House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 047 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Tuesday, May 15, 2007

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 15, 2007

● (0905)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): Good morning. I will call the 47th meeting of our committee to order, please.

Committee members, I just want to advise you that your steering committee met late yesterday afternoon to discuss the work plan with respect to the motion that was passed on Thursday and one other matter. I want to let you know that the steering committee report will come to you for discussion and approval or not on Thursday morning as the first item of business.

We are going to try to set up some witnesses, and hopefully they'll be available and ready to go should the steering committee report be accepted. If not, then I'll excuse them, of course. But I just don't want to lose a day if I can avoid it.

So that's how we're going to proceed.

Today we're continuing our study on identity theft, and we have people who we've seen before on other issues.

Welcome.

We have Mr. John Lawford, counsel to the Canadian Consumer Initiative. And we have the executive director of the Canadian Internet Policy and Public Interest Clinic, Philippa Lawson, and along with her is Mr. Mark Hecht.

I take it that there will be two opening statements, will there? Yes, okay.

We'll go with Ms. Lawson first and then Mr. Lawford, and then we'll go with the questioning.

Mrs. Philippa Lawson (Executive Director, Canadian Internet Policy and Public Interest Clinic): Thank you, Mr. Chair.

Bonjour. Good morning, honourable members.

Je vais parler en anglais ce matin.

Thank you very much for the opportunity to speak today about a very serious problem that is directly affecting an increasing number of Canadians and indirectly affecting all of us.

My name is Philippa Lawson. I'm director of CIPPIC, the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa. It was my pleasure to testify before you back in December on PIPEDA, the Personal Information Protection and Electronic Documents Act.

With me today is Mark Hecht, who is a professor of law and CIPPIC's lead researcher on this identity theft project.

We've submitted a written brief to the clerk, which I understand will be translated and distributed to you.

CIPPIC is part of a multi-institution research project on identity theft that's funded by ORNEC, the Ontario Research Network for Electronic Commerce, a public-private partnership, including four major Canadian banks and four Ontario universities. A number of researchers at these universities have been looking into various issues involving the definition and measurement of ID theft, management approaches, and technical solutions to the problem.

We at CIPPIC and at the University of Ottawa are looking at legal and policy approaches to identity theft, and we've been engaged in a big comparative review of what other jurisdictions are doing in this area and where the Canadian law is at.

We've published a series of working papers on identity theft, on various aspects of the problem, most of which are posted on our website—www.cippic.ca—and a couple more will be published shortly.

As you know, we've published a white paper on security breach notification, and we were very gratified to see your recommendations on that in your recent report on PIPEDA.

We've also posted a web page on identity theft, with frequently asked questions and resources for the public.

Our intention, after further research and analysis this summer and fall, is to issue a white paper, with a broad set of recommendations for law and policy reform. And we intend to do that by the end of the year.

You've pre-empted us with these hearings, so we're making some recommendations now, but we will be making more detailed ones later, including in the criminal law area, which I understand you're not looking into in these hearings.

I understand I have about 10 minutes. Do I have less? Okay, great.

The Chair: You now have less, of course.

Mrs. Philippa Lawson: The term “identity theft” is somewhat misleading, insofar as the activity we're talking about covers not just the unauthorized collection or theft of information but the fraudulent use of it. You will find that many experts talk about identity fraud when they're talking about unauthorized use. It really is a two-stage crime. It involves both the unauthorized collection and the fraudulent use. We're using the term “identity theft” broadly as it is commonly used to refer to both stages here.

Identity thieves use a number of techniques to gather personal information. There are relatively unsophisticated methods such as dumpster diving, mail theft, bribing insiders of corporations, and pretexting, which is posing as someone who's authorized to obtain the information in order to get it. There are also much more sophisticated techniques such as skimming, “phishing”, “pharming”, keystroke logging, and hacking into large databases.

A single individual may be victimized many times before he or she knows it. Indeed, victims of identity theft are often unaware of it until they apply for credit from a lending institution and are refused or start getting calls from a debt collection agency. By that time their credit rating has been destroyed and they will likely experience great difficulty restoring it. The victims experience a myriad of difficulties restoring their reputations and recovering the losses suffered, often as a result of no negligence on their part.

I know you're interested in trends. One trend worth pointing out is the use by identity thieves of the Internet to gather and trade in stolen information. It's very easy to find websites right now offering credit card data for sale. Hard drives with personal information on them are being sold on eBay, for example. The Internet, as I'm sure you know, is also used to fool unsuspecting consumers into handing over their account information using techniques such as phishing and pharming. I can explain those later if you're interested.

Unfortunately there are few reliable statistics on identity theft in Canada. PhoneBusters publishes stats based on complaints it receives, but these represent only a fraction of the problem. There are some public opinion surveys that provide insight into the problem, but again it's not complete. We have little else to go on.

Our first recommendation is that we need a national strategy for gathering reliable, reasonably comprehensive data on the incidence, types, and costs of identity theft in Canada.

On identity theft prevention, our research suggests that identity thieves are benefiting as much if not more from unnecessary collection, storage, and trading of personal information by organizations as they are from deficiencies in criminal law enforcement or consumer credulity and carelessness. In many cases there's absolutely nothing the consumer could have done to protect themselves, short of not dealing with the organization that suffered the leak in the first place.

So if we're to attack this program successfully, efforts will be needed in four key areas: data protection law enforcement, prosecution of identity thieves, consumer rights and remedies, and public education.

We have a reasonably good data protection law here in the form of PIPEDA. The law prohibits organizations from collecting more information than they need, retaining it for longer than necessary, and using or disclosing it for purposes other than those for which the individual has consented. It also requires that organizations put in place reasonable security measures to protect against unauthorized access and identity theft.

The big problem with PIPEDA is not any particular substantive deficiency—many of which you have identified in your recent report on PIPEDA—but rather the fact that PIPEDA lacks an effective enforcement mechanism to encourage industry compliance. As a result, many organizations are collecting far more personal information than they need and holding onto it for longer than they should, thereby exposing individuals to a greater risk of identity theft. There are examples of this we can talk about.

Organizations are also failing to secure the personal information they hold through effective encryption, careful employee screening, and other measures. Our study last year of 64 online retailers, which we provided to you last December, confirms that there is widespread non-compliance with even the most basic requirements of the act.

● (0910)

A data breach notification requirement holds some promise for creating incentives for compliance, but only if such notification is made public and only if breaches are not so frequent and widespread as to diminish the reputational damage of publicity. But even so, breach notification rules need to be supplemented with an enforcement regime that creates a real risk of financial penalty for over-collection of personal data or other violations of PIPEDA that contribute to the ID theft problem.

In our submission last December to the committee we made a number of recommendations for strengthening PIPEDA's enforcement regime, including allowing for class actions against organizations that violate PIPEDA, removing financial disincentives for individuals to pursue lawsuits against organizations for breaches of PIPEDA, and punitive damages as a possible remedy for violation of PIPEDA.

We were disappointed that none of these recommendations was adopted or even mentioned by the committee in its report. Addressing this incentive problem, the most important deficiency of PIPEDA and a key factor in the growing problem of identity theft, in our view, is critical if we want to make headway on this problem.

Turning to the issue of public awareness, there are many excellent websites and brochures explaining ID theft schemes and offering tips to avoid identity theft, but there is still a problem. Individuals continue to fall prey to these social engineering schemes, such as phishing and pharming. Young people are posting detailed information about themselves on the Internet, without appreciating the risks.

We are recommending that the Financial Consumer Agency of Canada be mandated to undertake a national public education campaign on identity theft, in consultation with financial institutions, law enforcement agencies, and consumer organizations. The campaign should focus on the most common scams used by identity thieves to gather information directly from individuals and should use mass media, as well as inserts in government mailings, posters, and brochures in store-front offices.

On the issue of consumer protection, first, victims of identity theft usually have no way of knowing the theft occurred until the damage has been done. We think data breach notification will be very helpful in this regard.

Second, even the most educated and motivated victims encounter tremendously frustrating obstacles when they try to attempt to stop the damage and regain their reputations. If such obstacles were removed, victims would be able to mitigate the damage and take preventative action more quickly. In some cases, they could also assist the police in identifying and prosecuting criminals.

● (0915)

The Chair: Excuse me, Ms. Lawson. Could I ask you to bring it to a conclusion? I'm sure anything you haven't covered will come up in questions.

Mrs. Philippa Lawson: Sure. Okay.

The brief mentions a number of specific consumer protection measures that we think are needed to empower consumers.

Our final recommendations are that all of the players in Canada, from law enforcement agencies to consumer protection agencies to financial institutions to consumer groups, work together to address the problem. We need to develop a national strategy for combatting identity theft, and I have seven recommendations.

First, as I mentioned, amend PIPEDA so as to create meaningful incentives for compliance.

Second, appoint a lead agency at the federal level responsible for gathering and reporting ID theft statistics and for coordinating efforts to combat identity theft across Canada.

Third, as I mentioned already, mandate the Financial Consumer Agency of Canada to undertake a national education campaign.

Fourth, establish a national ID theft victim assistance bureau, again with a mandate to gather statistics, analyze the problem, and make recommendations for legislative and policy reform.

Fifth, require credit-granting institutions to report on incidents of ID theft.

Sixth, provide consumers with rights that improve their ability to detect, prevent, and mitigate the effects of identity theft. Those rights should include allowing consumers access to the version of their credit report relied on by lending institutions, which right now is a problem because they are denied access to that, and allowing consumers the right to a credit freeze upon request to credit bureaus, which again is currently not permitted.

