraud, attempted fraud and the related activities of identity theft, deceptive spam and phishing.[17]

17. Spam is considered any bulk commercial e-mail sent without the express consent of recipients. Spam is a concern with respect to its role as a mass-marketing vehicle that is used by some to defraud consumers and businesses through deceptive spam. Phishing is the impersonation of a trusted person or organization in order to steal a person's personal information generally for the purpose of identity theft.

Methodology

This section provides more methodological information on the Aggregate Uniform Crime Reporting (UCR) Survey and the Incident-based Uniform Crime Reporting (UCR2) Survey, such as counting procedures, survey coverage and data revisions.

The Aggregate Uniform Crime Reporting (UCR) Survey

The aggregate UCR survey records the number of incidents reported to the police. It includes the number of reported offences, actual offences, offences cleared by charge or cleared otherwise, persons charged (by sex and by an adult/youth breakdown) and those not charged. It does not include victim characteristics.

The aggregate UCR survey classifies incidents according to the most serious offence in the incident (generally the offence that carries the longest maximum sentence under the *Criminal Code*). In categorizing incidents, violent offences always take precedence over non-violent offences. As a result, less serious offences are under-represented by the UCR survey. The aggregate UCR survey scores violent incidents (except robbery) differently from other types of crime. For violent crime, a separate incident is recorded for each victim (i.e. if one person assaults three people, then three incidents are recorded; but if three people assault one person, only one incident is recorded). Robbery, however, is counted as if it were a non-violent crime in order to avoid inflating the number of victims (e.g. for a bank robbery, counting everyone present in the bank would result in an over-counting of robbery incidents). For non-violent crimes, one incident (categorized according to the most serious offence) is counted for every distinct or separate occurrence.

The Incident-based Uniform Crime Reporting (UCR2) Survey

The Incident-based UCR2 survey captures detailed information on individual criminal incidents reported to police, including characteristics of victims, accused persons and incidents. Police forces switch over from the aggregate to the incident based survey as their records management systems become capable of providing this level of detail. In 2004, 120 police services in 8 provinces supplied data for the complete year to the UCR2 survey. These data represent 58% of the national volume of reported actual (substantiated) *Criminal Code* crimes. The incidents contained in the 2004 database were distributed as follows: 40.7% from Ontario, 32.1% from Quebec, 11.5% from Alberta, 7.6% from British Columbia, 4.8% from Saskatchewan, 1.8% from Nova Scotia, 0.9% from Newfoundland and Labrador and 0.6% from New Brunswick. Other than Ontario and Quebec, the data are primarily from urban police departments. The reader is cautioned that these data are not geographically representative at the national or provincial level. Continuity with the UCR aggregate survey data is maintained by a conversion of the incident-based data to aggregate counts at year-end.

The UCR2 Trend Database contains historical data, which permits the analysis of trends in the characteristics of the incidents, accused and victims, such as weapon use and victim/accused relationships. This database currently includes 69 police services who have reported to the UCR2 survey consistently since 1998. These respondents accounted for 45% of the national volume of crime in 2004. This list of respondents will remain unchanged until such time as large police services such as the RCMP and OPP have been providing at least five years of data to the UCR2 survey, at which point they will become part of this trend database. The incidents contained in the 2004 Trend database were distributed as follows: 41.5% from Quebec, 30.1% from Ontario, 14.8% from Alberta, 6.6% from British Columbia, 6.2% from Saskatchewan and 0.8% from New Brunswick.

Data Revisions / Notes

Ontario

During the production of each year's crime statistics, data from the previous year are revised to reflect any updates or changes that have been received from the police services. During the revision of the 2001

data for the province of Ontario, a discrepancy in methodology applied by the forces in the province using the Ontario Municipal & Provincial Police Automated Co-operative (OMPPAC) system was detected. These forces report approximately one-third of the total criminal incidents for the province and include the OPP and about 60 small and mid-sized municipal forces. This discrepancy resulted in an over-count of less serious criminal incidents. A similar problem with data from Toronto Police was detected in 1992. During 2003 and 2004, the Canadian Centre for Justice Statistics (CCJS) consulted with affected police services and analyzed both historical aggregate UCR data and more recent UCR2 microdata to determine the impact of this over-reporting.