Finally, we need a thorough review of legislation governing credit bureaus, lending institutions, and police agencies, with a view to identifying other ways in which these agencies could assist in the prevention, detection, and mitigation of identity theft.

Thank you.

The Chair: Thank you.

Thank you very much for your paper. I know those points are in there. As soon as it is translated, it will be distributed, and we'll have an opportunity to consider your points in more detail.

We now go to Mr. Lawford and his opening remarks.

Mr. John Lawford (Counsel, Canadian Consumer Initiative): Thank you very much.

I'm here today on behalf of the Canadian Consumer Initiative, which is a group of six consumer organizations, including the Public Interest Advocacy Centre, where I work; Union des consommateurs; Option consommateurs, in Quebec; the Automobile Protection Association; and the Alberta Council on Aging. We are presenting to you today our common policy position on identity theft, which we came to agreement on in the last year.

The most important thing to take away from our presentation today is something we're going to echo Philippa's comments on; that is, we believe there's a large role to be played by business and government in attacking identity theft, which has not yet been done, and that consumers also need to be educated, but that the primary steps you can take as legislators would be to move government and business along to better protection of personal information, which will then lead to less identity theft.

I'll just give you a couple of statistics from PhoneBusters, which you probably already have from your researcher. Last year the total reported to PhoneBusters was $16 million in losses on 7,000 to 8,000 complaints, and this is approximately double the amount of money lost but half the number of victims from the year before. I'm not sure if this trend is going to continue, but it's a bit disturbing in the sense that identity theft may be becoming more profitable, and there are more ways to make money from the actual fraud related to it, to be honest.

We also wanted to underline for you that it doesn't have to be this way, because at the federal level, there's a bit of a vacuum in the sense that consumers don't know where to go. When someone gives us a call asking about identity theft, really, I have to take a deep breath and say, where should I send them first? Should I send them first to the police to get their police report? Should I send them to the credit bureau to get their credit report so they know how far this has gone? Should I send them to PhoneBusters to report it? Should I send them to their bank? The actual answer is all of those things, and yet there is no one place for someone to go to the federal government and see that this is the approach to take.

It's not so in the United States, because they have the Federal Trade Commission looking after consumer affairs, and they have taken quite a few steps at their Federal Trade Commission to provide a website that addresses both consumer and business concerns about identity theft.

Take, for example, the FTC's business guide. They have now a safeguard rule in the United States, where if you handle personal financial information you have to follow this rule. It's fairly simple, and it's a bit like PIPEDA, in fact. You have to know what information you have in your files, you have to reduce it to the minimum possible, you have to protect it with security measures that are adequate, you have to dispose of what you don't need, and you have to plan for a data breach.

We have the rule here as well under PIPEDA to do all that; it's just not being done. Our concern here, on behalf of the Consumer Initiative, is that the Office of the Privacy Commissioner of Canada has not been driving that forward, largely because the act itself requires individual complaints. The Privacy Commissioner could take steps to audit companies that seem to have a lot of leaks that might lead to identity theft but has not been terribly aggressive in doing so.

In that situation, it's difficult for us to make recommendations more than Philippa has, along the lines of giving the Privacy Commissioner more authority to act, to make orders, but that has not been suggested by the committee.

One thing we did want to get, and that was suggested in the PIPEDA report, was a breach notification rule. That will lead, we think, to a lot of identity theft being cut off at the knees, if you will, because with the amount of time it takes to actually perform identity theft, a lot of the losses occur in the first two, three, or four days. If something could be put out from the company in that timeframe, people could take some steps to lock down their accounts by calling their bank and getting their credit bureau involved.

● (0920)

One of the things that we suggested for legislation, besides that, was overuse of social insurance numbers, and it still continues today. Social insurance numbers are a key to getting new credit, and part of the identity theft phenomenon is opening new accounts in the victim's name, for which you usually need a social insurance number. The difficulty here is that businesses use social insurance numbers as a unique identifier of the person, and in our common position we called for business to be asked or told in legislation not to use social insurance numbers for that purpose any more and that they be restricted again to what they were originally intended for, which was employment purposes.

Now, we appreciate the difficulty of businesses coming up with a unique identifier and something they can use for credit granting. However, because of the actual nature of the social insurance number being so ubiquitous and used for so many other purposes, it is really a key to fraud. At the bottom line, our position is that we would like the government to look quite hard at the use of social insurance numbers by business and to reduce it to the minimum possible.

Another suggestion in our common position is that the provinces look at credit freezes, so that when you hear about a situation where your identity has been stolen, you can contact the credit bureau and actually disallow any new credit being granted without some extraordinary measures. That's not, perhaps, in your bailiwick, but it does lead to some questions about use of identity information by credit bureaus.

Lastly, you're not dealing with the criminal offences today, but just the mere possession of boxes and boxes of identity at the moment is not a crime, and we are supportive of the justice efforts to make that a crime.

The last thing we'd like to mention comes back to the same point about not having a one-stop shop for Canadians for identity theft. We also have no statistics that are really very detailed on this. We do rely on PhoneBusters, but again, they only take complaints from people who know they take identity theft complaints, so that cuts out a large portion right there, and many other people never actually complain to PhoneBusters.

I know there was an attempt at the RCMP to have a database called RECOL, and I'm not sure where that stands at the moment, but that seems to be an obvious place to try to start centralizing these statistics. An interesting idea that has come about in the United States is asking banks to report on identity theft so that when they get a complaint of identity theft—and they are usually advised by consumers when there's a problem—they could report that either to the RCMP or some other organization to collect statistics on that. We are supportive of that idea, although we haven't put it in our common policy position.

The last point we want to make is that, in this situation, we don't want the consumer to become further victimized, and we see two trends that are not happy ones. One is that financial institutions and others are now offering identity theft insurance, and we don't think that's a silver bullet or really a solution at all because it's not very good coverage. We've done a report on it at PIAC. It covers only your actual time off work to sort out your problems. It doesn't cover the actual identity theft fraud, the money you lose. It has a number of other very minor coverages, but at a more fundamental level, we think it's putting the burden and the cost of trying to deal with identity theft back on the consumer, and it runs counter to the incentive we'd like to give business, which is to protect information more fully.

Finally, we're concerned about the silver bullet, if you will, of biometrics or national identity cards, these sorts of schemes to try to identify a person absolutely. Because identity theft is more of a social crime involving factors like easy credit and lack of care on the part of individuals and over-collection of data, we don't think that having one unique identifier that is linked to everything will make it better. It may in fact make it worse.

So those are our submissions for the committee today, and I'm happy to take questions in English or French. Merci.

● (0925)

The Chair: Thank you very much, Mr. Lawford.

Before we go to the questioning, which we'll start with Mr. Pearson, Ms. Lawson, could you define phishing and pharming, please?

Mrs. Philippa Lawson: Sure. Phishing refers to e-mail communications that are made by the identify thief masquerading as a trusted institution such as a bank or eBay or PayPal or some financial institution. They request the recipient of the e-mail message to provide their account information in order to correct a problem or get access or whatever. I'm sure all of you have received these phishing e-mails. I receive them every day. They're simply ploys by fraudsters to get information that they need to access bank accounts and other accounts, in order to use them fraudulently.

Pharming refers to a similar kind of technique, where the thieves actually set up a website that very cleverly imitates the trusted financial institution or otherwise. They're able to basically redirect traffic intended to go the legitimate website to the fake website. Again, they invite people to enter their account details, etc., and then use that to engage in fraud.

There's a third new trend, which is “vishing”, which refers to voice communication. They're now using telephone communications and computerized messages to call someone. The consumer picks up the phone. There's a computer message that says it's such-and-such a bank—or trusted institution or whatever—and there's a problem with your account. Call this 1-800 number to deal with it. You call the 1-800 number, there's an interactive voice system, and it gets you to plug in all your account information. Once again, they collect it all that way.

● (0930)

The Chair: Thank you.

Mr. Pearson.

Mr. Glen Pearson (London North Centre, Lib.): Thank you, Mr. Chair.

That's a lot of information. I hadn't heard of vishing before.

I have a number of questions, but before I go any further, did you say in your report that the occurrences of identity theft are levelling off?

Mrs. Philippa Lawson: John referred to this, too.

The PhoneBusters data suggests that is the case. I do not consider that data reliable. PhoneBusters is a partnership project by the RCMP, OPP, and the Competition Bureau. I suggest that you have someone from PhoneBusters come and testify about the stats.

Mr. Glen Pearson: It's a bit confusing. All the witnesses have talked about the rapid increase and the various dimensions of it, just as you have this morning. Then on the other hand, we hear that it's actually levelling off. I think we have a responsibility not to intrude too much into things and not to change it if it doesn't need to be fixed. It's difficult to know how to balance that.

You talked about a national strategy, Ms. Lawson, for gathering—You think that this really needs to be done. Who should do that?

Mrs. Philippa Lawson: We think an agency should be appointed to be responsible for that. It should be done, first of all, by requiring organizations that encounter ID theft in their operations—and I know this would be an added burden on business—to keep track of identity theft incidents that their customers have actually suffered, or they have suffered, or that they've avoided and they know about, and to report those annually.

I think that's a way of getting a much better sense of the extent of the problem.

Mr. Glen Pearson: Are you talking about a government agency?

Mrs. Philippa Lawson: Well, someone needs to be responsible for it.

As John pointed out, we have a problem. There is no consumer protection agency at the federal level. Industry Canada, with the Consumer Measures Committee, has some activity in this area, in particular with coordinating provincial approaches. The Competition Bureau does not consider itself a consumer protection agency. It is not particularly interested in this problem, from what I can see.

Mr. Glen Pearson: One of the things the Privacy Commissioner said a couple of weeks ago when she was here was that the real problem is that there is no database of all these things. That's obviously one of the things we're going to have to work on here—how best to do that.

You have listed a bunch of recommendations. We don't have your report, but there were a lot of them. If you had to pick one priority—and I know that's difficult, but we need your direction, since we don't have the report—what is the direction you would like to see us, as a committee, move in?

Mrs. Philippa Lawson: I think it's a complicated problem. It would probably benefit from a task force, something like the task force on spam a couple of years ago. I was part of that. I was involved in a couple of working groups. I think it was a really beneficial, worthwhile process. It brought the various stakeholders together, hammered out some tough issues, and came out with a really good set of recommendations, which unfortunately have not yet been acted on.

I hate to postpone things. I think there are some specific measures that can be taken right away. I've suggested some of those. I do think that if you want to look at the whole picture, this is an issue that would benefit from a task force approach.

I hate to come back to an investigation and review that you've already conducted, but we do feel very strongly that there needs to be some better incentives for businesses to comply with the data protection law.

Mr. Glen Pearson: Thank you.

Mr. Lawford, I volunteer at a food bank. We used to collect social insurance numbers all the time. Charities have pretty well gotten out of that because people don't have to give anything. Yet what you're saying is that lending institutions and others don't use that as a basic form of ID.

You also said you don't like the idea of the biometric card, but you do feel that this whole idea of the SIN number and other things needs to be reduced.

How would you do that? Can you give me an example?

Mr. John Lawford: That is the hard issue because you need a unique identifier. What you maybe don't need is a unique identifier that works for everybody. Why not have one for the credit bureaus, which is the credit bureau type of number? In order to identify yourself for credit, you become whatever this long stream of numbers is, for the purpose of credit. It doesn't have to be for all of the other purposes in society that a social insurance number is used for and has become used for. The trouble with the social insurance number is, of course, that it's used as a password for so many things.

If you create a national identity card, the concern on our part is that it will become like the social insurance number times two—used for everything and only accepted for everything. The idea of keeping things in silos is perhaps one way to go. Now, I'm not suggesting that it's the best way, because we haven't studied the actual use of that and how to get from here to there, but the idea that your identifier can work all across society and for many purposes is part of the problem.

● (0935)

Mr. Glen Pearson: You would look at it then and say we should develop different identifiers for different groups. That seems a little difficult to manage.

Mr. John Lawford: It falls more in with the idea behind the privacy legislation, which is that you use the personal information only for the purposes for which it's been gathered. The social insurance number works like a key across so many different avenues.

Mrs. Philippa Lawson: I will just add that the problem of authentication is a big part of this issue. It's being addressed by industry and the marketplace and government. I'm part of a working group that Industry Canada is chairing on principles for electronic authentication. It's a huge challenge.

One accepted principle is single-factor authentication, that is, like a simple password is insufficient. It's easily cracked. We need to move, and companies are moving, to multi-factor authentication.

Another big problem is that often people want to go with a kind of simplistic form of authentication that involves collection of personal information. In fact, technologists, engineers, and computer science experts have come up with reliable methods of authentication that do not require collection and storage of any personal information. It can be done through computer algorithms, and so forth. The challenge there is to have industry adopt those measures that minimize the collection of personal information rather than the more simplistic ones that don't.

Mr. Glen Pearson: My final question, if I have—

The Chair: No, I'm sorry. You'll have lots of time in round three.

Madame Lavallée, sept minutes.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Thank you, Mr. Chair.

Good morning. Right at the beginning of your presentation, you told us how difficult it is to keep track of this situation. As I listen to you, I gather that several types of fraud happen over the Internet. Fraudulent activity also takes place over the telephone. I have heard of it at home, where I live. People are being defrauded in every way imaginable. In some cases, they are asked for information by people posing as representatives of their credit card institution. Copying credit or debit cards seems to be a third way to steal identities. Are there others?

Mrs. Philippa Lawson: Yes, there are many. We published a report on the techniques of identity theft.

[*English*]

It's posted on our website and it lists the many ways in which identity thieves gather personal information. I can go through more of them now if you wish, but as I said earlier, there's the whole gamut. There are the old-fashioned methods of going through the trash, all the way up to hacking into computer databases. Identity thieves are using all sorts of these methods.

One classic one for debit card theft involves the creation and use of a skimming machine that is often hidden under a counter. You hand over your debit card, and if you don't watch very closely, the guy in the store, the fraudster, will run it through the correct machine, but also through the machine that's designed to collect it for their fraudulent purposes. These skimming machines are sold openly in the marketplace.

● (0940)

[*Translation*]

Mrs. Carole Lavallée: You said earlier that there are traditional methods such as going through garbage and mailboxes, the Internet, where more sophisticated methods are used, as well as by telephone and in stores. I think those are essentially the four methods used. I am trying to get them straight in my mind.

Mrs. Philippa Lawson: Information theft is often done by—

[*English*]

insiders being bribed, so employees of organizations selling the information are handing it over to the thieves. A number of incidents have been traced to insider theft.

[*Translation*]

Mrs. Carole Lavallée: So identity theft happens frequently, and there are many ways to do it. I myself have received an e-mail at home that seemed to come from my financial institution. It was asking me to renew my subscription to something. I am sure that you know the technique. More and more, we hear people say that their credit card or their debit card has been copied. Along with that, we hear that banks are becoming more cautious and that they will instantly cancel the debit card or the credit card of people who have made a transaction where one of their clients' cards has been copied. I understand that financial institutions are becoming more and more cautious, but it is very difficult for consumers to lose the use of their credit card or their debit card over a Christmas weekend. So there is a real problem.

You say that you do not know how many people have had their identities stolen. You do not have any data on that?

[*English*]

Mrs. Philippa Lawson: As I said earlier, there are only two sources of information in Canada on that. One is PhoneBusters, based on the relatively few complaints they get, and the second is some public opinion surveys.

Some colleagues of mine, Dr. Norm Archer and Dr. Susan Sproule, who are part of the ORNEC-funded project I spoke about at McMaster University, are focusing on this statistics issue. They have done a consumer survey, which I believe they have the results of already and will be reporting soon. You might want to hear from them on this issue. The problem is we don't have the statistics we need.

As John did, I would point to the United States, where the FTC has been specifically tasked, through identity theft legislation, to gather and report on statistics. So if you look at the FTC, there is much more information in the United States on the extent of the problem there—still not enough, but much better than here.

[*Translation*]

Mrs. Carole Lavallée: But even so, the banks should have statistics. We certainly see them reacting and becoming more cautious. They are freezing credit cards much more quickly than before. They must know the extent of the problem.

[*English*]

Mrs. Philippa Lawson: I believe the banks are probably the best source of information on the extent of the problem, and that's why we're recommending they be required to report on it.

The Chair: Merci.

For the information of committee members, we have invited PhoneBusters and the people from McMaster to appear before us.

On CIPPIC's website they have—I would say this is a knife with two edges, perhaps—techniques for identity theft. There are 23 techniques listed. So any budding identity thieves, here's where you want to go to see what you can do.

A voice: So these committees are schools for theft.

The Chair: Somehow I feel that not too many identity thieves would be sitting and listening to our committee's deliberations, but you never know.

We'll go to Mr. Stanton, please, for seven minutes.

● (0945)

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chair, and thank you to our witnesses for coming out this morning and shedding some insight on this incredible problem.

First, Madam Lawson, you made a comment in the course of your presentation to the effect that essentially—and I don't know the exact words—many consumers who fall victim to identity theft actually could not have done anything. They inadvertently found themselves in that situation; that is, there was nothing they could have done to prevent that.

At the same time, a good part of your recommendations, and others, I should say, point to the need for more consumer information.

There appears to be an essential conflict between those two points, and I wonder if you could comment on that.

Mrs. Philippa Lawson: The problem has many facets. We're saying that in many, perhaps most, cases, there's nothing the individual consumer could have done. In some cases, there was. In some cases, the problem occurred because the consumer fell victim to a phishing e-mail or a social engineering scheme. They could have avoided that by simply not responding to those e-mails and by just assuming that any e-mail purporting to come from a bank or financial institution is a fraud and deleting it. That's the kind of education we need to focus on.

There are a few things consumers can do. Shred documents with their personal information before putting them in the garbage. Do not respond to those e-mails. And when doing online banking or any kind of on-line financial transaction, look at that URL, the website address, and make sure it's an http address, because the pharming ones usually aren't.

There are certain things consumers can do. Some of the problem stems from consumer credulity and carelessness, but not all of it.

Mr. Bruce Stanton: Thank you.

Mr. Lawford, it came as an incredible surprise that there are still organizations using SIN numbers as unique identifiers. You cited I think an example of opening a bank account. Is it not standard practice now, as far as you know, that when opening, certainly, any kind of financial account, for savings or for investments, whatever the case may be, that photo identification is sort of the new standard that financial institutions have gone to?

Mr. John Lawford: Yes, I know that's often demanded by financial institutions, and that does add a layer of double-checking, if you will.

Part of the recommendation in the first report PIAC wrote on this was that businesses take a few more steps, simple steps like that, to try to verify identity.