The effect at the Canada level was, on average, 1% per year from 1977 to 2000. This over-counting peaked in 1991, where it was estimated that the total crime rate for the country was over-estimated by approximately 1.8%. However, the overall historical trend changed very little. The impact in Ontario is more noticeable, but the overall trend is still very similar. On average, the effect of the over-counting was 2-3% per year, with the biggest change occurring in 1991, where the Ontario crime rate is 5% lower as a result of the adjustment.

For further information on the UCR and UCR2 surveys as well as historical adjustments to crime data for Ontario, readers should refer to the Statistics Canada website at www.statcan.ca, and click on Definitions, data sources and methods, then Surveys and statistical programs, then Alphabetical list, then Uniform Crime Reporting Survey.

References

Allen, J. et al. 2005. *Fraud and technology Crimes: findings from the 2002/03 British Crime Survey and 2003 Offending, Crime and Justice Survey.* Home Office Online Report 34/05. London: Home Office.

Anderson, Keith B. 2004. *Consumer Fraud in the United States: An FTC Survey*. Federal Trade Commission of the United States. Available at www.ftc.gov.

Bi-national Working Group on Cross-Border Mass Marketing Fraud. 2004. *Report on Identity Theft*. Available at www.psepc-psppcc.gc.ca.

Bi-national Working Group on Cross-Border Mass Marketing Fraud. 2003. *Mass Marketing Fraud*. Available at www.psepc-psppcc.gc.ca.

Canadian Bankers' Association. 2005. *Taking a closer look: Electronic banking.* May. Available at www.cba.ca.

Dryburgh, Heather. 2001. *Changing Our Ways: Why and How Canadians Use the Internet.* Statistics Canada catalogue no. 56F0006XIE. Ottawa: Statistics Canada. Available at www.statcan.ca.

Industry Canada. July 2005. *Key Small Business Statistics.* Industry Canada catalogue no. Jul-9/2005-2E. Ottawa. Available at http://strategis.gc.ca.

Perrone, S. 2000. "Crimes against small businesses in Australia: A preliminary analysis." *Trends and issues in crime and criminal justice*, no. 184. Canberra: Australian Institute of Criminology.

Pricewaterhouse Coopers. 2005. *Global Economic Crime Survey 2005: Canada.* Available at www.pwc.com/ca/ifs.

Statistics Canada. 2004a. "Household Internet Use Survey." *The Daily.* July 8. Ottawa. Available at www.statcan.ca.

Statistics Canada. 2004b. "E-commerce: Household shopping on the internet." *The Daily.* September 23. Ottawa. Available at www.statcan.ca.

Statistics Canada. 2005a. "Internet service provider industry." *The Daily.* December 15. Ottawa. Available at www.statcan.ca.

Statistics Canada. 2005b. "Electronic commerce and technology." *The Daily*. April 20. Ottawa. Available at www.statcan.ca.

Statistics Canada. 2005c. *Canadian Business Patterns.* June. Catalogue no. 61F0040XCB. Ottawa.

Taylor, Natalie and Pat Mayhew. 2002. "Patterns of Victimisation Among Small Retail Businesses." *Trends and Issues in Crime and Criminal Justice,* no. 221. Canberra: Australian Institute of Criminology.

Task Force on Spam. 2005. *Stopping Spam: Creating a stronger, safer Internet.* Catalogue no. lu64-24/2005E-PDF. Ottawa: Industry Canada. Available at www.e-com.ic.gc.ca.

Van Kesteren, John, Pat Mayhew and Paul Nieuwbeerta. 2000. *Criminal Victimisation in Seventeen Industrialized Countries.* The Netherlands: WODC.

Appendix 1 - Draft questionnaire for Survey of Fraud Against Businesses

The following draft questionnaire presents questions that have been developed as a result of consultations conducted for the feasibility study to improve the measurement of fraud in Canada. Final definitions of concepts and units of count have not been included with this draft questionnaire as these require further refinement. However, working definitions of some concepts are included at the end of this questionnaire.

Should a survey such as this be undertaken, participation by business establishments would be voluntary. Further, as with all Statistics Canada surveys, all information provided by respondents would remain confidential under the authority of the *Statistics Act*, Revised Statutes of Canada, 1985, Chapter S19.

Survey of Fraud Against Businesses

Purpose of the Survey of Fraud Against Businesses

The purpose of the Survey of Fraud Against Businesses is to collect data on the number of incidents of fraud experienced by certain business sectors. These data are required to respond to a need for better information on the nature and extent of fraud in Canada in order to improve policy and public education with respect to this issue. The survey also collects information on fraud detection and prevention and actions taken in response to incidents of fraud (including use of the criminal justice system).

Your participation is important

Participation in this survey is voluntary. However, your co-operation is essential to ensure the accuracy of the information collected.

The data you report are confidential

Statistics Canada is prohibited by law from publishing or releasing statistics that could reveal information obtained from this survey questionnaire. The data reported on the questionnaire will be treated in strict confidence and used for statistical purposes only. The confidentiality provisions of the *Statistics Act* are not affected by either the *Access to Information Act* or any other regulation.

If you have any questions regarding this survey or the questionnaire, please contact {NAME} at {toll-free number} or by email at {email address}.

1. Please indicate your last 12-month fiscal period.

	DD MM YYYY		DD MM YYYY
From:	|_|_| |_|_| |_|_|_|_|	To:	|_|_| |_|_| |_|_|_|_|

2. How many employees are currently employed by your establishment? |_|_|_|_|

3. Which of the following best describes your establishment?

- ○ 1 – Retail → **Go to section A**
- ○ 2 – Banking → **Go to section B**
- ○ 3 – Payment company (e.g. VISA, Mastercard, Interac) – **Go to section C**
- ○ 4 – Health or disability insurance → **Go to section D**
- ○ 5 – Property & casualty insurance → **Go to section E**
- ○ 6 – Manufacturing – **Go to section F**

Section A – Retail

A 1. How many of the following types of attempted and real fraudulent incidents did your establishment experience during your last 12-month fiscal period?

	Number of incidents	
Fraud committed by non-employees		
a) Fraudulent use of credit cards issued through payment companies (e.g. Visa, Mastercard, American Express, etc.)……..……		O not applicable O Don't know
b) Fraudulent use of private label credit cards (i.e., your company's private label card)		O not applicable O Don't know
c) Fraudulent use of bank cards……		O not applicable O Don't know
d) Fraudulent use of cheques ……..		O not applicable O Don't know
e) Use of false identity or false information in applications or other documents…….		O not applicable O Don't know
f) Counterfeit notes……		O not applicable O Don't know
g) Advance fee schemes..……		O not applicable O Don't know
h) False billing…… ……..		O not applicable O Don't know
i) Other fraud……..……		O not applicable O Don't know
Fraud committed by employees		
j) Asset misappropriation……		O not applicable O Don't know
k) Improper claims on expense accounts by employees……..…		O not applicable O Don't know
l) Financial misrepresentation…….		O not applicable O Don't know
m) Other fraudulent acts by employees……		O not applicable O Don't know

A 2. Does your company issue its own brand of credit card (i.e., private label) for clients?

- ○ Yes
- ○ No → **Go to the Question A6**

A 3. For each incident of fraud involving your company's brand of credit card, please indicate the number of incidents experienced by your establishment according to the source of fraudulent activity.

	Number of incidents	
a) Skimming……..…….……		O not applicable O Don't know
b) False application……		O not applicable O Don't know
c) Counterfeit cards……		O not applicable O Don't know
d) Lost or stolen cards……		O not applicable O Don't know
e) Non-receipt of cards……..		O not applicable O Don't know
f) Card not present/no signature (i.e. Mail order/phone/Internet purchases)…		O not applicable O Don't know
g) Account takeover…….		O not applicable O Don't know
h) Method unknown……		O not applicable O Don't know
i) Other, please specify _____.....		O not applicable O Don't know
Total incidents		

A 4. During the 12-month reference period, did your establishment mail out any pre-approved credit card applications?

O Yes
O No

A 5. During the 12-month reference period, did your establishment mail out any unsolicited credit cards?

O Yes
O No

A 6. Of the incidents of fraud your establishment experienced in the last 12-month reference period, were there any that were committed by a person residing outside of Canada (i.e., the United States or any other country)?

O Not applicable: did not experience any fraud incidents in the 12-month reference period
O Yes
O No
O Don't know

A 7. Of the incidents of fraud your establishment experienced in the last 12-month reference period, what was the most frequent way in which they were committed? (*check only one*)

- O Not applicable: not experience any fraud incidents in the 12-month reference period
- O e-mail
- O Internet
- O telephone
- O regular post
- O in person
- O other
- O don't know

Please go to Section G

Section B – Banking

B 1. How many of the following types of attempted and real fraudulent incidents did your establishment experience during your last 12-month fiscal period?