Sometimes people will take your credit card from you and not even read the name or check the signature you scrawled down. A simple step is to train clerks to make sure they actually check that the signature matches, and that sort of the thing.

I'm not saying that's a bad thing. I'm thinking more of unnecessary credit checks. Someone is asked to have a credit check done for a new cellphone account. It may or may not be necessary. If it's not necessary, that SIN number gets stored in the cellphone company's database of records. If that database is then compromised, that SIN number goes out, and here we go. That's the sort of situation in which people are making credit applications part of their standard business procedure, and it may or may not be necessary. And they'll always ask for a SIN at that time.

Mrs. Philippa Lawson: Could I make a quick comment on that?

The Privacy Commissioner has decisively found that collecting social insurance numbers, except where required by banks and employers and so forth, violates PIPEDA. It's a violation of the law. So we come back to the problem I was talking about before. The problem is that we're not enforcing the law.

Mr. Bruce Stanton: Thank you.

Surprisingly, that was my next point.

I had visions of a PIPEDA review too, as we heard your presentation this morning. We're back into similar points of discussion around PIPEDA being the driving mechanism by which we can require compliance and a certain set of practices on the part of businesses and organizations. You made the point very clearly that businesses have a role to play in this.

But the Office of the Privacy Commissioner, the Privacy Commissioner herself, clearly lands on the side of believing that the order-making powers are not as necessary and the ombudsman model, if you will, is working effectively. She points to the increase in consumer education around privacy issues. In fact, in one of your points, which I think was point number two, you suggested a lead agency on these matters, as it relates to identity theft.

I would come back to this. Why is it that you take such a separate view from the Privacy Commissioner on these issues? Wouldn't the Privacy Commissioner be the appropriate agency to do exactly that?

● (0950)

Mrs. Philippa Lawson: Sure. I can't explain why. I couldn't disagree with her more on this point.

Mr. Bruce Stanton: You're at odds. You have a different point of view, and that's where we'll leave it.

To go back to consumer protection laws, we had a presentation at our last meeting from the Consumer Measures Committee. This is an organization that is really like an umbrella organization that pulls together the various provinces. We know consumer protection laws are under provincial jurisdiction.

Here we have an organization that is in fact doing exactly what you have recommended should happen. Where do you see that the gap still exists? If the Consumer Measures Committee is in fact driving it, it's an education program, and it's helping to bring it together, where is the weakness?

Mrs. Philippa Lawson: Yes, I think the Consumer Measures Committee is doing great work on this, but it's not enough. It's not pulling in the law enforcement side of things. The police have a lot of information. There's a lot more that they can be doing, particularly once someone has been victimized. Victims are a great source of information about the nature of the problem, as well as the extent of it.

On pulling in other players, we've talked about the banks and lending institutions and their roles. Credit bureaus are a big player in all of this. We find that as we talk to victims and look at case studies, there are problems with the way the credit bureau credit reporting system works. We need to look at that.

On consumer organizations, I think we need to look at the full picture, from the criminal, civil, private and public sector, federal, and provincial aspects. CMC has done a certain amount, but they haven't covered the waterfront.

Mr. Bruce Stanton: There's more work to be done.

Thank you, Mr. Chair.

The Chair: Mr. Pearson, followed by Mr. Van Kesteren.

Mr. Glen Pearson: Thank you, Mr. Chair.

I still have some questions around the SIN, but I'll let it go.

Mr. Stanton, were your questions answered on that? Was it clarified for you?

Mr. Bruce Stanton: Yes.

Mr. Glen Pearson: Okay. Then I won't go into it.

Ms. Lawson, you talked about class action. I know Mr. Lawford said one of the things you want to do is not put too much onus on the consumer. Yet it seems to me a class action almost does that. Is it not true? Could you speak to that?

I know this is popular in the United States. It's not as popular up here. Could you help me with that?

Mrs. Philippa Lawson: We have a number of class actions. Quebec is actually the jurisdiction in Canada that is the furthest ahead with class actions. A number of consumers have achieved remedies through that.

Class actions are in fact specifically designed to empower consumers to make it easier for consumers to stop bad practices and get redress, first of all, by allowing them to obtain legal representation without cost and to be represented automatically as part of the class, even if they make no effort to initially obtain it.

But all you need is one person who represents a whole class of consumers who were subjected to the illegal practice to take the matter to court and retain a class action lawyer. The lawyers will generally take responsibility for the case and will take it forward, typically on a contingency fee basis, and proceed with it in that way. It in fact removes the burden from the individual consumer and obtains redress for the wide class of consumers.

Mr. Glen Pearson: Mr. Lawford, you spoke about the Federal Trade Commission in the United States. On this matter that you and I discussed here in my previous question, about the SIN number or the biometric card, you said there's not necessarily one particular way. You could see a series of options of how to do that. How do they handle it?

● (0955)

Mr. John Lawford: The FTC, at the moment, I believe, has not come out in favour of a similar situation in the States, with the Real ID Act. That idea was, again, that you would be able to use driver's licences that were approved and had a biometric in them for a lot of purposes in the United States, and I believe the FTC came out against it. I would have to check for you.

In terms of your question, how do they handle it, I'm not quite sure what you mean. How do they handle—?

Mr. Glen Pearson: How is it that people's identity, then, can be protected if we're not—?

Go ahead.

Mr. John Lawford: What the FTC does is funnel people to one place, so they say if you have a complaint about identity theft, please tell us, we'll take statistics—and they do. It's the number one hit when you Google identity theft; you get FTC's home page on identity theft.

That's where people go. They know what they're doing. They do take action against individual businesses because they have their consumer protection legislation. Section 5 of their Federal Trade Act says you have to protect consumers, and they have had prosecutions under that; for example, I think Card Systems in the United States had a loss with ChoicePoint. They did start prosecutions. That would be helpful here if we had an agency like that. They said their total sum data practices were negligent in this situation and it was in violation of their Federal Trade Act.

So that's their approach. It's enforcement, it's information gathering, and it's tips for consumers and for business as well.

Mr. Glen Pearson: And did they have recommendations to make about, for example, a biometric card—that it's the best thing—or a social insurance number? You suggested other options. Did they make recommendations?

Mr. John Lawford: I'd have to look and see. I think they came out against the Real ID Act, which is a biometric-type of solution, but I would have to double-check for you.

Mr. Glen Pearson: Okay.

Ms. Lawson, I have a final question, if I have time. You are talking about how businesses need to take more responsibilities, and so on, so it doesn't fall so much on the consumer. One of the things that many of us have been concerned about here is the onerous weight that actually puts on small businesses to be able to do that. Could you speak to that issue?

Mrs. Philippa Lawson: I think it's usually large businesses that are implicated, or at least the cases we hear about. It's usually large databases, larger business, credit-granting institutions that run into trouble, so I'm not sure we're talking about a huge burden on small business.

Again, what we're talking about when we're looking at data protection law enforcement is doing what's common sense anyway, what's good for the business and what's good for your customers.

The Chair: Thank you.

Mr. Lawford, perhaps you wouldn't mind checking. If you can get those answers, perhaps you could contact our researchers and give them the answer.

Thank you.

Mr. Van Kesteren.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you, Mr. Chair.

Thank you, witnesses, for coming again.

It becomes pretty apparent that this is a three-stool approach to a solution.

First of all, we need to make consumers aware, and I agree with your recommendation. I think that's prudent and that's something that needs to be done very soon, and we should take the initiative to do that.

Secondly, yes, I think there must be responsibility to corporations and those that handle credit information.

Thirdly, we mustn't forget one element that needs to be addressed, and continuously needs to be addressed in society, and that's the criminal element. There is a private member's bill, Bill C-299. Are you familiar with that? Do you understand that it deals with phishing and it deals with I think the phone soliciting, the pretext. How do you feel about that? Are we heading off in the right direction? Are we pretty excited about that now?

Mrs. Philippa Lawson: I absolutely support that, but I think it's only one piece of the puzzle. It's certainly not the full solution on the criminal law side, and I understand that the Department of Justice is looking at all of the potential Criminal Code amendments that could give the police the tools they need to pursue identity thieves. We know from our research that there are many more possible ways in which the Criminal Code could be amended to help law enforcement go after the criminals in this area. Pretexting, absolutely, is one of the ways, and we support Bill C-299.

Mr. Dave Van Kesteren: Secondly, and you touched on this, too, there are some pretty exciting new technologies that are available: the national ID card, and you mentioned the biometric ID, radio frequency identification devices. Then I was reading through your brief and there's a note of caution. You seem to be somewhat reluctant to move in that direction: national identity cards, biometric identifiers, integrated government databases have all been suggested as methods by which to reduce the incidents of ID theft; however, these initiatives raise serious privacy issues and should not therefore be taken without thorough public consultation, debate and careful consideration of their dangers in terms of civil liberties and freedom from state control.

I wonder if you could elaborate on that. You seem to be a little reluctant to move in that direction. I wonder why.

● (1000)

Mr. John Lawford: I think at the end of your statement you mentioned its effect on civil liberties, and that's the main concern there: it's a bit outside the field of identity theft. We're also concerned that it won't necessarily lead to the magic bullet, if you will, about identity theft, again because it's not just that someone gets a hold of your identification; it's also that it's very easy to then obtain credit. It's difficult for the victim after they've been victimized to remove past traces of credit and to rehabilitate their credit. So the identity theft objection we have to using biometrics and national identity cards is that on one side there's, again, the public security point of view from civil society that this is not the way to go to monitor people to that extent. We're concerned that it will become a way to track you through your daily life, if you will, because you'll have to present your identity card everywhere you go, and it's then easy to trail people, and that has implications for civil liberties. Then, on the other hand, it may not solve identity theft altogether.