	Number of incidents	
Fraud committed by non-employees		
a) Fraudulent use of credit cards……		O not applicable O Don't know
b) Fraudulent use of bank cards…….		O not applicable O Don't know
c) Fraudulent use of cheques …….		O not applicable O Don't know
d) Mortgage fraud…….		O not applicable O Don't know
e) Other loan fraud……		O not applicable O Don't know
f) Worthless deposits (ATM)……		O not applicable O Don't know
g) Fraudulent bankruptcy ……		O not applicable O Don't know
h) Use of false identity in applications other than mortgages or loans……		O not applicable O Don't know
i) Counterfeit notes……..		O not applicable O Don't know
j) Advance fee schemes…….		O not applicable O Don't know
k) False billing…… …….		O not applicable O Don't know
l) Other fraud ……..		O not applicable O Don't know
Fraud committed by employees		
m) Asset misappropriation…….		O not applicable O Don't know
n) Improper claims on expense accounts by employees……..…		O not applicable O Don't know
o) Financial misrepresentation …….		O not applicable O Don't know
p) Other fraudulent acts by employees……		O not applicable O Don't know

B 2. Phishing is a term used to describe an activity that uses e-mail to deliver fake messages designed to look like they are coming from banks or other legitimate companies to lure many individual customers into revealing personal or financial information. In the last 12-month reference period, how many phishing sites did your establishment close down to halt the transmission of these fake messages to consumers?

☐☐☐

B 3. During the 12-month reference period, did your establishment mail out any pre-approved credit card applications?

O Yes
O No

B 4. During the 12-month reference period, did your establishment mail out any unsolicited credit cards?

O Yes
O No

B 5. Of the incidents of fraud your establishment experienced in the last 12-month reference period, were there any that were committed by a person residing outside of Canada (i.e., the United States or any other country)?

O Not applicable: did not experience any fraud incidents in the 12-month reference period
O Yes
O No
O Don't know

B 6. Of the incidents of fraud your business experienced in the last 12-month reference period, what was the most frequent way in which they were committed? (*check only one*)

O Not applicable: not experience any fraud incidents in the 12-month reference period
O e-mail
O Internet
O telephone
O regular post
O in person
O other
O don't know

Please go to Section G

Section C – Payment companies

C 1. For each incident of credit card or bank card fraud, please indicate the number of incidents according to the source of fraudulent activity.

	Number of incidents	
a) Skimming…….……		O not applicable O Don't know
b) Identity theft……		O not applicable O Don't know
c) Counterfeit cards……		O not applicable O Don't know
d) Lost or stolen cards……		O not applicable O Don't know
e) Non-receipt of cards……..		O not applicable O Don't know
f) Card not present/no signature (i.e. Mail order/phone/Internet purchases)…		O not applicable O Don't know
g) Account takeover…….		O not applicable O Don't know
h) Method unknown……		O not applicable O Don't know
i) Other, please specify _____.....		O not applicable O Don't know

C 2. How many of the following types of attempted and real fraudulent incidents did your establishment experience during your last 12-month fiscal period?

Fraud committed by non-employees	Number of incidents	
a) Advance fee schemes……		O not applicable O Don't know
b) False billing ……		O not applicable O Don't know
c) Other, please specify _____.....		O not applicable O Don't know
Fraud committed by employees		
d) Asset misappropriation……		O not applicable O Don't know
e) Improper claims on expense accounts by employees……..…		O not applicable O Don't know
f) Financial misrepresentation ……		O not applicable O Don't know
g) Other fraudulent acts by employees…		O not applicable O Don't know

C 3. Phishing is a term used to describe an activity that uses e-mail to deliver fake messages designed to look like they are coming from banks or other legitimate companies to lure many individual customers into revealing personal or financial information. In the last 12-month reference period, how many phishing sites did your establishment close down to halt the transmission of these fake messages to consumers?

☐☐☐

C 4. During the 12-month reference period, did your establishment mail out any pre-approved credit card applications?

O Yes
O No

C 5. During the 12-month reference period, did your establishment mail out any unsolicited credit cards?

- O Yes
- O No

C 6. Of the incidents of fraud your establishment experienced in the last 12-month reference period, were there any that were committed by a person residing outside of Canada (i.e., the United States or any other country)?

- O Not applicable: did not experience any fraud incidents in the 12-month reference period
- O Yes
- O No
- O Don't know

C 7. Of the incidents of fraud your establishment experienced in the last 12-month reference period, what was the most frequent way in which they were committed? (*check only one*)

- O Not applicable: not experience any fraud incidents in the 12-month reference period
- O e-mail
- O Internet
- O telephone
- O regular post
- O in person
- O other
- O don't know

Please go to Section G

Section D – Health or disability insurance

D 1. How many of the following types of fraudulent incidents did your establishment experience during your last 12-month fiscal period?

	Number of incidents	
Fraud committed by non-employees		
a) Insurance claim fraud – health and disability insurance: investigated incidents…….		O not applicable O Don't know
b) Insurance claim fraud – health and disability insurance: suspected incidents….....		O not applicable O Don't know
c) Advance fee schemes……..		O not applicable O Don't know
d) False billing……		O not applicable O Don't know
e) Other, please specify _____.....		O not applicable O Don't know
Fraud committed by employees		
f) Asset misappropriation…….……		O not applicable O Don't know
g) Improper claims on expense accounts by employees……..…		O not applicable O Don't know
h) Financial misrepresentation ……		O not applicable O Don't know
i) Other fraudulent acts by employees……		O not applicable O Don't know

D 2. In your opinion, what were the most common fraud modes that your organization, as a health insurance provider, dealt with during the reference year? Please rank the following modes of fraud from 1 to 6, with 1 being the most common and 6 being the least common.

___ Misrepresentation to obtain payment
___ Treatment that is outside the scope of practice
___ Kickbacks and referral schemes
___ Billing for services and/or supplies not performed or not provided
___ Intentionally making false representations to obtain payment for services and/or supplies
___ Deliberate performance of medically unnecessary services for the purpose of financial gain.

D 3. In your opinion, what were the most common sources of fraud that your organization, as a health insurance provider, dealt with during the reference year? Please rank the following sources of fraud from 1 to 8, with 1 being the most common and 8 being the least common.

___ Individual policy holder acting alone
___ Group plan member acting alone
___ Plan sponsor acting alone
___ Health care providers acting alone
___ Clinic and/or group of health care providers
___ Combination of individual policy holders or group plan members and clinic and/or health care providers
___ Large organized rings
___ Small organized rings

D 4. Of the incidents of fraud your establishment experienced in the last 12-month reference period, what was the most frequent way in which they were committed? (*check only one*)

O Not applicable: not experience any fraud incidents in the 12-month reference period
O e-mail
O Internet
O telephone
O regular post
O in person
O other
O don't know

D 5. How many claims did your establishment open during the reference year and what was the total dollar amount paid out? *If you are a third party paying on behalf of a participant, skip this question and go to Section G.*

a) Number of claims opened _____

b) Dollar amount paid out $_____

Please go to Section G

Section E – Property and casualty insurance

E 1. How many of the following types of fraudulent incidents did your establishment experience during your last 12-month fiscal period?

	Number of incidents	
Fraud committed by non-employees		
a) Insurance claim fraud – auto/property insurance: investigated incidents……		O not applicable O Don't know
b) Insurance claim fraud – auto/property: suspected incidents….....		O not applicable O Don't know
c) Insurance claim fraud – casualty/injury insurance: investigated incidents……..		O not applicable O Don't know
d) Insurance claim fraud – casualty/injury: suspected incidents….....		O not applicable O Don't know
e) Advance fee schemes……..		O not applicable O Don't know
f) False billing……		O not applicable O Don't know
Fraud committed by employees		
g) Asset misappropriation……..……		O not applicable O Don't know
h) Improper claims on expense accounts by employees……		O not applicable O Don't know
i) Financial misrepresentation …….		O not applicable O Don't know
j) Other fraudulent acts by employees….		O not applicable O Don't know

E 2. In your opinion, what were the most common modes of fraud that your organization, as a property/casualty insurance provider, dealt with during the reference year? Among the following 11 modes of fraud, please rank the top five (5) most common that that your organization, as a property/casualty insurance provider, dealt with during the reference year (with 1 being the most common and 5 being the least common).

___ Fraudulent information provided by client during underwriting process, including the withholding of information
___ Material change misrepresentation
___ Inflated insurance claims
___ Organized auto theft rings
___ Organized injury rings
___ Intentional (i.e. planned) auto thefts
___ Intentional (i.e. planned) auto accidents
___ Arson
___ Intentional (i.e. planned) property damage (other than arson)
___ Intentional (i.e. planned) property theft
___ False injury claims

E 3 In your opinion, what were the most common sources of fraud that your organization, as a property/casualty insurance provider, dealt with during the reference year? Please rank the following sources of fraud from 1 to 4, with 1 being the most common and 4 being the least common.