Mrs. Philippa Lawson: Could I just add one point to this? It could in fact make the problem worse, as John stated. Victims have trouble enough right now when their social insurance number has been compromised, for example, dealing with that. Imagine if your biometric identity is compromised, and I can guarantee you it will be. None of these technical solutions is perfect. It will be an absolute nightmare for people to deal with identity theft of their biometric identifier.

Mr. Dave Van Kesteren: Do I have a little more time, Mr. Chair?

The Chair: Yes, 45 seconds.

Mr. Dave Van Kesteren: We're trying to find a balance here. The consumer, too, has to take some responsibility.

John, you were mentioning you were a little bit concerned about tracking people, but we still have cash. I really don't care if somebody knows I go from Ottawa to Chatham, then I take off to Detroit. If I do, I can choose to use cash. Some of these methods really seem to offer some promising solutions. I don't think I've heard enough yet to convince me that this is not the direction we should be going in.

Mr. John Lawford: Very briefly, I can say that I'm not convinced that it's a good idea to leave that trail and that there are more concerns about it, especially as you combine databases. It's possible you can cross-reference your calling records with your movements that day with all sorts of things, and I think there are more implications to this that can be bad in certain situations than we're thinking about.

As far as using cash is concerned, you can't use cash over the Internet and you can't use cash in a lot of businesses—they want to take a credit card—so you're leaving a trail there.

I don't know if that answers your question.

The Chair: Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: You have mentioned PhoneBusters on a number of occasions. I imagine that the image is very clear in English, but I do not understand; is there a French equivalent?

Mr. John Lawford: Actually, even in English, PhoneBusters is a little old as a concept. When they started, the group was set up to deal with telephone fraud. It has evolved since and now receives complaints about identity theft. So the English name could well be replaced by something more appropriate.

Mrs. Carole Lavallée: I just want to understand what it is. Is it an agency, a government organization, a not-for-profit group?

Mr. John Lawford: It used to be an agency of the Ontario Provincial Police, but I think that now it also works with the RCMP. As I said, it is a little vague, it has evolved in the last few years. It would be best to check.

● (1005)

Mrs. Philippa Lawson: The Competition Bureau is also involved with PhoneBusters.

Mrs. Carole Lavallée: Is it an association?

Mr. John Lawford: I do not know the organization's exact status.

Mrs. Philippa Lawson: It is an initiative.

Mr. John Lawford: In fact, it could disappear tomorrow.

Mrs. Carole Lavallée: I suppose there is a telephone number that people can use. I guess that it does not exist in Quebec, because I have never heard of it.

Mrs. Philippa Lawson: Maybe it only works in English, I do not know, but there is a website where you can find information: www.phonebusters.com, I believe.

Mrs. Carole Lavallée: I really do not know much about it, but would they have data on identity theft? Is that included in the questions for the witnesses who are going to be appearing? Okay, I see.

[*English*]

The Chair: They'll be able to explain to us exactly who they are, what they are, what their legal status is, etc.

[*Translation*]

Mrs. Carole Lavallée: Fine. Thank you very much, Mr. Chair.

At the beginning of your presentation, you said that laws needed to be changed. I would like to know which laws you were referring to and how exactly we must change them.

I would ask you to answer one after the other, but not both at the same time.

Mr. John Lawford: There is the Personal Information Protection Act. As the committee has mentioned, the law must be changed to make it mandatory to disclose information leaks.

I do not know whether the social insurance number is included in the act that...

Where does that come from?

Mrs. Philippa Lawson: It is already against the law to use the social insurance number if there is no need to. The problem does not lie in that part of the act.

[*English*]

The problems include enforcement—the lack of incentive and penalty for organizations that collect social insurance numbers when they shouldn't. They refuse the consumer the right to see the credit report that the privacy law says they have a right to see. TJX and Winners are swiping shoppers' credit cards—Maybe everyone should be using cash, and maybe that's what we should be recommending. But that would certainly be contrary to the government's policy of trying to encourage electronic commerce.

They are swiping credit cards and keeping the detailed information from the magnetic stripe, which they are not supposed to keep and are not allowed to keep under privacy law. They're storing it in a database in the United States for years, thereby providing a gold mine for identity thieves.

The big amendments we really need to make here are on the enforcement regime of PIPEDA. We need to give complainants more effective mechanisms to pursue their complaints in courts and to get recourse. We need to have real financial and reputational penalties for organizations that don't comply with the law.

We should also be looking at provincial laws that regulate credit bureaus and provide consumer protection. The Consumer Measures Committee has already done some work in this area, but we need to see how the laws can be improved. For example, they should provide consumers with the right to freeze their credit on the credit report. That means that no lending institution could get access to their credit report without the consumer's explicit permission. That makes sense for victims of identity theft and people who have good reason to suspect they might be victims.

The Chair: Thank you.

Mr. Wallace is next, followed by Mr. Martin.

Mr. Mike Wallace (Burlington, CPC): Thank you, Mr. Chair, and thank you to the witnesses for coming.

I have a couple of clarification questions to understand where you're from. I have a report that you did together in 2003. That was with the Public Interest Advocacy Centre. Now I see that you're two different organizations. Are you all under one umbrella?

A voice: They're divorced.

Mr. Mike Wallace: They're divorced. I see they kept the "law" part of their name.

● (1010)

Mrs. Philippa Lawson: It's coincidental to some extent. I worked as a lawyer for 12 years with the Public Interest Advocacy Centre. The last thing I did was the report on identity theft. When I left in August 2003, the report was almost, but not quite, complete. John took it over and finished it.

In September 2003, I left the Public Interest Advocacy Centre and set up CIPPIC, Canadian Internet Policy and Public Interest Clinic at the University of Ottawa. We are completely separate organizations.

Mr. Mike Wallace: We have the report *Identity Theft: The Need for Better Consumer Protection*, which was completed in 2003. Have any of the recommendations and conclusions in here been implemented? Do you have any idea?

Mr. John Lawford: It has been recommended by this committee for data breach notification. I think that's the major one at the moment. I have to grab my recommendations at the back of it.

Mr. Mike Wallace: Did Industry Canada pay for this study or part of this study?

Mr. John Lawford: Yes, they funded it.

Mr. Mike Wallace: They funded the whole thing. Okay. My researcher got this for me, and I didn't know whether we had done anything on this or not.

I have another clarification question. The consumer group that was here last indicated in their report that there was no data protection law in the United States. Is that accurate, or has that changed?

Mr. John Lawford: That is correct. However, for example, the rule I cited before from the FTC...they have a certain jurisdiction to enforce their general consumer protection act. Under their rule-making power, they've made a rule with financial institutions that requires them to take steps like PIPEDA in terms of safeguarding information.

Mrs. Philippa Lawson: Can I just add to that? The U.S. has a patchwork of sector-specific and issue-specific data protection laws. They do not have this nice, comprehensive law that we have. In fact, the biggest recommendation of consumer and privacy advocates in the United States is that the U.S. adopt a PIPEDA-like law.

Mr. Mike Wallace: Ms. Lawson, you're working on a project right now. Is that correct? Who's funding that?

Mrs. Philippa Lawson: The Ontario Research Network for Electronic Commerce, ORNEC, which is a public-private partnership. Four of the major banks in Canada are funding it, and their funding is matched by the Ontario government.

Mr. Mike Wallace: Sounds great.

The issue we're dealing with here on identify theft—we're trying to stay away from the criminal side of the piece. The issue for me is that if you don't hear about it, you don't see it, you don't know about it, right? So we're trying to talk about communication issues. You talk about these websites and so on. You could have the best website in the world, but if you can't drive anybody to it, it's very beautiful but very useless.

As an organization, and over the years you've been working on this, have you come up with anything unique or anything that would drive—? What would you recommend for us to recommend to drive people to this, to actually read this information?

Mrs. Philippa Lawson: I think you have to use the mass media to reach people.

There are three things we've thought of: using the mass media; inserts in government cheque mailings, possibly, and putting up good posters and brochures in government storefront offices; and working with the banks. The banks are doing a reasonable job, and credit bureaus too have some good public education brochures and things on this issue. But still, people are falling prey.

I think banks are in a difficult situation because they don't want to dissuade people from on-line banking. So they don't want to say you can't trust e-mail, but they have to say you can't trust those e-mail messages you're getting.

Mr. Mike Wallace: John.

Mr. John Lawford: Perhaps I can add that you may want to look at the Financial Consumer Agency of Canada being an agency that might take over that public education role, because they have that role for the banking system.

Mr. Mike Wallace: Just this week my bank that I deal with—and I do a lot of it over the Internet, almost all of it—provided me with a new series of questions that I have my own personal answers to, and then every time I log on they ask me one of the questions: where my high school was—I can't remember them all. There's a series of probably 30, 40 questions they're asking. So I'd say that this particular bank has taken it relatively seriously.

Now this weekend I got an e-mail from my Internet supplier, who's a cable company, at home, saying they were shutting me down because somebody is using my e-mail address to send out spam. Is that identity theft, in your mind?

● (1015)

Mr. John Lawford: That's one of the definitional issues that I hope your next study will cover.

If it leads to a further fraud, such as someone then sending out phishing e-mails and then that person can piggyback off your account, well, that's pretty close, but if you're not losing any particular money, it's not identity fraud, at least. But I still think it should be inside the identity theft umbrella.

Mr. Mike Wallace: This might be my last question.

The other thing I have done—

The Chair: Sorry, Mr. Wallace, here I am, conversing with our researcher and our clerk, and I've given you a bit more time. So I'm going to cut you off now.

Mr. Martin.

Mr. Pat Martin (Winnipeg Centre, NDP): Thank you, Mr. Chair.

Seeing that I was unable to be here earlier, may I have my earlier seven minutes added onto this five minutes?

The Chair: Start with your five minutes and we'll see how we go.

Mr. Pat Martin: Thank you, witnesses. I have only two fairly brief issues, other than to thank you for the briefs.

The NDP has been worried that the new permanent voters list may create what we call an "identity theft kit", in that it's now going to have the date of birth associated with it. Name, address, phone number, and date of birth are a pretty good package of information about any individual, if you had the inclination to use that information. It's freely distributed. In an election campaign, you might have 200 or 300 people coming and going throughout the campaign, and if they're working the phones for you, you tear off a sheet of the voters list and say "Phone these 50 people." So it's wildly, freely distributed.

What is the view of your organizations on the use of the date of birth on the permanent voters list?

Mrs. Philippa Lawson: We oppose it, at least insofar as it's provided to political parties.

There may be good reason for Elections Canada to collect that information for its own internal purpose and to keep it carefully safeguarded and to ensure that it is used for no other purpose. But there is absolutely no reason, in our view, for date of birth to be provided with the list that goes to political parties, and that should not be the case. It runs completely contrary to data protection law principles and fair information practices accepted worldwide.

Mr. Pat Martin: Did you hear that, Mike?

Mr. Mike Wallace: I don't know if there are phone numbers on the list. I don't think they are.

Mr. Pat Martin: Of course, they are.

Well, we put those on the list.

Mr. Mike Wallace: Well, yes, you can look it up.

You're invading people's privacy, Mr. Martin.

The Chair: We're being very collegial today, but maybe you could get to your next question.

Mr. Pat Martin: We were being pretty collegial.

The next issue is brief as well.

I notice that you identify duty to notify as a key concern in your brief. We dealt with that a lot during the review of PIPEDA, and the private sector came in with gnashing of teeth and rending of garments that this was an overwhelming inconvenience. It was impossible. We couldn't possibly tell people, just because we screwed up and lost their information or put it in a dumpster, or something. It would be unbelievable. So we ended up with a very soft recommendation on the duty to notify, leaving it quite mushy.

How far would you go? I notice that you say notice should be given if there's a breach, or even a potential breach.

Mr. John Lawford: That recommendation was in the sense that if there has been a breach and you've recovered your hard drive, or there was a hacking attempt but you're not sure where the data has gone, you would still notify people. That remains our position, because you don't know now, when information moves so quickly; it could be out there.

Mr. Pat Martin: So you're saying notify everybody, not just the credit bureau or the police; notify the individual clients?

Mr. John Lawford: Notify the individuals, because individuals could take immediate steps with their banks to cut off further credit or emptying of accounts. They can get a fraud alert on their credit report—we would prefer a credit freeze, but there you go. They can take a lot of steps, including, if they start seeing things, going straight to the police as soon as they know, rather than saying, "That looks funny", and waiting for a few days until the problem piles up.

Mr. Pat Martin: Ms. Lawson.

Mrs. Philippa Lawson: There are two purposes, in our view, of security breach notification. One is to give individuals the ability to take precautionary measures if it's the kind of situation in which they can. But the second and equally, if not more, important reason is to provide these incentives that I keep talking about on organizations to take those security measures in advance in order to prevent the security breach in the first place. The incentive there is that it's going to get out in the media and they're going to suffer reputational damage.

So I have some concerns with a regime that requires the organizations to report only to the Privacy Commissioner and not necessarily make it public. If you want to get that incentive in place, the information needs to be made public so that the media can decide whether it's newsworthy, and if so, report on it.

● (1020)

Mr. Pat Martin: I agree. Also, pressure from clients, because even if I didn't suffer any financial injury, if my personal information has been compromised two or three times by the same company, I'm not going to do business with them any more. I'm going to move my accounts to this group, which works a little harder to keep my information safe. So that point is very well—

Mrs. Philippa Lawson: Absolutely. I'd say it complements market forces, in that sense.

Mr. Pat Martin: Thank you, Mr. Chair.

The Chair: Thank you, Mr. Martin.

Anyone from there? Okay, I'll take the slot.

Ms. Lawson, you indicated it was your view that the Financial Consumer Agency of Canada—this is my wording—should be mandated to launch a massive education campaign. This is somewhat along the lines of Mr. Stanton's question.

First of all, maybe you could tell us a little bit about the Financial Consumer Agency of Canada, as to who they are, who runs them, to whom they are reportable. We heard last week from Industry Canada's group, the Consumer Measures Committee, which seems to have a good working relationship with their provincial and territorial equivalents, because of course this is an interjurisdictional situation, which is something we really haven't touched on with you. So if we already have them—and I think you said they were doing a good job—why do we need to get the Financial Consumer Agency of Canada involved?

So two questions. What is the Financial Consumer Agency of Canada, and why get them involved if CMC is doing a good job?

Mrs. Philippa Lawson: I'm going to let Mr. Lawford jump in because I think he's done more work with the FCAC.

It's a national agency responsible, as I understand it, for bank regulations involving consumer protection issues. The nice thing about FCAC is that it's national. It doesn't cover all financial institutions, only federally regulated banks, but it has national coverage, which is what we need.

The Consumer Measures Committee has some great information on their website. They are encouraging provinces to do likewise. Some provinces have made some great strides in this area, but when it comes down to it, the CMC is a coordinator of provincial measures, so the citizens of those provinces that choose not to take those measures lose out.

At least in areas of federal responsibility, I think it makes sense to use the federal agency to provide consumers with more one-stop shopping solutions.

I'll let John add to it.

Mr. John Lawford: The Financial Consumer Agency of Canada has taken some tentative steps along this line. I believe they're working on phishing documents, so it would be a natural outgrowth for them to continue their work. Whether banks like it or not, they are at the centre of all this, because inevitably, identity theft is reported to them.

The Financial Consumer Agency of Canada has a mandate to educate the public on matters of financial prudence as well as security, and although it only deals with federal financial institutions, as I said, that's the crossroads for this. So it's one place you can look to in the federal government, and it's a logical place, because it doesn't seem that the Privacy Commissioner is interested in doing this stuff and it doesn't seem that the Competition Bureau is interested either.

The Chair: Is this an agency created by the banks, or is it an agency created by the Government of Canada, or a cooperative, or what?

Mr. John Lawford: It is an independent agency, created by an act, which reports annually to Parliament. However, it is financed by the financial institutions rather than by taxpayers.

The Chair: The CMC, by the way, also has interesting little brochures, cut-outs with interesting information on them.

Mr. Lawford, you mentioned the Federal Trade Commission, and we've talked about it a couple of times. What is their legislative jurisdiction? We've heard there are all kinds of consumer protection laws in each of the individual 50 states; some may have more, some stronger, some weaker, and some may have none. I don't know.

Mr. Lawford, I understood you to recommend that we take a look at them as a model, and I'm just trying to figure out their jurisdiction in the United States.

● (1025)

Mr. John Lawford: This particular safeguard, which I've cited to you, comes out of the Gramm-Leach-Bliley Act in the United States, which requires financial institutions to take due care with regard to customers' personal financial information. That's the source of their jurisdiction, in this particular case. They also have general jurisdiction under the Federal Trade Commission Act to protect consumers. I think section 5 is the right section. So they use both of those.

I know they've had a couple of prosecutions under the section 5 power of businesses after a breach.

The Chair: Go ahead, Ms. Lawson.

Mrs. Philippa Lawson: Unlike our Competition Bureau, the FTC has broader jurisdiction to deal with consumer protection issues. In my view, this is one of the greatest gaps in the federal regime, the fact that the Competition Bureau does not see itself as having a mandate of protecting consumers.

The Chair: Thank you very much.

We go to Mr. Tilson. The only other person I have listed as a questioner is Mr. Van Kesteren. If anyone else wants to question, would you please let our clerk know? Otherwise, that's it—Mr. Tilson and then Mr. Van Kesteren.

Mr. David Tilson (Dufferin—Caledon, CPC): Thank you.

As you know, when we were studying PIPEDA, the topic of notice came up quite a bit. We debated among ourselves and had witnesses. This was as a result of information that escaped from banks—either they thought it escaped and it didn't, or it did escape and ended up in some dump down in the States somewhere. I think Winners was another one. We were given the impression from different speakers that these sources of information didn't want it to get out that these things were happening, and they were going to deal with it.

The credit card companies themselves, Mr. Lawford, are going to cover you if someone takes something on your credit card and you can show that you didn't buy it. It probably justifies their 24% interest charge or whatever. The impression I got from most of the witnesses we heard was that these groups—the banks, the credit card companies, retailers themselves, lawyers—don't want people to know that the information got out or that they got ripped off. Accountants don't want to know that—it's bad for business—so they're going to do whatever they can.

Is this whole topic blown out of proportion? That's my question.