___ Individual claimant only who is individual policy holder
___ Individual claimant only who is commercial policy holder
___ Large organized rings
___ Small organized rings

E 4. Please provide the number of incidents that your establishment investigated for fraud during the last 12-month fiscal period, according to the nature of the claim (i.e. property or casualty), the nature of the case (i.e., potentially organized rings or not) and the nature of the claimant.

Property claims			
Potentially involving organized rings		*Involving an individual claimant only*	
Claimant is an individual policy holder	Claimant is a vendor	Claimant is an individual policy holder	Claimant is a commercial policy holder
Number of incidents investigated	**Number of incidents investigated**	**Number of incidents investigated**	**Number of incidents investigated**
a)	b)	c)	d)

Injury claims			
Potentially involving organized rings		*Involving an individual claimant only*	
Claimant is an individual policy holder	Claimant is a vendor	Claimant is an individual policy holder	Claimant is a commercial policy holder
Number of incidents investigated	**Number of incidents investigated**	**Number of incidents investigated**	**Number of incidents investigated**
e)	f)	g)	h)

E 5. Of the incidents of fraud your establishment experienced in the last 12-month reference period, what was the most frequent way in which they were committed? (*check only one*)

O Not applicable: not experience any fraud incidents in the 12-month reference period
O e-mail
O Internet
O telephone
O regular post
O in person
O other
O don't know

E 6. How many claims did your establishment open during the last 12-month fiscal period and what was the total dollar amount paid out during that same period?

a) Number of claims opened _____

b) Dollar amount paid out $_____

Please go to Section G

Section F – Manufacturing

F 1. How many of the following types of attempted and real fraudulent incidents did your establishment experience during your last 12-month fiscal period?

	Number of incidents	
Fraud committed by non-employees		
a) Fraudulent use of credit cards…….		O not applicable O Don't know
b) Fraudulent use of bank cards……..		O not applicable O Don't know
c) Fraudulent use of cheques ……..		O not applicable O Don't know
d) Use of false identity in applications or other documents……		O not applicable O Don't know
e) Piracy or counterfeiting of your product…….		O not applicable O Don't know
f) Counterfeit notes……		O not applicable O Don't know
g) Advance fee schemes…….		O not applicable O Don't know
h) False billing…… ……..		O not applicable O Don't know
i) Other fraud… ……		O not applicable O Don't know
Fraud committed by employees		
j) Asset misappropriation……..……		O not applicable O Don't know
k) Improper claims on expense accounts by employees……		O not applicable O Don't know
l) Financial misrepresentation ……		O not applicable O Don't know
m) Other fraudulent acts by employees……		O not applicable O Don't know

F 2. Of the incidents of fraud your establishment experienced in the last 12-month reference period, were there any that were committed by a person residing outside of Canada (i.e., the United States or any other country)?

- O Not applicable: did not experience any fraud incidents in the 12-month reference period
- O Yes
- O No
- O Don't know

F 3. Of the incidents of fraud your establishment experienced in the last 12-month reference period, what was the most frequent way in which they were committed? (*check only one*)

- O Not applicable: not experience any fraud incidents in the 12-month reference period
- O e-mail
- O Internet
- O telephone
- O regular post
- O in person
- O other
- O don't know

Please go to Section G

Section G – Consequences of fraud

G 1. Please indicate the range of financial losses incurred by your establishment as a direct result of frauds experienced during the last 12-month fiscal period? *Include only the amount defrauded and not other expenses incurred as a result of the fraud (e.g. costs associated with civil charges, etc.). Do not include incidents where the amount defrauded was recovered.*

- ○ $0 (no direct financial losses incurred, or no fraud experienced in last 12-month fiscal period)
- ○ $1 to $10,000
- ○ $10,001 to $20,000
- ○ $20,001 to $30,000
- ○ $30,001 to $40,000
- ○ $40,001 to $50,000
- ○ $50,001 to $60,000
- ○ $60,001 to $70,000
- ○ $70,001 to $80,000
- ○ $80,001 to $90,000
- ○ $90,001 to $100,000
- ○ $100,001 to $150,000
- ○ $150,001 to $200,000
- ○ $200,001 to $300,000
- ○ $300,001 to $400,000
- ○ $400,001 to $500,000
- ○ $500,000 to $1,000,000
- ○ More than $1,000,000
- ○ Don't know

G 2. Please provide the estimated amount of dollars your establishment either recovered or avoided losing as a result of detecting fraud.

- ○ $0 (no recoveries or losses avoided as a result of fraud detection, or no fraud experienced in last 12-month fiscal period)
- ○ $1 to $10,000
- ○ $10,001 to $20,000
- ○ $20,001 to $30,000
- ○ $30,001 to $40,000
- ○ $40,001 to $50,000
- ○ $50,001 to $60,000
- ○ $60,001 to $70,000
- ○ $70,001 to $80,000
- ○ $80,001 to $90,000
- ○ $90,001 to $100,000
- ○ $100,001 to $150,000
- ○ $150,001 to $200,000
- ○ $200,001 to $300,000
- ○ $300,001 to $400,000
- ○ $400,001 to $500,000
- ○ $500,000 to $1,000,000
- ○ More than $1,000,000
- ○ Don't know

G 3. Did your establishment incur any financial costs related to any of the following as a result of incidents of fraud experienced during the last 12-month fiscal period? (*check all that apply)*

- O Criminal court procedures
- O Civil court procedures
- O Investments in or operational costs related to fraud detection or prevention initiatives
- O Damage or destruction of databases
- O Other, please specify _____

G 4. Were any of the following impacted as a result of incidents of fraud experienced during the last 12-month fiscal period? (*check all that apply)*

- O Staff morale
- O Business relationships
- O Client relationships
- O Business procedures/policies
- O Brand image
- O Share price
- O Reputation
- O Your business' openness to on-line transactions
- O Your clients' or other business' openness to on-line transactions
- O Other, please specify _____

Section H – Fraud detection and actions taken

H 1. How is fraudulent activity detected by your establishment? Among the following 11 ways, please rank the top five (5), with 1 being the most common way in which fraud is detected by your establishment and 5 being the least common.

___ Reporting by the public, clients, customers, business associates
___ Detection by staff other than internal investigators
___ Use of internal investigators
___ Use of private investigators
___ Use of detection technology
___ Use of letters to verify and confirm services
___ Use of risk management systems
___ Internal audit
___ External audit
___ By accident
___ Other, please specify _____

H 2. In general, how often are the police contacted when a fraud is detected by your establishment?

O Always
O Often
O Sometimes
O Rarely
O Never *(Go to Question H4)*

H 3. When police <u>are</u> contacted, what are the reasons for doing so? Among the following 9 reasons for contacting police, please rank the <u>top five (5) reasons</u> from 1 to 5, with 1 being the most common reason and 5 being the least common reason.

___ Company policy
___ Incident is serious enough: losses were significant
___ Incident is serious enough: suspicion of links to organized crime
___ To try to recover losses
___ To pursue criminal charges
___ Advised by someone to do so
___ Sense of duty
___ Satisfactory experience in the past with police responses
___ Other, please specify _____

H 4. When police <u>are not</u> contacted, what are the reasons for not contacting them? Among the following 11 reasons for not contacting police, please rank the <u>top five (5) reasons</u>, with 1 being the most common reason and 5 being the least common reason.

___ Incident is too minor
___ Don't think the police can do anything
___ Resources required to pursue criminal charges outweigh losses
___ Unsatisfactory experience in the past with police responses
___ Unsatisfactory experiences in the past with criminal courts
___ Company policy
___ Fear of negative publicity
___ Fear of litigation
___ Losses recovered through other means
___ Dealt with another way
___ Other, please specify _____

H 5. How often does your establishment pursue cases of fraud in civil court?

O Always
O Often
O Sometimes
O Rarely
O Never

H 6. At any time during the 12-month reference period did your establishment report fraudulent activity to any of the following? *(check all that apply)*

O Royal Canadian Mounted Police's web-based Reporting Economic Crime On-line (RECOL)
O Ontario Provincial Police's PhoneBusters
O Provincial Consumer Protection Agencies
O The Competition Bureau of Canada
O Other regulatory body
O Better Business Bureaus
O Investigative services of the Insurance Bureau of Canada
O Canada Post
O Financial Transactions Reports Analysis Centre of Canada (FINTRAC)

Section I – Fraud prevention

I 1. Which of the following measures does your establishment have in place that would prevent the occurrence of fraud? *(check all that apply)*

O Formal or informal training/raising awareness among employees

O Formal or informal training/raising awareness among management

O Public announcements/information for clients and business associates regarding fraud prevention

O Publicizing your business' fraud detection measures and/or intolerance for fraud

O Destruction or securing of documents and files containing personal information such as account information, social insurance numbers, etc.