Mr. John Lawford: In the sense that businesses, like banks and credit card companies, make an effort to try to stop identity theft, that is true. On the other hand, as you said, they certainly don't have any interest in telling people when there's been a breach.

Would it be okay to just let it go? No, we don't think so, because the lost information can be used now in so many ways. Some of the ways are setting up new credit or defrauding people in other ways, people who aren't compensated. The credit card companies cover you to a $50 loss in the United States and sometimes down to zero here in Canada, but that's not true when someone uses your personal information to put a mortgage on your house. We had to pass an act in Ontario to cover that situation; a couple of people had their house stolen out from under them. That's a horrifying example.

We just don't know the knock-on effects. The immediate ones might be dealt with by the bank, but perhaps there are more for which consumers won't get redress at all. That's our concern.

Mr. David Tilson: In connection with the mortgage fraud, there was a court case, I think, as well. I don't know which court it was, but somebody said to the banks—the mortgagee, whomever —"That's your problem."

Then you start asking the question. Your presentation was very good, but with all of this information, with everybody who gets this information—everything from your mother's maiden name to your birth date to everything else—and someone commits a fraud on you, even though you've given out this information, is the onus on them to show...should they sustain the loss? I'm comparing it to the mortgagee situation. It may be impossible in many cases, particularly if they've stolen from your bank account, I suppose, but in many cases why should the consumer suffer, particularly when they're being asked to jump through hoops to provide all this information to people?

● (1030)

Mrs. Philippa Lawson: That's exactly why we're recommending that we make it easier for consumers to, for example, engage in class actions against companies that have been so negligent that large numbers of consumers have suffered. We do need to take some legislative actions here to ensure that negligent organizations are held accountable. I don't think it's happening enough right now.

Mr. David Tilson: You mentioned the issue of auditors going into companies and doing audits. Is that too intrusive?

Mr. John Lawford: The Privacy Commissioner of Canada has that power now. So I'm assuming that Parliament didn't think it was that intrusive to put it in at the time. But she has a requirement that she has to have reasonable grounds.

I think when something has come out in the media two or three or four times with one organization, that might be reasonable grounds. Certainly, if we were compiling statistics or there were some other indicators that were objective and factual that might lead to a certain trouble spot or a frequent flier, if you will, on a certain retailer or a certain financial institution, it might be worth an audit, if it's a real chronic problem.

Mr. David Tilson: I know we don't want to talk about the Criminal Code too much, but you're both lawyers.

We haven't heard from you; it would be nice to hear from you.

But have you any thoughts on penalties? Anyone?

Mrs. Philippa Lawson: I can just say that our research shows that the penalties are simply not high enough, and it's just a cost of doing business for the criminals.

Mr. David Tilson: Do you have more on that? Would you make a recommendation?

Mrs. Philippa Lawson: We have published a working paper on case law, which I believe covers criminal law cases as well as civil law cases in this area. I don't have it with me right now with the details. We will be publishing a further one on the issue of enforcement of criminal laws affecting ID theft.

I can just say that our conclusion is that it's very clear and it's one of the problems the police face—and I hope you'll be hearing from them on this: what's the point of spending hundreds of thousands of dollars and hours of their time investigating these often very complicated white-collar crimes when, at the end of the day, they finally catch the guy, they're successful, they've done all their work, and the court just gives them a few months' sentence or a fine that is really just a cost of doing business?

The Chair: There may be some kind of an impression that we're not dealing with the criminal aspects of this, but as far as I know, that has not been a decided fact by this committee at this point, and in fact we're going to be hearing from the Department of Justice. So as part and parcel of our deliberations, we may decide to leave the criminal aspects or we may not, after we hear all the evidence. So I don't want people to think that we have somehow already predetermined that we're not going to be examining the criminal aspects of this. We may choose to do that, but we have not yet done so.

I have two people left: Mr. Van Kesteren and Madame Lavallée.

Mr. Van Kesteren.

Mr. Dave Van Kesteren: Thank you, Mr. Chair.

I have just a few short questions. I wanted to just talk on what Mr. Martin was talking about.

The reason that was given for breach notification and the reluctance to adopt that type of a legislation or policy, or at least the main reason from the witnesses I heard, was that once we begin to do that, consumer apathy would grow and there would be a disinterest; every day you would be saying, “No, there's another one from Zellers, and this one's from the bank”, and after a while you just don't pay any attention.

What about that?

Mr. John Lawford: There's a risk of fatigue in that. However, I believe our recommendation to the Privacy Commissioner on that was that there be a description in the notice you get with a general indication of how serious it is. So hopefully there would be a number that were not so serious that would indicate, “I'm not so serious, we think this is not a big deal”, and others that would indicate, “Yes, this is quite serious, and perhaps you should take some action”. That's one way to approach it.

Another way to approach it, which we suggested to them, was that perhaps there should be a register of every breach. And then people can go through the registry at the end of the year and say, “Oh, actually, I did have an identity theft against me, and look, my company was on there three times”, but not necessarily get a notice unless the Privacy Commissioner, as the committee recommended, thought it was serious enough to recommend a notice go out.

Those are two ways to deal with it. Other than that, I guess we're just disturbed that if there are that many notices going out, isn't there really a huge problem?

● (1035)

Mr. Dave Van Kesteren: No, I would disagree.

Should we make it a law that companies are responsible...they're going to cover their butts, quite frankly, and they will, for any reason, start to—I'm wondering how we get around that—

Mrs. Philippa Lawson: Excuse me. We have a law saying the companies are responsible right now. The problem is it's not good enough.

Mr. Dave Van Kesteren: If we put some teeth into it—So at this point now, if they don't give breach notification, they're liable. I can assure you that we'll be just flooded with anything that—

Mrs. Philippa Lawson: If you're looking seriously at this, I would recommend that you perhaps think about calling some witnesses or hearing from some people from California, which put in place its data breach notification law at least three years ago. They've had experience with it. I've heard some people say there is a problem with notification fatigue.

I think we need, and I personally want to see, some good unbiased studies. Unfortunately, there are very biased studies. Javelin Research, for example, has been hired to do polling and reports by industry who oppose security breach notification, and they're clearly biased reports.

To get a really neutral, unbiased report on the results, how successful that particular approach to data breach notification has been, very much depends on the thresholds you set for notification. Obviously, the higher the threshold, the fewer notifications will be required. There are different ways of doing it, as you have suggested in your report, and as John is saying now, which could involve a public registry, the Privacy Commissioner as a kind of filter, and check on whether or not notification is required in that particular circumstance.

Mr. Dave Van Kesteren: Very quickly getting back to responsibility of consumers, I don't read anywhere and I wonder why—Why don't we put warning labels, like we do on cigarette packages? Simply throw them up on the screen, you know, that this and this can happen? Is that a possibility? Is that something you've —?

Mr. John Lawford: It's a question that might come up in a situation like on-line banking, where you could say this is a potentially risky activity. I don't know whether the fatigue would show up there or not. But one of my concerns is that consumers take in e-mails, and if they're from a financial institution, as Philippa said, they don't know that 99% of those from financial institutions are frauds. Perhaps they should get a list mailed to them from their bank once a year, telling them that when they get an e-mail from someone asking for account details, do not reply. I don't know if it's being done or not.

Are there other warnings you can think of?

Mrs. Philippa Lawson: I think the problem is that banks and other industry are quite loath to issue such warnings because they don't want to deter people from engaging in on-line commerce.

Mr. Dave Van Kesteren: But if we made it a requirement that if you accept moneys over the Internet, when an institution does that, they are required to say that when you do this sort of stuff there are risks. That would provide some consumer awareness.

Mrs. Philippa Lawson: Two problems. One is that the fraudster isn't going to issue those warnings. I'm trying to think how it would technically work. What's happening is that the individual is not in fact dealing with legitimate organizations. They think they are, but they're dealing with the fraudsters. So how is the warning going to reach them at the time it needs to reach them? I'm not sure how that would work.

Secondly, as I've already pointed out, even if you were able to warn customers—actually, if you could get all customers to stop responding to all phishing and pharming and all of that, it's only going to deal with a fraction of the problem. We still have, but without the statistical support, what seems to us is that perhaps the majority of the problem here is leaks by businesses, hacking into computer databases, insider theft and such, which consumers have absolutely no power over.

The Chair: Thank you.

Madame Lavallée, and then an intervention by Mr. Wallace.

Mr. Reid, a point of order.

● (1040)

Mr. Scott Reid (Lanark—Frontenac—Lennox and Addington, CPC): Thank you, Mr. Chairman.

I apologize to Madame Lavallée and to our witnesses for doing this at this time. I'm simply worried that we're about to run out of time at this meeting.

My understanding is that the subcommittee that deals with studying the agenda for this committee has made arrangements to deal with the matters of the motion that had come before this committee and was voted on relating to Afghanistan and so on. I assume that involves summoning witnesses as early as Thursday, and I am concerned that we won't have a chance to discuss this prior to that actually taking place. That would obviously be problematic from the point of view of ensuring that the committee has reached a consensus with regard to who we're summoning.

I'm hoping we can all find a way of leaving ourselves enough time to deal with that today.

The Chair: Thank you for bringing that up. I'm sure we're not going to exhaust the clock, so let me deal with that. It's not a point of order, but it's a legitimate question. I was going to deal with it.

First of all, the committee decides what we do, not the steering committee. The steering committee makes recommendations. In fact, the steering committee did meet, and it has recommendations, which will be circulated.