O Securing of electronic databases

O Signing procedures for release or transfer of funds (e.g. need for more than one signature, etc.)

O Daily financial reviews or financial reconciliations

O Use of public information on fraud scams, fraud prevention, etc.

O Background checks on clients using credit bureau information, address verification or other databases available.

O Organization's ethics or codes of conduct with respect to employee fraud and reporting

O Pre-employment screening of employees (e.g. criminal record checks; other reference checks)

O On-going security clearances of employees

O Other, please specify _____

I 2. In your opinion, which of the following initiatives would help to further prevent fraud experienced by your industry (i.e., either retail, banking, payment companies, property and casualty insurance or manufacturing)? Among the following 13 choices, please rank the top five (5) initiatives, with 1 being the most helpful to further prevent fraud experienced by your business industry and 5 being the least helpful.

___ Investment in better detection/security technology that is currently available

___ Investment in specialized/expert human resources

___ Better employee and client training and awareness

___ Better public awareness/public information campaigns

___ A national fraud reporting centre that all victims could report to and that could be a source for businesses and the public to obtain information on fraud scams, prevention, etc.

___ Cooperation and exchange of information among businesses in the same line of work (e.g. through networks, associations, conferences, etc.)

___ Cooperation and exchange of information across all types of businesses (e.g. though networks, associations, conferences, etc.)

___ Partnerships between the police and businesses

___ Informing the judiciary regarding the nature of different types of fraud and their effects on individuals and businesses

___ Changes to the *Criminal Code of Canada*

___ Changes to *Privacy Act*

___ Changes to the *Personal Information Protection and Electronics Document Act* (PIPEDA)

___ Changes to other legislation, *please specify* _____

___ Other, *please specify* _____

Working definitions of selected concepts

The following working definitions of selected concepts were compiled as a result of consultations with credit card companies, representatives from the banking industry, and with reference to definitions used by the RCMP's Reporting Economic Crime On-line (RECOL), the OPP's PhoneBusters and Pricewaterhouse Coopers' Global Economic Crime Survey.

Advance fee schemes: An offer to the business of future benefit that requires an "upfront" fee and where the perpetrator has no intention of fulfilling the offer.

Asset misappropriation: The acquisition through fraudulent means of company assets - including monetary assets/cash, supplies or equipment - by company directors, others in fiduciary positions or employees for their own benefit. Includes embezzlement by employees.

Counterfeit credit cards: Fraud is executed using high-quality imitation credit cards.

False billing: The receipt of bills for products whereby their representation by the promoter was either false or misleading, or whereby the products were either never ordered or received (e.g. paper, toner, business directories, etc.).

Financial misrepresentation: The alteration or presentation of company accounts so that they do not reflect the true value or financial activities of the company.

Fraudulent bankruptcy: Fraud against parties to a bankruptcy, such as suppliers, creditors, partners, shareholders.

Fraudulent use of cheques: The intentional use of cheques with insufficient funds or the use of stolen, counterfeit or altered cheques. Include cheques with forged signatures or false endorsements. Counterfeit cheques are those purporting to be issued by a legitimate account holder where the account holder did not write or authorize the cheque. Counterfeit cheques are often complete replicas of an authentic cheque using a variety of printing methods. Altered items are cheques, drafts or money orders with an altered date, payee or amount.

Fraudulent use of credit cards and bank cards: The use of credit cards or bank cards acquired through theft, theft of identity or personal information, or through counterfeiting to obtain cash, goods or services.

Lost or stolen cards: Losses from the use of a lost or stolen credit card where a secret code is not required.

Non-receipt of credit cards: Interception and theft of a credit card during the process of delivery to the authorized user.

Phishing: An activity that uses e-mail spam to deliver fake messages designed to look like they're coming from banks or other legitimate companies to lure many individual customers into revealing personal or financial information.

Product piracy/counterfeit products: Incidents of illegal copying and/or distribution of fake branded goods in breach of patent or copyright.

Skimming: Skimming occurs when account information is taken from a credit or debit card (via the magnetic strip) and copied by a capture device. Legitimately, this technology is used at point of sale (POS) terminals to gather the necessary information and charged to a customer's account. In debit card skimming, the perpetrator also gains access to the PIN (personal identification number), commonly captured through use of a pinhole camera or by looking over the customer's shoulder (also known as "shoulder surfing").

Worthless deposits (Automatic bank teller machines): Items deposited that are later returned due to empty envelopes.