The first item of business on Thursday will be the steering committee report. It will be up to the committee to decide whether it wishes to adopt that report, either as presented or as amended.

On the off chance that the committee will adopt that steering committee report, either as presented or as amended, we do have a confirmed witness—one so far—for Thursday. Mr. Jeff Esau is a freelance journalist, who sold his story to the *Globe and Mail*. He has made two access to information requests with respect to this matter.

Obviously he will be here so we don't lose the time. If we spend the entire meeting discussing the steering committee report, so be it. That's the decision of the committee. But he will be here in the event that the decision is relatively quick. If we don't get to him, he'll be available once the committee makes the final decision.

At the present time, the committee's decision is to proceed with identity theft. But because of the wording of “urgently consider”, I'm putting the steering committee's report as the number one item of business for Thursday morning at 9 a.m.

Does that answer your question?

Mr. Scott Reid: It does, Mr. Chair.

The Chair: Thank you.

Madam Lavallée, and then Mr. Wallace.

[*Translation*]

Mrs. Carole Lavallée: I do not necessarily have questions. I would like to talk about the list of guests who are going to discuss identity theft. I wonder when it would be best to do that.

[*English*]

The Chair: Not now. We have our witnesses here.

You could make your suggestions to our clerk. He can discuss whether they are already on the extensive list of witnesses. If they are not, then we can discuss it among ourselves. So just give the list to the clerk.

[*Translation*]

Mrs. Carole Lavallée: Fine.

[*English*]

The Chair: Okay. *Avez vous des questions?*

[*Translation*]

Mrs. Carole Lavallée: Yes. Earlier, we started to talk about the laws that need to be changed, and I did not feel that you were sufficiently clear on which federal laws we can change. During the discussion, you added that we must require stores to be more vigilant in combating fraud. You mentioned making class actions easier to bring. in Quebec, we have everything we need to bring class actions; I do not know how things happen in other provinces. You also mentioned provincial laws.

In your opinion, does identity theft fall under federal or provincial jurisdiction?

Mrs. Philippa Lawson: Both, federal and provincial.

[*English*]

In terms of the class actions, we are recommending specific amendments to PIPEDA. If you look at our recommendations numbers 1 to 7 in our submission of November 28 on PIPEDA reform, we're saying the provinces, particularly Quebec, have a very effective class action system. The problem is that complainants under PIPEDA have no way of pursuing those complaints in a Quebec class action right now. You need to amend PIPEDA in a way that allows them to use the class action system to pursue their complaints.

[*Translation*]

Mrs. Carole Lavallée: No, because in Quebec, there is another act that protects personal information, a Government of Quebec act. Class actions work well in that system, so we do not need, in PIPEDA—

● (1045)

Mrs. Philippa Lawson: But if problems arise with a bank that is regulated—

Mrs. Carole Lavallée: Yes.

[*English*]

Mrs. Philippa Lawson: If it's a federally regulated institution, the matter falls under PIPEDA, as opposed to the Quebec law.

[*Translation*]

Mrs. Carole Lavallée: That is worth checking out, but I think that there have even been class actions in Quebec against the federal government. So I think that the system or the program of class actions has nothing to do with the person being sued. I am not a lawyer, I am just telling you what I have seen and heard.

You do not just need a translator, but an interpreter as well.

Mr. John Lawford: The proposed amendment is intended to make it absolutely clear that you can undertake an action or a process like that in Quebec, following your own rules.

[*English*]

Mrs. Philippa Lawson: If I can also add, it may be the case that for most cases in Quebec, consumers have the recourse and remedies they need provincially. It's not the case in all other provinces. We still need to reform the federal law for the rest of Canada, even if Quebec consumers are adequately protected.

[*Translation*]

Mrs. Carole Lavallée: Last week, one of the witnesses—I believe it was the lawyer from the Office of the Privacy Commissioner—told us that it is not a crime to steal someone's identity, but it is a crime to use the information obtained.

Can we come up with some kind of legislation so that identity theft becomes a crime?

[*English*]

Mrs. Philippa Lawson: This is one of the recommendations that many people are making for a Criminal Code amendment. It is in fact an offence under the Criminal Code right now to collect and possess credit card information without lawful excuse. I believe it may be so in some other specific situations.

The law enforcement agencies say they can sometimes catch someone with a huge amount of non-credit card data and other personal information and documents, such as social insurance numbers, names, and addresses, which it's pretty clear that person was planning to use for identity fraud purposes. But because there is no specific offence in the Criminal Code for possession of that kind of information without lawful excuse, they have nothing to charge the person with.

It is one of the possible Criminal Code amendments that I know the Department of Justice is looking at and we are looking at as well.

But I think you need to be very careful before simply creating new offences. There may be many situations in which people lawfully have information about others, with a lawful excuse. There definitely needs to be a criminal intent requirement. But it is certainly the case that much of the unauthorized collection is not a criminal offence right now.

The Chair: Thank you. Merci, Madame.

Madame Lavallée, when you discuss suggested witnesses with Mr. Rumas, you might think about le Barreau or some legal entity in Quebec. They could come and give us the exact status of class actions, how they're started in Quebec, and what the rules are.

Hopefully, it would clear up the question you were dealing with about a specific witness with expertise in Quebec law. *D'accord?*

[*Translation*]

Mrs. Carole Lavallée: Fine.

[*English*]

The Chair: Our final questioner is Mr. Wallace.

Mr. Hecht, this is your last chance to get your voice on tape. This will be it for you.

Mr. Wallace.

Mr. Mike Wallace: I'm sorry, Mr. Hecht. This is not really a question for you, but you're welcome to answer, if you want to.

I want to make sure I understand. Out of this, we will have a report on what the recommendations are.

Ms. Lawson, you said a task force would be one of the primary ones on your list. We did the report in 2003 and industry paid for it. How much did it cost? Do you have any clue? Was it hundreds of thousands of dollars or was it $50,000?

● (1050)

Mrs. Philippa Lawson: I can't remember the amount. It was between $25,000 and $40,000.

Mr. Mike Wallace: Okay. It was under $100 Gs for that.

It was finished in 2003, and nothing has really happened with the recommendations and conclusions that were in there. What would you say?

Mrs. Philippa Lawson: Some of the work the Consumer Measures Committee has done since this report is consistent with our recommendations, such as creating a standard affidavit for victims.

Mr. Mike Wallace: It's about the value for money. Is another task force going to do anything different from what's already in your 2003 report?

The Chair: Ms. Lawson, it's my fault, because I've let the meeting go on, but you do not need to push that button. We have a person to do it.

Mr. Mike Wallace: Oh, I thought I had asked the wrong question or something.

The Chair: It's really my fault. Just don't touch the button. She'll look after it for us at all times. I should not have let it go until the final hour before we got to it.

Sorry, Mr. Wallace.

Mrs. Philippa Lawson: The recommendation for the task force is just designed to try to bring everything together under one umbrella and to make sure it all gets dealt with. I think there are a number of initiatives and legislative amendments and policy reforms that clearly can be made.

I was asked what would be the most important one. Creating a national identity theft victim assistance bureau would be incredibly useful, not just to assist victims but to collect the statistics and understand the problem better.

Mr. Mike Wallace: Just so I understand, a task force is not a volunteer organization. Industry or somebody would pay for that study to be done.

Mrs. Philippa Lawson: I'm talking about an exercise similar to what occurred with the task force on spam.

Mr. Mike Wallace: Okay. Thank you very much.

Mrs. Philippa Lawson: Industry Canada oversaw that and put a lot of effort into it.

Mr. Mike Wallace: I just wanted to be clear, for my understanding. Thank you.

The Chair: I'm sorry, it's a national identity theft—

Mrs. Philippa Lawson: It would be a national identity theft victim assistance bureau.

The Chair: —victim assistance bureau.

We'll have a short question from Mr. Tilson.

Mr. David Tilson: You just mentioned actually, by coincidence, the question I was going to ask. From your 2003 paper that you prepared, can you briefly elaborate on the standard ID theft affidavit? It's on page 52 of your report.

Mrs. Philippa Lawson: Yes. This is to make it easier for victims. Right now, victims have to deal with many different institutions, and each institution has its own forms and requirements for authentication and proof that there was in fact fraudulent use of their information. It's an incredible nightmare and a huge task for the poor souls.

Mr. David Tilson: How about an affidavit? You can take a fraudulent affidavit.

Mrs. Philippa Lawson: Yes, that's part of the problem. They are treated as suspects.

Mr. David Tilson: I just wanted to understand the form. If you're going to go to the trouble of defrauding someone, a fraudulent affidavit is a piece of cake.

Mrs. Philippa Lawson: Yes, but we're also talking about making things easier for victims. There are ways that this can be done.

Mr. David Tilson: Thank you.

The Chair: Okay. Thank you very much.

I want to thank our witnesses for their expertise and their viewpoints and their recommendations. We'll look forward to Mr. Lawford, I believe, getting back to us on the Federal Trade Commission, if he can.

I'll adjourn the meeting, then, until 9 a.m. on Thursday, at which time we will deal with the subcommittee on agenda and procedure's first report.

Mr. Mike Wallace: Who's adjourning the meeting?

The Chair: I am.

I'm sorry, Mr. Martin, did you have your hand up? I didn't see you.

Mr. Pat Martin: You just announced that on Thursday we will deal with the subcommittee's recommendations to the main committee.

The Chair: Correct. That is the first item of business. And we have Mr. Jeff Esau confirmed as a witness should the committee decide to proceed.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca
