House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 026 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Tuesday, January 30, 2007

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, January 30, 2007

● (0900)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): Good morning. I'm pleased to call this meeting to order.

Welcome to 2007 on our committee. I hope everybody had a good break.

Before we go any further, I just want to point out that there have been some changes in the membership of the committee. We have three new members to replace three members who were on the committee in the last year.

On my left we have Mr. Glen Pearson, who is now sitting where Mr. Paul Zed used to be. On the right, although he's not here, Mr. Scott Reid will be here for Mr. Jason Kenney, and Mr. Robert Vincent will replace Monsieur Laforest.

Go ahead, Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Good morning, Mr. Chairman. It's a great pleasure to see you again. I hope you had nice holidays.

Unfortunately, there was December 15th. A motion by the committee asked the Minister of Justice—no, you can't run or hide, Mr. Wallace— to present to us a modernized and strengthened access to information bill by December 15. Unfortunately, the Minister of Justice did not fulfil his obligations. Moreover, he was replaced.

Under these conditions, perhaps we could find a moment today, at the beginning rather than at the end of the meeting, to determine whether it would be possible to examine or reiterate this motion or even to ask the new Minister of Justice to meet with us to discuss his intentions regarding the access to information bill.

[*English*]

The Chair: That's all very interesting. I have to point out that the meeting was called for the purposes of hearing our witnesses, and they are here today, so I don't think it's fair to them to have us get into a prolonged discussion on that issue. If there's time at the end of the meeting, then we could certainly deal with it.

I don't disagree with anything that you said, Madame Lavallée, and it would not be a bad idea if we had an opportunity to call the Minister of Justice on this issue; however, we've already decided on a work plan that provides for what we're going to be doing with respect to PIPEDA from now until pretty well the end of February, so if you want to bring another motion or have the committee consider it, please by all means do that.

I also point out that there is the opportunity for the oppositionto ask questions of the ministers in the House of Commons, and one hopes that possibly an answer might be forthcoming, so if you don't mind, I'd like to welcome our witnesses and encourage you to find the appropriate method by which to bring this matter forward.

Go ahead, Monsieur Vincent.

● (0905)

[*Translation*]

Mr. Robert Vincent (Shefford, BQ): Mr. Chairman, I think that you're acting rather hastily.

When a member makes a request, it's not enough to simply say we're going to follow the established agenda and simply ignore that request. A motion was tabled, and I think we have to consider it. I think it's up to the committee and not up to the chair to decide what will go on. In my opinion, the job of the chairman consists in managing the committee, not deciding on everything that will happen there.

Therefore, if a member asks to speak, to invite a minister to appear or to have a motion adopted, I think that supercedes anything the committee does with regard to witnesses.

[*English*]

The Chair: Of course, I appreciate the views of the new member. I don't agree with your characterization of the duties of a chair—I suppose you'll find that out as you continue to sit on this committee with me. In any event, there is no motion that is recognizable this morning. If there is a motion, under our procedure, properly put forward and for which notice is properly given, you can be assured that the chair will bring it to the attention of the committee.

I do agree that the committee is the master of its own business—there's no doubt about that—and the business of the committee has been decided: it is to continue with the PIPEDA review, and that's why we have the witnesses here before us today.

Go ahead, Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: First of all I'd like to apologize to our guests. You will understand that we must now settle certain logistics problems. I'm really very sorry, and with your permission, I will continue.

Mr. Chairman, we were to stand on procedure or be legalistic about this, you would have to acknowledge that I am allowed to table a motion. In fact, in order to do so, I would have to give notice of motion. However, a motion asking the minister of Justice to appear about an access to information bill has already been voted upon and adopted.

Under the circumstances, I would have thought that logic and the principle of reasonable accommodation would have meant that during today's meeting—I would have preferred it to be at the beginning, but it could also be at the end—you would make a commitment to reserve five or ten minutes to see whether it would be possible to receive the new Minister of Justice, or to submit our motion to him.

[*English*]

The Chair: I am completely in agreement with you. We can certainly deal with it when the witnesses have given their evidence. The fewer the questions there are from members, the faster the evidence will go. If there's time before 11 o'clock, then of course we can deal with that matter and see if there's a consensus in the committee, or if things will have to be done according to strict procedure. So let's see how we can handle it based on the number of questions to our witnesses.

D'accord?

[*Translation*]

Mr. Robert Vincent: Yes.

[*English*]

The Chair: I would like to welcome, from the Canadian Bankers Association, Mr. Warren Law, senior vice-president; Mr. Terry Campbell, vice-president of policy; and Linda Routledge, director of consumer affairs. From the Credit Union Central of Canada, we have Gary Rogers, vice-president of financial policy; and Charlene Loui-Ying, general counsel and government relations officer for the Credit Union Central of British Columbia. Welcome to you all.

You will have an opening statement—two statements, I presume—and then we'll have our usual questioning. We already have some other issues, so we'll see how it goes.

Mr. Law, perhaps you could start.

Mr. Warren Law (Senior Vice-President, Corporate Operations and General Counsel, Canadian Bankers Association): Thank you, Mr. Chair.

Mr. Chair and members of the committee, thank you for inviting us to be here with you today to contribute to your review of part 1 of the Personal Information Protection and Electronic Documents Act, PIPEDA.

I am the senior vice-president of corporate operations and the general counsel of the Canadian Bankers Association. I also act as its chief privacy officer. With me today, as you've heard, is Terry Campbell, our vice-president of policy, and Linda Routledge, our director of consumer affairs.

At the outset may I say that the banking industry has long been a leader in privacy protection, being the first industry to have a detailed privacy code, first introduced about 20 years ago. The industry also participated in the development of the Canadian Standards Association model privacy code that is referenced in schedule 1 of PIPEDA. Our privacy code was the first to be acknowledged as being consistent with that standard. I might say that protection of personal information has always been a cornerstone of banking and one of the banks' highest priorities.

● (0910)

[*Translation*]

Nevertheless, when handling over 11 million transactions each day for our customers, errors can and do happen. The banks' goal is to minimize such errors, to protect our customers' interests, and to take steps to ensure that such problems do not recur. Considering the almost daily interactions that customers have with their banks, the relatively small number of privacy complaints raised with the Privacy Commissioner provides strong evidence of the banks' success in protecting personal information.

The banking industry was one of the first industries to be subject to the PIPEDA when it came into force in 2001. Generally the banks are of the view that the act has served Canadians well. We have only a few suggestions—mostly of a technical nature—for changes that we recommend be made to the act. They are set out in detail in our submission, but I would like to highlight a few of them for you today.

[*English*]

I'd like to speak first about a proposal dealing with the public interest exemption. Situations arise where the act's current requirements prevent employees from acting in the interest of the greater good of an individual or group of individuals. An example of such a situation in the banking context is where a banker suspects financial abuse, particularly with seniors, and when a customer is withdrawing money from his or her account and it appears that the customer may be under pressure from the person accompanying him or her, or the withdrawal is uncharacteristic of that person.

Prior to PIPEDA, under common law, banks were able to disclose their suspicions about abuse to the authorities, to the vulnerable customer's family, or to another responsible person who might be able to investigate and stop any abuse. Financial abuse of the elderly is a significant issue in Canada. The public and families of such customers expect bankers to help prevent any abuse. Under the current legislation, though, while branch employees want to help, they are not allowed to because there are no exceptions that cover such situations.

We are recommending an exemption for disclosure without consent when it is in the public interest.

Next I'd like to suggest changes to the way PIPEDA deals with investigations. The banks spend considerable effort and expense to prevent their operations and customers' personal information from being used for any kind of financial crime, whether it is a scam, identity theft, deceptive telemarketing, debit or credit card fraud, or money laundering. They provide employee training and customer awareness programs, and they cooperate with governments, law enforcement agencies, and other bodies at both the national and international levels.

It would help our efforts if the act were amended to follow British Columbia's approach. Instead of designating “investigative bodies”, as is the case now under PIPEDA, adopting the B.C. approach would allow organizations to collect, use, and disclose personal information for the purposes of an investigation. This would eliminate some of the current inconsistencies and allow information to prevent fraud.

Inconsistencies in the act frequently interfere with the bank's ability to investigate and prevent illegal or fraudulent activities. For instance, while the act allows an organization to collect and disclose information relating to a breach of an agreement, it does not allow for internal use of that same information to prevent further fraud against that customer, other customers, or the bank itself.

Similarly, a bank investigating a fraud could find and use internally information suggesting contravention of a foreign law, but would be unable to collect any further information to confirm that suspicion. The bank could even disclose that information to the banking industry's investigative body, the Bank Crime Prevention and Investigation Office, but the BCPIO could not do anything further with that information because it is not able to disclose information relating to the contravention of a foreign law, even to local authorities or other local organizations that might be similarly impacted. This causes significant barriers to investigating and preventing further crimes against the broader cross-section of the industry and its customers.

We are recommending that the act be amended to include these and other valuable enhancements from their provincial statutes.

There is also a need to change how PIPEDA deals with corporate groups.

● (0915)

[*Translation*]

To meet regulatory reporting requirements, for example for anti-money laundering and risks/capital adequacy, banks are required to report on their entire corporate group as one entity. Many organizations, including the banks, have located their privacy officer at the most senior levels in the overall corporate group and this officer acts in that capacity for all entities within the group. In both types of situations it is necessary for personal information to be collected, used and disclosed within the entire corporate group, not held exclusively within one part of it. The act needs to be amended to better address the needs for corporate groups to share information amongst corporate entities for such purposes.

[*English*]

I should note that there are areas where some stakeholders are seeking changes to the act, but where the banks believe that the legislation continues to effectively balance the needs of various stakeholders. For example, let's talk about the commissioner's powers. The commissioner's existing ombudsman approach to oversight appears to be working well. In almost every instance where the complaint has been deemed well founded and the commissioner has recommended changes, the organizations affected have followed the commissioner's recommendations. Where there have been any difficulties, the threat of Federal Court action generally has led to compliance. The commissioner has the option also, where it is in the public interest, to name organizations that have not complied with the act, and the commissioner has done so at least twice. She also has the ability to conduct audits and to instigate her own complaints, which she has already begun to do. In our view, the current oversight approach and the tools for the Privacy Commissioner are consistent with similar regulatory bodies. The banks concur with the commissioner's own view expressed to you that her current powers have proven to be effective and that no changes are needed at this time.

There is also the issue of breach notification. The banks support the need for an organization to notify individuals of a breach if an internal investigation concludes that there is a reasonable risk that the individual's personal information could be misused for fraudulent purposes or for identity theft. This is a standard accepted internationally in financial services. Banks take very seriously the responsibility to keep their customers appropriately informed and believe that organizations in Canada have been fulfilling this responsibility effectively on a voluntary basis. We do not believe that legislated requirements are needed.

Lastly, there is the issue of outsourcing. The existing provisions in the act provide the necessary framework to protect personal information about Canadians when organizations outsource functions either domestically or internationally. An organization must ensure that the personal information provided to third party processors is given the same protection as the organization itself must provide under PIPEDA. Outsourcing is a reality of Canadian business and contributes to Canada's economic growth and prosperity. The act provides the necessary protections to balance this interest with the protection of individuals' personal information.

Mr. Chair and members of the committee, we thank you for your attention to our comments, and of course we would be pleased to answer your questions.

The Chair: Thank you very much, Mr. Law. Thank you for being succinct and for making some specific recommendations.

Will it be Mr. Rogers giving the presentation? Go ahead, sir.

Mr. Gary Rogers (Vice-President, Financial Policy, Credit Union Central of Canada): I'll begin.

Good morning, Mr. Chair and committee members.

Thank you for this invitation to come before the committee today to discuss the Personal Information Protection and Electronic Documents Act.

My name is Gary Rogers. I'm vice-president, financial policy, with Credit Union Central of Canada, commonly known as Canadian Central. My co-presenter today is Charlene Loui-Ying, general counsel and government relations officer at Credit Union Central of British Columbia, commonly known as B.C. Central, which is our largest shareholder and member institution.

Canadian Central is a federally regulated financial institution that operates as the national trade association and financial facility for our shareholders, which are the provincial credit union centrals and through them the 501 affiliated credit unions across Canada.

I mentioned that Canadian Central is federally regulated. Provincial centrals are provincially regulated, although some of them are also federal regulated through OSFI. And credit unions, of course, are provincially regulated.

A statistic that surprises many is that our credit unions employ more than 24,000 Canadians coast to coast, many or most of whom require knowledge of and training regarding privacy issues. Those employees serve our members, who number over 4.9 million Canadians.

At the end of the third quarter of 2006, our credit unions held close to $93 billion in assets, which grew by 10% over the previous year.

The evolution of PIPEDA is of great interest to the credit union system, because the activities of some parts of our system, including Canadian Central, fall directly under that act. Credit unions are also directly regulated by PIPEDA in those provinces that have not introduced substantially similar privacy legislation. Further, the evolution of PIPEDA will undoubtedly have a strong impact on provincial privacy legislation, which in turn will directly impact credit unions.

Like all Canadians, credit union members set a high priority on the protection of their personal information, and credit unions have a long-standing commitment to protect the privacy of our members. In fact, Canadian Central was a contributing member of the Canadian Standards Association technical committee on privacy that worked on drafting the model code for the protection of personal information. That model code eventually formed the basis for PIPEDA.

Credit unions work to prevent their members' personal information from being used in a manner that's not been consented to and they endeavour to prevent such information from being used in any kind of financial crime, be it identity theft, deceptive telemarketing, debit and credit card theft, or money laundering.

This commitment to member privacy is enhanced through employee training programs, strong internal policies and procedures, member awareness programs, and continuing cooperation with provincial and federal governments and law enforcement agencies.

In general, the credit union system believes that PIPEDA serves Canadians well in protecting personal information. The act, and similar provincial legislation, has provided business organizations, including credit unions, with that practical framework for formalizing our policies and procedures aimed at protecting the privacy of member customers.

We recommend that the federal government proceed cautiously with changes to PIPEDA, especially in light of the fact that Canada is only two years into the full application of the act. It may be too early to properly judge the real impact of the existing legislation.

If amendments to PIPEDA are to be recommended, Canadian Central suggests aiming for a couple of principles: that there be greater harmonization between federal and provincial privacy legislation, and that consideration be given to selecting the easiest and most cost-effective approach to achieving the objectives of each change.

In the following comments, my colleague, Ms. Charlene Loui-Ying, will outline six specific recommendations in regard to PIPEDA, although three more are included in our submission. These recommendations are the result of consultation within our credit union system among representatives who have experience in the area of privacy protection, as well as with our national legislative affairs committee, which has representation from across Canada.

● (0920)

Mrs. Charlene Loui-Ying (General Counsel and Government Relations Officer, Credit Union Central of British Columbia): Turning to our first recommendation, Canadian Central believes the existing ombudsman model has been generally effective in protecting the privacy rights of individuals and garnering the compliance of organizations that are subject to privacy complaints. Thus, we recommend that the enforcement powers of the Privacy Commissioner not be enhanced at this time.

As you know, the Privacy Commissioner currently has the power to investigate complaints, conduct audits, make findings, issue recommendations, and initiate court actions. In particular, the current ability to publish names of offending organizations has been effective in inspiring compliance, as most organizations value their reputation. Once again, it is important to consider that Canada is only two years into the full application of PIPEDA and, as consumers and businesses increase their awareness of privacy issues, the effectiveness of legislation will also expand.

Recommendation 2: Canadian Central manages a credit union office for crime prevention and investigation, which is an investigative body designated under PIPEDA. Under PIPEDA organizations are allowed to disclose personal information to a designated investigative body without the knowledge or consent of individuals concerned. However, to do so, there must be reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province, or a foreign jurisdiction.

PIPEDA also permits investigative bodies to disclose personal information without the individual's knowledge or consent if the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province. Canadian Central is concerned, however, that the act does not define the term “investigation”, thus leaving some ambiguity in the legislation and requiring organizations to interpret the act on their own.

Canadian Central recommends that the legislation be amended to include a definition of “investigation” in the act, especially one that specifically addresses fraud prevention activities in the definition. This may be done by adopting the model found in the Personal Information Protection Act of British Columbia.

Recommendation 3: Canadian Central recommends that PIPEDA be amended to allow designated investigative bodies performing similar functions to share information with one another. For example, the Credit Union Office for Crime Prevention and Investigation should be able to readily share information with other designated investigative bodies, such as the Bank Crime Prevention and Investigation Office, for the purposes of fraud prevention.

Along with this, the current framework should be clarified to identify when and how information sharing should take place between investigative bodies. Specifically, what is an appropriate response to a request for information from another investigative body? This guidance may not be necessary through legislative or regulatory measures, but rather through the issuance of guidelines.

Recommendation 4: At the moment, PIPEDA does not contain provisions allowing an organization to disclose personal information to prospective purchasers or business partners without the consent of the individuals whose personal information forms part of the transaction. Canadian Central supports an amendment to PIPEDA's consent requirements to permit the disclosure of information in the event of a business purchase, merger, or mortgage securitization. Of course, such disclosures should only take place when there are stringent confidentiality agreements in place.

Furthermore, such agreements should include provisions to ensure that information is either returned or destroyed if a transaction is not completed unless laws otherwise require retention. This sort of amendment will have the dual impact of facilitating business transactions while further ensuring that the protection of personal information is specifically contemplated during these transactions.

Recommendation 5: The privacy community is debating whether a “duty to notify” should be included in PIPEDA. Such a duty would require that organizations suffering involuntary disclosures or security breaches or the outright theft of personal information mitigate the risk of identity theft to the individuals involved. Such mitigation after a security breach could involve notifying the individuals whose information is at stake, along with credit agencies, relevant government agencies, and other commercial entities such as financial institutions.

● (0925)

Canadian Central supports, in principle, the concept of a duty to notify. However, if the Government of Canada decides to legislate in this area, there must be reasonable thresholds established before such notification is required. For example, before a notification takes place, there should be a determination that there is a clear risk of fraud, that the loss or theft creates a reasonable likelihood that the personal information will be used to the detriment of the individual affected, or that the loss involves large numbers of records with similar concerns. Those thresholds should also consider if notification might either cause a greater risk of fraud or other harm or might unduly alarm individuals. Canadian Central would be pleased to participate in future consultations in determining such thresholds.

Turning to the final recommendation that I'll be highlighting this morning, in a 2005 decision the federal Privacy Commissioner concluded that under PIPEDA, business email addresses are considered an individual's personal information. In investigating the case, the Privacy Commissioner found that while the definition of personal information in PIPEDA excludes an employee's name, business title, address, and telephone number, business email addresses, because they are not mentioned, are personal information.

Canadian Central recommends that this anomaly be addressed by amending PIPEDA to mirror B.C. and Alberta legislation that specifically excludes business email from coverage under provincial law. There appears to be little purpose served if business telephone numbers are exempt from the legislation, but business email addresses are not.

In closing, I would like to thank the committee for this opportunity to present our views on PIPEDA. We would be happy to answer any questions the committee may have.

● (0930)

The Chair: Thank you very much.

I note that your presentation has nine recommendations, of which you discussed six, so there are still three that you want us to consider; I presume that in the interest of time, you highlighted the six that you thought were the most important for this morning, so thank you very much.

We'll begin our questioning. We'll start the seven-minute round with Mr. Peterson.

Hon. Jim Peterson (Willowdale, Lib.): Thank you for being here.

Are there any differences between the two groups?

Mr. Terry Campbell (Vice-President, Policy, Canadian Bankers Association): Mr. Peterson, I'll look to see what my friends in the credit union industry have to say, but I think we're very consistent. As we've gone through the two recommendations, I think the overall view is that the legislation works well. We think it's a good base. We think it's working well. I think we both need what I would call some “technical tweaks” to make it work better, work more efficiently, but I don't think we see the need.... For a piece of legislation that is so relatively new, quite frankly the track record, from our sense, shows that it operates quite effectively. The Privacy Commissioner's office operates quite effectively. I don't think we need much more than technical tweaks. That's our sense, but I'll defer to my friends at the Credit Union Central.

Mrs. Charlene Loui-Ying: I think we're generally of the same view. Perhaps we may vary in a couple of the nuances or in how far we think changes need to be made, but generally we're of the same view—that it's generally working well and only needs some technical tweaks.

Hon. Jim Peterson: In the case of identify theft, have your financial institutions ever penalized a customer whose identity has been stolen, or do you bear the loss as an institution? This is to both of you.

Mrs. Charlene Loui-Ying: It's circumstance-driven. There have been cases in which members have contributed to the loss, but even in some of those cases, the financial institution has reimbursed the members.

Hon. Jim Peterson: In what way did the members contribute?

Mrs. Charlene Loui-Ying: They gave their debit cards and PIN numbers to someone else, and that person took money out.

Mr. Terry Campbell: There are a number of provisions. I know my colleague Mr. Law will want to talk about this. You can look through different kinds of products—for instance, on credit cards there's a zero-liability policy out there: if somebody gets your identity and uses your card fraudulently, you, the customer, are held blameless. It's zero liability.

I'm very glad you raised identity theft, because it really is an issue. I'll ask Mr. Law to comment a bit further.

Mr. Warren Law: Just to underscore what Mr. Campbell has said, for many, many years we have been pressing the Government of Canada to do something about the problem of identity theft. It's a huge problem. It's growing, and unlike the United States, the Government of Canada has not acted on the problem with respect to addressing it in the Criminal Code. It's interesting when you look at the Criminal Code. There are provisions in the Criminal Code, for example, that deal with sending a telegram under a false name, but there's nothing to deal with e-mails. The fact of the matter is there's no provision in the Criminal Code that specifically addresses the identity theft problem in Canada, and I would urge the Government of Canada to look at this.

The Department of Justice has done at least a couple of consultations. They're inching towards the point where they may be proposing legislative changes to the Criminal Code. It is a significant problem. It's not enough simply to have the Criminal Code kick in when in fact a fraud has occurred. My view and the view of the Canadian Bankers Association is that the Criminal Code should get involved at the point where personal information has been misappropriated, because it's at that point where the trauma has been created for the individuals affected. It's at that point that losses do begin.

It's something that I think the Government of Canada should consider very seriously.

● (0935)

Hon. Jim Peterson: Are you saying that I could engage in identity theft and fraud with impunity until this amendment is made? It sounds very attractive.

Mr. Warren Law: Well, yes, and after your political life, Mr. Peterson, perhaps you might consider it.

The Criminal Code kicks in when in fact a fraud occurs, obviously. But what we're saying is that the Criminal Code should kick in much earlier in the continuum of criminal activity, at the point where in fact the bad guy has gone on the Internet and stolen personal information about you. I don't think we should wait for the point where a fraud has been committed; I think the Criminal Code should apply at the time the misappropriation has occurred.

Hon. Jim Peterson: Going back to my question, whenever there's a fraud, the client is kept whole. The client whose identity was stolen is not penalized. Is that the ongoing practice of all financial institutions in this country?

Mr. Terry Campbell: That's the basic principle; that is exactly the basic principle. Of course, what we try to do is to have systems in place that stop it before a fraud happens. We have systems that can detect unusual patterns, say, on your credit card; if there's a purchase in Toronto in the morning and a purchase in Bangkok in the afternoon, the system shuts that down. We try to stop it, but the principle you've articulated, sir, is exactly right.

Hon. Jim Peterson: On the latest spate of identify theft involving Winners et al, do you have any views on whether Winners and others handled these issues properly in terms of notification?

Mr. Terry Campbell: Well, it's very difficult to speak for another part of the economy.

You make a good point, in the sense that it's important to bear in mind that those breaches took place at retailers, but I think the point is, let's look at what has happened here. Nobody likes to see breaches, but when they do happen, you want to see that steps have been taken, that notification has happened, that the authorities were brought in and the Privacy Commissioner was dealt with, and that the VISA and Mastercard systems were immediately contacted. They're the principal entities working with the retailers in question. In turn, VISA and Mastercard will let the banks know they've been working with our customers.

But in that chain of events, there was notification, as the authorities and the Privacy Commissioner were contacted. Our sense, from publicly available information, is that the retailers are working closely with the commissioner. Our sense is that shows the system is working well.

Hon. Jim Peterson: Thank you very much.

The Chair: You said that your basic principle was that the customer is held “whole”, as Mr. Peterson put it. I presume you're talking about credit cards and not real estate.

There is currently a problem with people's identities being stolen and their homes being sold from under them, and I believe the bankers' position is that their mortgages are valid in that case. Is that not true?

Mr. Warren Law: I think you've got to look at it on a case-by-case basis. As you probably know, there was a case before the Ontario Court of Appeal that came to a conclusion. I also know that the court of appeal is just about to relook at that situation, but I think this very much underscores something that my colleague from the credit union said, that you have to look at it on a case-by-case basis.

The Chair: Thank you.

Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: I will give up my time to Mr. Vincent.

Mr. Robert Vincent: Thank you for being with us here today.

Did I hear you correctly earlier when you said that debit cards were the client's responsibility? Mr. Law, you said that credit cards were fully reimbursed, but that in the case of other cards, for instance debit cards, when a PIN number ends up in someone else's hands, that is the client's responsibility and that same type of reimbursement does not apply. Is that correct?

● (0940)

Mr. Terry Campbell: I'm sorry, but I must answer in English.

[*English*]

I mention credit cards as a particular instance. But no, if there's a problem with debit cards, if somebody has attained access to a card through identity theft or skimming, the customer is taken care of. The customer is made whole.

What we do make a point of—which I think the Credit Union Central people were saying—is that it's very important nowadays for individuals to take care of their debit card numbers. There are all sorts of cases where basically the bad guys either look over your shoulder or have a little camera on the PIN pad.

We recommend strongly that when you use your cards, you do so carefully. You make sure that it's covered. You make sure that there is no obvious tampering on the machine.

We say, do not share your number with people. It's amazing to have to say this, but it's still true sometimes. Don't share your card and don't share your number, even with somebody you know, because these cards get around. Don't write the number on the back of the card; don't have a little slip of paper in your wallet.

If in fact you have contributed to it, that's a different issue.

I mention credit cards, but we take care of the debit card problems as well.

Perhaps my colleagues at Credit Union Central will want to add to this.

Mrs. Charlene Loui-Ying: I would add that Credit Union Central, and I believe the bankers, have endorsed the debit card code of practice that requires the financial institution to reimburse in the event of a fraud, unless the debit card user has contributed to the loss.

There are some time limits on how the decision-making occurs, but the general premise is that the member should not have to suffer for fraud.

[*Translation*]

Mr. Robert Vincent: My question was as follows: if a sum of money is stolen from someone's bank account, does that person receive a total reimbursement?

In the case of a stolen debit card, what kind of investigation do your institutions carry out? Can the person be reimbursed quite quickly or does the investigation drag on so that the victim of the theft is only reimbursed months later? What measures do you take to protect people and their bank accounts from wrongdoing?

[*English*]

Mrs. Linda Routledge (Director, Consumer Affairs, Canadian Bankers Association): There is a process in every institution, so that if you go into a branch, it's generally escalated to a central adjudication centre, where it's handled very quickly. There are limits in the debit card code. They have ten days for the investigation to proceed, and then they'll get back to the person.

There may be some additional investigation afterwards, if it's a complex situation, but they try to resolve it very quickly. That's the commitment in the debit card code.

[*Translation*]

Mr. Robert Vincent: According to the information provided to us by the Office of the Privacy Commissioner, a large number of the complaints received by that organization regarding PIPEDA involve financial institutions. Can you explain why there are so many privacy complaints in this sector, especially if you consider that banks were among the first organizations to be subject to the legislation?

[*English*]

Mr. Terry Campbell: Let's put this in context. Warren mentioned in his opening remarks that we have 11 million transactions a day. That's hundreds of millions of transactions a month, billions a year. We're aiming for perfection, but we're all people. Mistakes will occur, but they occur very rarely.

Sir, if you look at the actual statistics coming out of the Privacy Commissioner, out of the literally billions of transactions a year, there were about 133 complaints against the banks. I think we have the statistics here. It's a very small number. I believe that when the Assistant Privacy Commissioner was before this committee some time ago, she said yes, the banks have the greater number, but it's largely because they're one of the biggest institutions. In the actual scheme of things, relatively, it's a very small number.

I think the reason for that is.... We take privacy very seriously because in effect it's the core of our business. We'd like that number at zero, but we're dealing with people and sometimes there are human mistakes. I think that's the sense of it.

● (0945)

[*Translation*]

Mr. Robert Vincent: How much time do we have left?

The Chair: You have 30 seconds.

[*English*]

Mr. Tilson, followed by Mr. Dhaliwal.

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

I'd like to ask a question. An issue was raised about Winners. The tone of my questions, I want you to understand, is about whether committees are trying to review this legislation, trying to improve it. To Mr. Campbell in particular, we're not out to attack any bank or Winners or anyone else. Incidents have happened and they're all relevant to all of these topics, whether it's the outsourcing information, notification, or the investigation issue. All of these issues are tied in. With respect to my questions and others, I don't want you to get the wrong interpretation.

On the issue of notification, both the Credit Union Central of Canada and the Bankers Association say pretty much the same thing. The credit union people say that there must be a clear risk of fraud for notification. The bankers, to use your word, whether it's “tweaking” or not, say similar matters. I guess we'll let the lawyers decide.

Is there a reasonable risk that their personal information could be used for fraudulent purposes or identity theft? Well, the problem is if you look at these news stories that have just recently come out with a story by Emily Mathieu in the *National Post* about HomeSense and Winners, talking about "significantly less than millions of holders" information was removed from company databases and the CBC story on the CIBC losing almost half a million Talvest fund customers, in which case client names, addresses, signatures, dates of birth, bank account numbers, beneficiary information, and/or social insurance numbers....

I'm looking at all that stuff that's been stolen, and you guys are saying that unless there are signs of fraudulent activity, you don't think you should notify. My God, if someone had my name, signature, date of birth, bank account number, beneficiary information, and social insurance number, I'd want to be told. I'd want to be notified. I don't want any sign of fraudulent activity. I want to be told.

Mr. Warren Law: I have no problems with that.

Mr. David Tilson: But that isn't what your report said.

Mr. Warren Law: Sure it is. Banks take very seriously the privacy of their clients. For example, in the Talvest situation, sure, there was a clear risk, a reasonable risk, that the information could be used for fraud or identity theft, and the bank acted responsibly.

Mrs. Linda Routledge: And the bank notified all its customers. Mr. Wallace can attest to that.

Mr. David Tilson: That's why I introduced my comments saying this is not necessarily an attack on anyone. I'm looking at the policy that you're recommending to the Privacy Commissioner—to notify only if there's a risk of fraudulent activity. Doesn't the release of any information allow for the possibility of identity theft or fraudulent activity? The police tell me that if a credit card is stolen, nothing may happen for a year.

Mr. Terry Campbell: I take your point. This is very sensitive stuff, and it absolutely is the case that notification has to happen. We firmly believe that.

We had two points. First of all, however you set the threshold, you have to set that threshold in a way that you are going to avoid two problems. You don't want to have every minuscule or potential breach resulting in issuing notices, because what will happen then is people will be inundated with things and they'll stop paying attention. They'll get inured to it and it will be just a regular routine kind of thing. That's the first thing you want to avoid. What you want to do is have a notice, where in consultation with the Privacy Commissioner, your own privacy experts, and with the police, people say you need to have a notice here.

The second thing you want to avoid is scaring people. There have been cases in the United States, at the state level, where there are these automatic breaches at a whiff of a problem. People get really upset. There was a veterans affairs issue there, where an automatic statutory breach notification went out and people got terribly upset. At it turned out, when people looked at it, there was really nothing going on there.

This is what you have to do when these things happen. There's an incident, but what is it? Is it a breach? How did it happen? Has personal information been accessed? These are just questions, but it's hard to determine. If accessed, is there evidence that they have been used or decoded? You have to get to the bottom of that first. Once you get to the bottom of that, everybody around this table would say oh, absolutely. Of course when you have these suspicions, you go right to the police and the Privacy Commissioner and you work with them.

The main point we're making is that we take notification really seriously. The evidence is that we in fact notify. Our point is that the current voluntary system is working well, as is the evidence, I think. It gives you flexibility. Then you can work with the commissioner on the facts of the case rather than having it hard-wired and at the whiff of something you get something kicking in. It's flexible. It works.

Let me just conclude this part of my comments by saying we agree with what you're saying. We very much agree. What we want to avoid is an inappropriate notification system. We want to signal our sense that the evidence out there suggests it is working well.

● (0950)

Mr. David Tilson: I'd like to move on to another question, if I have time.

I'm just going to tell you that I've had it happen to me personally, on two occasions, with a credit card company, which of course is tied in with the bank. They have notified me that someone may be using my card information inappropriately. I have appreciated that. I have been concerned, yes, but I want to be notified.

My question is for Ms. Loui-Ying, and anyone else who is a lawyer. She's the only one who is admitting she is a lawyer.

The question has to do with outsourcing. I find this business of people in India and China, whether it's telemarketing...an unbelievable thing. They're being trained. They call somebody in Texas, and some Indian is being trained to talk with a Texas accent. It's unbelievable. Massive information is being outsourced. I'm told accountants outsource their information to people in India to do income tax returns in our country. It is mind-boggling.

My question has to do with the comment—I believe it was Mr. Law's—on the issue of contravention of foreign law. That's an interesting topic. I gather you're saying there is a difficulty on that issue.

Mr. Warren Law: It's a problem with the investigative bodies.

Mr. David Tilson: Are there other areas we should be looking at? I'm thinking, for example, of the issue of reciprocal agreements with foreign jurisdictions such as we do in other areas of the law on enforcing. Our laws could be different from laws in India or the United Kingdom or any other country.

The Chair: Mr. Tilson, I've allowed you a lot of leeway. You asked the question.

Mr. David Tilson: Well, think about that, and we'll come back to it.

The Chair: Mr. Tilson asked the question. I believe it was to Mrs. Loui-Ying and any other lawyers.

Mrs. Charlene Loui-Ying: The issue of outsourcing is actually one of the matters that we did not address or highlight in the presentation this morning. Canadian Central does have a position on outsourcing. Recognizing that, for the most part, outsourcing is a business reality, as pointed out by our colleagues, credit unions generally don't have the size and scope for the same bargaining power in outsourcing agreements that other larger organizations, particularly federally regulated organizations, might have. That said, there has been discussion among members of Canadian Central about the need to share information with other jurisdictions. The general feeling at this point is that the mechanisms already in place are appropriate, so that perhaps the Privacy Commissioner does not need a direct mechanism, as might have been contemplated in some of her submissions, since there are other mechanisms in place for information sharing at that level.

● (0955)

The Chair: Ms. Routledge had her hand up.

Mrs. Linda Routledge: Sorry, Mr. Law.

On the issue of outsourcing, the banks have the obligation under PIPEDA to protect the information they collect. So when they outsource, their outsourcers are agents, and they will have contracts in place with those agents to make sure that those agents offer the same protection as the banks would offer if they were holding the information and doing the job themselves.

The Chair: Did you want to add anything?

Mr. Warren Law: The only thing I can add to that is the fact that you have a specific guideline, the OSFI guideline, that deals with outsourcing on the part of the banks, and it provides another controlling mechanism regarding the extent to which information can be outsourced.

The Chair: Thank you.

Both Mr. Peterson and Mr. Tilson raised more or less the same point, that you seem to be more or less in agreement on things. I don't know if it's just me, but I detect a nuanced difference in your approach to what one calls breach notification and the other one calls duty to notify.

The banks say they do not believe that legislative requirements are needed, period, full stop, end of story. The credit unions support in principle the concept of duty to notify, but if the Government of Canada decides to legislate, there should be a reasonable threshold. That's not quite the same as saying there should be no legislative requirements. Am I right in that interpretation? Yes? Okay, thank you.

Mr. Dhaliwal.

Mr. Sukh Dhaliwal (Newton—North Delta, Lib.): Thank you, Mr. Chair.

Thank you to the panel that came out today.

When I look at the corporate groups, they are already defined under the Income Tax Act. How is your definition any different from what falls under the Income Tax Act when it comes to corporate groups?

Mr. Warren Law: I don't think we've gone down to that level of detail, but I think it would probably be the same affiliates and subsidiaries. The fact of the matter is—and this is a point I made in my opening remarks—that banks, as do a lot of corporations, operate as a corporate group now. Within a banking group you have a mutual fund dealer, a trust company perhaps, a securities dealer, and a bunch of companies carrying on different kinds of businesses, but for all intents and purposes they operate as one group. I think, as a result, it would be useful if you could share information among the particular companies within that group in an effort to prevent fraud.

I know of situations that have happened in the banking industry, for example, in which our BCPIO, our investigative body, has been seized of information concerning fraudulent activity, money-laundering activity, but it has been unable to share that information with a subsidiary of one of our member banks because of the fact that PIPEDA does not operate on a corporate groups approach. As a result, I think it would certainly be beneficial for this committee to consider making amendments to the act to allow corporate groups to share information among the members of their group.

Mr. Gary Rogers: Specifically to your question about the Income Tax Act definition, it probably doesn't work well enough in this instance. In the credit union system we have a large number of players with very small shareholder interests, so therefore the concept of associated corporations and related corporations in the Income Tax Act wouldn't be broad enough to cover what would be intended here for privacy purposes. We're interested in having a conversation about how that could be defined appropriately.

● (1000)

Mr. Sukh Dhaliwal: The question is, on the one hand we are saying that we should be carefully considering the modifications to PIPEDA, and on the other hand, we are saying that it's only a two-year-old act and we should not touch it. Why would you have a conflicting statement in your own proceedings?

Mrs. Charlene Loui-Ying: I'm not sure it's so much of a conflict, but saying we recognize some tweaking is needed, to use the word of the day. It's not so much an overhaul, but we need to look at changing the whole way privacy operates in Canada. Because of the statutory review, it is useful to take a look and say what's been going on in other jurisdictions and what's been working well. Are there things that can help improve this legislation for the benefit of all Canadians to make it work more effectively so it's more cost-efficient for business and more effective for consumers as well? I'm not sure we meant it to be a conflict, but more part of the continuum.

Mr. Sukh Dhaliwal: With technologies changing every second, do you still think there should be no changes made to cover the technology we have today, rather than what we had two years ago in the banking industry?

Mrs. Charlene Loui-Ying: Because this has a lot of general application, I'm not sure it speaks specifically to any particular technology. You're speaking to personal information here and what you're talking about is the scope of personal information.

Mr. Sukh Dhaliwal: On identity theft, when it comes to all those issues, in outsourcing you said there are issues with identity theft as well as going from one country to the other. We didn't have outsourcing two years ago or ten years ago to the extent we have it today. Depending on that country's law, I don't feel very comfortable when it comes to outsourcing and saying we should have the laws from two years ago.

Mrs. Charlene Loui-Ying: If you look at the provisions of the act, it would apply generally to whether the manner of outsourcing worked five years ago or today. As my colleague has pointed out, the law says you are responsible for that personal information. When you outsource or use agents, you have to have them agree to protect it the same way you have to protect it.

I'm not sure it's the delivery method, with the exception of business e-mail addresses, where perhaps e-mail was less trusted five years ago than it is perhaps in the business community today. I'm not sure there are significant changes that aren't captured by the existing wording. If you examine that, you might come to the conclusion that the existing wording does deal with some of these changes and might have been worded generally enough to accommodate future changes in technology or relationships.

Mr. Sukh Dhaliwal: Thank you, Mr. Chair.

The Chair: Thank you.

Mr. Wallace, followed by Madame Lavallée.

Mr. Mike Wallace (Burlington, CPC): Thank you, Mr. Chairman.

Thank you for coming this morning.

I have four questions for you, and I don't think it will take too long.

I've spoken to other groups about the fact that there are privacy PIPEDA-type acts both in Quebec and British Columbia. Since you're a national organization, how is that treated, and which one takes precedence over the other in each? Does the B.C. law take precedence over the federal? How does that work from a practical point of view from the main perspective?

Mrs. Linda Routledge: PIPEDA applies to federal works and undertakings across the country. If it's a bank, telecom, or transportation company, PIPEDA applies wherever you are. The provincial legislation does not apply. In B.C., Alberta, and Quebec, for provincially regulated organizations, those acts apply, and PIPEDA does not apply. In provinces where there is no provincial legislation, PIPEDA applies to the commercial operations of organizations. Nothing covers not-for-profits and so on.

● (1005)

Mr. Mike Wallace: Thank you.

Charlene, any comment?

Mrs. Charlene Loui-Ying: Thank you for highlighting another one of our submissions that we did not have an opportunity to highlight this morning.

You'll note in our submission that we've actually raised this as an area that perhaps could use a little bit of work, because the way the order in council was drafted it refers to specific activities as opposed to an organization. So an organization in British Columbia that is carrying on activities in British Columbia, as a B.C. credit union would do, is subject to the B.C. privacy legislation and would fall outside the scope of PIPEDA.

The B.C. legislation does say that if something falls under the scope of the federal legislation the B.C. legislation does not apply, so you're not going to have the same legislation apply in the same circumstance. But what's less clear because of the way the order in council was drafted was that the two different pieces of legislation could apply to the same organization in different circumstances.

Mr. Mike Wallace: I appreciate that, because one of my views of the world is that we try to make things simple and the less overlap the better.

The one area you have a lot to do with, probably mainly from the banks but I think also from the credit unions' point of view, is business information when businesses are sold and people are investigating whether there's an interest in making a purchase or a sale and so on. Could you give me a layman's view of what actually happens, without taking too long? And how does PIPEDA help or hurt that, and what do we need to do to make that easier?

Mr. Warren Law: Why don't I take a stab. I'm a lawyer, so I've been a through a few of these transactions in prior lives.

We have a simple deal to sell a company. We'll have business from company A to company B. Company B is interested in the assets that it's purchasing. The assets may include the employees of the business that it's purchasing. The problem under PIPEDA right now is that information concerning the name of the employee, address, etc., could be construed as personal information and therefore it would be difficult without the knowledge and consent of the particular employee to give that pertinent information to the prospective vendor of the company.

It's an asset that the purchaser is considering purchasing, but it's difficult to go through the due diligence process if you don't have that information. But because of the constraints in PIPEDA you can't give information with respect to employees.

Mr. Mike Wallace: Do you have a specific recommendation on how the wording would change to allow that to be made simpler?

Mr. Warren Law: I think it's been done in Alberta and B.C.

Mr. Terry Campbell: In fact what we do now.... Obviously, PIPEDA applies, and we rely upon the implied consent provisions in the legislation. What we're suggesting is it would be more useful for greater clarity and certainty.... Is it Alberta or is it British Columbia that is the suggestion we have?

Mrs. Linda Routledge: Alberta.

Mr. Terry Campbell: Section 22 of the Alberta provision we think is very specific. It happens now. We can work it under PIPEDA, but our sense is that for greater certainty and for clarity, section 22 in Alberta would be a useful one.

Mr. Mike Wallace: Any concurrence at the end there?

Mrs. Charlene Loui-Ying: Sure. I can reference section 20 of the B.C. act if you wanted the cross-reference.

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

My third question is a quick one. The Privacy Commissioner.... As I mentioned earlier, I got a letter that some of my information has gone missing from a mutual fund. The newspaper portrayed it as if it weren't for the Privacy Commissioner pushing them to notify and to make it public, it would not have happened. Do you agree with that approach?

Mr. Terry Campbell: Let's go right back to what I was saying earlier. When there is a breach or an incident—let's call it an incident, you don't know if it's a breach yet—you don't know what the "it" is, and when you notify the police and the Privacy Commissioner, you have to do a fair amount of work to really get to the bottom of it before you know what has to be done. That involves a lot of back and forth. We rely upon the Privacy Commissioner. We have a very high regard for that office and for the Privacy Commissioner herself. We take not just their input, their guidance, but we also take their direction.

In the particular case you're talking about, there is an investigation going on, so until the investigation is done, it's hard to say either way. But I can tell you that generally you have to go through that process, because the facts of the case, every case, are going to be different. There are different ways you can notify. You can notify individuals directly through.... You can issue a press release, take out an ad in the paper. What's the appropriate way? There is no one template. There is an investigation going on in that particular case, but I can tell you one of the values of having the current system that we have—and we think it works—is it gives you the flexibility to determine the right course of action, quite frankly, in dialogue with the Privacy Commissioner. You can tailor it and you go from there.

● (1010)

Mrs. Linda Routledge: It could be that the Privacy Commissioner suggested one type of notification and the bank thought another type of notification might have been more appropriate. Sometimes there is a different point of view.

The Chair: Mr. Wallace, your time is up. Could you put your fourth question—just put it?

Mr. Mike Wallace: The question was this. You mentioned that if somebody has unusual activity on their account, particularly a senior, it's a simple question. Is it in the Bank Act that you are required to notify, or is that just a customer service approach that you were taking?

Mr. Terry Campbell: There was actually a common law decision that said you can—

Mr. Warren Law: The Tournier case.

Mr. Terry Campbell: Yes, the Tournier case, in which it said you had the ability to take those steps. With PIPEDA coming in with the stricter sets of rules, it hemmed that in. So we're suggesting there should be an amendment that goes back to that common law standard.

Mr. Warren Law: Confidentiality has always been a part of banking, and the common law itself recognized that. The Tournier case was decided early in the 20th century and said yes, confidentiality is the hallmark of banking. There are certain very limited exceptions at common law where a bank is entitled to release information without consent, one of which is for public interest situations.

The Chair: Thank you.

Madame Lavallée, followed by Mr. Stanton.

[*Translation*]

Mrs. Carole Lavallée: Thank you very much, Mr. Chairman.

These ladies and gentlemen made an excellent presentation. They said that the changes they were proposing were of a technical nature and that overall they agreed with the legislation itself. Then they commented on the technical changes they were proposing. Their presentations were extremely interesting and their documents were excellent.

I'd like to give up my turn because we need to reserve a bit of time to discuss the Access to Information Act. I think that the Conservative members opposite will try to use all the time they will have left until the end, and by doing that, they'll have to force themselves to find more questions to ask and they will waste everybody's time, including the time of our distinguished guests.

Thank you, Mr. Chairman, but I'll give up my turn.

[*English*]

The Chair: Madame Lavallée never gives up, does she?

Okay, good for you.

Mr. Stanton, can you rag the puck?

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chairman.

Very briefly, Mr. Chairman, I have just a couple of questions.

I noticed through the course of our question and answer that some of this has already been brought up, but my central question is this. Both of your organizations have had the experience now of operating where there are provinces that have their own privacy legislation in place, in the three provinces that apply to at least your sector and also the federal government. I would have to believe that for the purposes of reviewing PIPEDA there are some lessons to be learned, both pro and con, in the provincial examples. There have been a couple of examples noted already: the question of business e-mail being a positive change; the definition of "investigation"; and then the last one that was identified through your discussions with Mr. Wallace, this overlap between activities versus organization.

Is there anything else that we should know? Are there any other lessons that we should be understanding to take forward from the provincial example that should be something we should consider for PIPEDA? What has worked extremely well that we should consider incorporating into any amendments for our consideration?

● (1015)

Mrs. Linda Routledge: In our submission, there are a number of small suggestions that we haven't highlighted in our speaking notes and so on. They include things like the correction of professional and expert opinions.

Say there's a mortgage appraisal. Someone coming into a bank and asking for access to information may disagree with the value placed on their house. That's our appraiser's professional opinion and the person should not be able to correct it under PIPEDA, so the provincial legislation has dealt with that.

On collection of information in an individual's interest, the example we use in our submission is that I want to send my mother some flowers. Well, the florist has to get my mom's name and address for me to be able to send the flowers to her. Technically, that's a contravention of PIPEDA. There are a few little things like that.

Another one is found where access might preclude collection. In the employment context or in a whistle-blowing context, collecting that information and having someone have access to that might stop someone from whistle-blowing. There are a few things like that too.

The Chair: Anyone from Canada Central?

Mrs. Charlene Loui-Ying: Our submission does highlight those issues, because we did try to take into account the lessons learned in preparing the submission. I would simply add to the issues you've already noted.

The fraud prevention issue does continue to be one of the biggest concerns in the industry. If you were looking at the lessons learned, I would say the B.C. model of fraud prevention would be one we would commend you to examine.

Mr. Terry Campbell: We would agree with that. I think that's a particularly important one from the provincial side. The B.C. model would be very good.

Mr. Warren Law: I think another constraint was mentioned earlier, but just to underscore it, the fact is that our investigative body cannot talk to their investigative body. That's silly because of the fact that the bad guys are attacking the banks, credit unions, and every other financial institution out there. Why in heaven's name we can't share information just makes no sense.

Mr. Bruce Stanton: Would it be fair to say that one of the objectives here would be to try to get some harmonization—

Mr. Terry Campbell: Absolutely.

Mr. Bruce Stanton: —as a general intent or objective coming out of this process?

Mr. Warren Law: Yes, harmonization, while remembering that the system as it is now works very well, by and large.

Mr. Bruce Stanton: Finally, just as one more point, on the point that you raise with respect to the public interest exemption, could you give us just an anecdotal example of that again? I take the case. It's well put here. But just give us a common sense example of how that would play out in a banking situation.

Mrs. Linda Routledge: It could be a senior who walks into the bank and wants to withdraw $30,000. Clearly this is atypical of this person. There may be a caregiver with them. In many cases, the caregiver is influencing the person and is going to walk away with the $30,000.

Mr. Bruce Stanton: So it's a suspicious circumstance, and this would be the employee in the bank who would be alerted to that kind of thing.

Mrs. Linda Routledge: Sure. A senior comes into the branch. The employees often will know this senior. They know what is typical behaviour for them in terms of banking transactions. If it's unusual, they'd really like to be able to call up another member of the family and say, “Is it okay for your mom to be doing this?”

Mr. Bruce Stanton: That's the part I didn't get. What can be changed, then, to allow what you're looking for here, that being a means that currently PIPEDA blocks you from doing? Is that my understanding?

Mrs. Linda Routledge: That's correct. Some of the provincial legislation—I can't remember offhand whether it's Alberta's or B.C.'s—does allow for disclosure of interest information when the law allows. If we even had “the law allows” in our common law, our ability to disclose when in the public interest could kick in.

Mr. Bruce Stanton: You don't need to answer this right now, but perhaps for the purposes of our deliberations here in order to come at the question of how one would go about defining that circumstance—because obviously you would have to be able to put some scope on that—what would be the triggers to allow that public interest exemption to be executed?

Mr. Warren Law: I was thinking about that coming up. You should take comfort about the fact that in many statutes, this test is used. For example, securities commissions can get involved in a situation and make an order if it's in the public interest. It's not defined, but it hasn't caused them any problems. And there are a lot of statutes at the federal level as well that use the undefined public interest test very well.

● (1020)

Mr. Terry Campbell: But we will take your advice. We'll follow up with the committee on that.

Mr. Bruce Stanton: I appreciate that.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Stanton.

Mr. Peterson, followed by Mr. Tilson.

Hon. Jim Peterson: Yesterday in the House of Commons it was suggested that fees for ATMs should be abolished. Can I assume that the Credit Union Central and the CBA would support that provision?

Mr. Terry Campbell: No.

There will be other venues to talk about that, but on that particular one, Canadians have access to their own money and their own.... If you have money in Scotiabank, you can use that Scotiabank machine without those extra charges.

We have a user pay system. It's transparent. If you want to use another bank, you have access to your money, but you are not the customer. That's not where your money is. You're provided with a choice. And I think the statistics show that most people are very savvy in how they go about business. You'll see the statistics rising where people say, “Well, I'm going to use my own machine because it just makes sense”. And that's the process.

We could go on at some length, Mr. Peterson, as you know. So there you go.

Hon. Jim Peterson: We'll enshrine that in PIPEDA.

Mr. Terry Campbell: Right.

The Chair: Anything else, Jim?

Hon. Jim Peterson: No.

The Chair: Mr. Tilson.

Mr. David Tilson: Thank you, Mr. Chairman.

I'd like to return to the question of notification.

I do find interesting your observations about the sharing of information, that the banks, the credit people, and I suppose the police should be allowed to share information. And I gather you're saying "without consent". You're all saying—

Mr. Warren Law: Yes, these are all "without consent" situations.

Mr. David Tilson: —without consent of the individuals. Notwithstanding, you're not going to tell the individual. Right?

Mr. Terry Campbell: On investigation—

Mr. David Tilson: I'm returning to my debate with you, quite frankly—and I suppose it is a debate—that if someone has a whole bunch of information that somehow disappears and we don't know where it is, maybe it's just lost or maybe it's been stolen, both organizations are saying that unless there are signs of fraud or reasonable possibilities of fraud, they don't need to be notified. Notwithstanding, you think it's okay to notify the police and other banks and other credit unions.

Mr. Terry Campbell: I think the difference is this—and I would characterize it as a discussion and not a debate—

Mr. David Tilson: Ah, indeed.

Mr. Terry Campbell: Yes, there you go.

I would characterize it like this—and I don't want to get too hung up here. In our remarks to you and in our submission, we have suggested some criteria for renotification, but we're not suggesting a hard bright line, because you have to look at every case. Is it serious fraud, or is it a bit of fraud?

We're just saying you can't hard-wire that. You have to look at the facts. And that's where the dialogue with the commission is important.

The difference here with what Warren is talking about is if person X is the bad guy and we're doing an investigation on person X, and we need to dig into some data to find out about person X because he's breached an agreement or he's kiting cheques or he's involved in money laundering, we don't want to tell him. But if you've had your personal information violated or breached, by golly, we're going to tell you. That's the difference.

Mr. Warren Law: Yes, there are two completely different situations.

Mrs. Linda Routledge: And what we're looking for as well is for the act to define "investigation", and to define it in a very narrow way.

What we're suggesting is allowing investigations related to a breach of an agreement, contravention of a law, prevention of fraud, or circumstance or conduct that may result in remedy or relief being available under an enactment, under the common law, or in equity. That's from the B.C. legislation. So it's very specific that this is what we want to be able to share the information more broadly for.

Mr. David Tilson: The Privacy Commissioner goes even further and says that information should be shared with credit bureaus. Do you have any comment on that, on whether that's a good thing?

Is my credit rating going to be damaged if someone—

● (1025)

Mrs. Linda Routledge: Usually what we suggest is that we go to the customer and we give the customer the information to be able to go to the credit bureau, so then the customer is in control of their own information.

Mr. David Tilson: Yes, the Privacy Commissioner.... Parliamentary information research, which is always excellent, gave us something here. One of their points is that the Privacy Commissioner has noted an addition to adding a duty to notify, or as an alternative, a provision could be added to PIPEDA that would allow for an organization that has suffered a security breach to notify credit bureaus about the breach without the consent of the individuals affected. That's her recommendation.

The rationale is that it would allow credit bureaus to be more proactive in protecting consumers from identify theft and fraud. Having heard that, do you have any observations about it?

Mrs. Linda Routledge: If there's a large breach and a number of customers are affected, the bank may go to the credit bureau and say that there has been a breach and you will be getting calls from customers, but the banks prefer to deal directly with the customer and have the customer notify the credit bureau.

Mr. David Tilson: I'd like to turn to the topic of blanket consent clauses. Again, this issue of the possibility that privacy consent clauses are too broad has been raised by the research people. Do you have any observation on that?

Mr. Terry Campbell: We look at the consents pretty carefully and take them pretty seriously. Our view—and I think it's been confirmed—is that the consents the banks use are consistent with PIPEDA.

I think the standard you want to have is this: the customer should have a pretty clear idea of how the consent is going to be used—so that, for instance, if we say when you open this account that we'll be sharing your information with our trust company and investment subsidiary, it should be clear enough that you should not be surprised if in turn you are contacted by the investment subsidiary.

The standard you want to meet is a balance: you don't want to have it so spare that nobody really knows what's happening, but at the same time you don't want to have it so long and so detailed that in effect either the customers won't read it or they'll be irritated by it. It's got to have that balance. We think we've struck that balance. I wouldn't characterize what we see in our industry as blanket; it's actually very specific, but we have tried to strike that balance so that nobody's surprised.

Perhaps my colleague with Credit Union Central can talk about that too.

Mrs. Charlene Loui-Ying: We would support their suggestion that there does have to be a balance, because the reality is that consumers aren't interested in another piece of paper or even business transactions. They like to do things very quickly, so if they needed to get another separate consent for a similar type of re-advance on their mortgage, they would see the process as being more bureaucratic than helpful if they weren't able to give a continuing consent for all the advances on a mortgage at the time the mortgage was originally entered into.

The test really should be whether it's informed consent from a public policy perspective, I would suggest, because if the individual knows what he or she is consenting to, then it isn't the form of the consent that matters so much, but the substance, so if there's informed consent and the blanket consent provides for the necessary information, then it is still in the best interest of the consumer.

The Chair: Thank you, Mr. Tilson.

I have two names left, mine and Mr. Van Kesteren's. If anybody else wants to ask a question, please put your hand up.

I have one question and I'll ask it of credit unions. It is on the issue of notification. Apparently the Ontario and the B.C. privacy commissioners have released a breach notification assessment tool as a guide for public and private sector organizations in responding to a breach. A direct notification is the preferred method in the guide whenever the identities of the individuals are known and current contact information is available.

Do you know about this breach notification assessment tool? If you do, do you agree with it, and would you recommend it to PIPEDA?

● (1030)

Mrs. Charlene Loui-Ying: I apologize for not having looked that up specifically, so I can't speak to it specifically.

The Chair: Okay.

Go ahead, Mr. Rogers.

Mr. Gary Rogers: I'm in the same boat. I don't have knowledge of that.

Mr. Terry Campbell: What we would say is we are aware of those. In effect, they are guidelines, and we have said a guideline approach is actually a very useful approach, because it works with flexibility and is the non-mandated approach that we talked about. We all want guidance on how best to do it, and if the commissioner can come out with suggestions and guidelines, they would be very useful for us to consider—so, yes, we think that's a useful approach, and quite frankly, sir, from our perspective it's better than hard-wiring it into the legislation.

The Chair: Thank you.

Mr. Van Kesteren.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Yes, very quickly.

Of course PIPEDA came about in our new age of technology and information. When I listen to you, I get the impression—and I'm not trying to flatter you—that for banks, it's really in their self-interest to do these things. I look at self-regulated industries, such as the insurance industry.

In my former business life I was a car dealer, and I know that OMVIC was created after Consumer Affairs ceased regulating the auto industry. Quite frankly, they're much more stringent than Consumer Affairs was.

I'm teeing up for a shot here.

Some hon. members: Oh, oh!

Mr. Van Kesteren: Do you feel that if the banks were also given the opportunity, regarding some of the present PIPEDA rules hindering you and the customer, you would be in a better position to present—and of course this would have to work in conjunction—something that would be more tailored to the banking industry?

Mr. Terry Campbell: My colleagues might wish to jump in, but I would say two things in response.

Your introductory comments are absolutely right. It is in our self-interest to do the best job we can. Without the trust that we're keeping personal information as secure as possible, banking just doesn't work. The flip side of this involves reputational issues. It is in our interest to do everything we can to work with the commissioner, because nobody wants reputation problems. In a functioning marketplace, there are lots of people playing and reputation is important. We want to keep that working for our self-interest. That's the first point.

I would still say that PIPEDA is working pretty well, with one exception that I would flag. I think my colleague and our colleagues at the Credit Union Central would agree that where it isn't working as well as it could, where it's interfering with ultimately effective consumer protection, is on the investigation side.

You do the investigations to stop the bad guys, so that the consumers don't suffer. It works fine, but it could work better in terms of fixing up those investigations...the use disclosure issues. We suggested the B.C. model as a way to do it. That would be the one area I would focus on, sir.

Mr. Warren Law: To underscore the point about investigations, developing this concept of an investigative body was a good first step in PIPEDA in 2001. But in my mind, it was a bit artificial, and the whole process of investigating and preventing fraud could be streamlined much more if you took the B.C. approach. It would provide for better opportunities to fight the good fight against the bad guy.

Mr. Dave Van Kesteren: Do you have a comment?

Mrs. Charlene Loui-Ying: As the bankers have noted, the credit union system has always been concerned about privacy, because as you've pointed out, it is in our self-interest.

The legislation was not so much a shock in substance to the system, because there was always the banker's duty of confidentiality that also applied to the credit union system. So it's not about tailoring the form of the legislation. Given that we're two years into the implementation, and some of the difficulties that may have occurred through learning the new legislation have been smoothed out, I'm not sure that a radical overhaul would be the way to go.

● (1035)

The Chair: Thank you.

Mr. Bruce Stanton: Mr. Chair, could I ask a statistical question?

The Chair: Please.

Mr. Bruce Stanton: Very briefly. What percentage of your 11 million transactions per day are web-based in this day and age? In other words, do you have a number or any idea of one?

Mr. Terry Campbell: That's a very good question. There's no question that when we follow up—as earlier we said we would—we could send you some information. I don't have an actual number, but I can show you a chart, where paper transactions are going up like this and flatlining.

Electronic transactions are literally taking off like a rocket, and that line was crossed in the late 1990s. We've never looked back, and that's all electronic transactions, including those by phone.

We'll send it to you.

Mr. Bruce Stanton: I appreciate that.

Thank you very much, Mr. Chair.

The Chair: Ladies and gentlemen, thank you very much for your presentations and answers. It was very interesting commentary. We'll do our best to do what we can to make the act better. Thanks a lot.

Colleagues, we have three new members, so in the interest of time, allow me to summarize briefly the issue that Madame Lavallée raised in the morning.

In our first report of this committee, we reported to Parliament, calling upon the Minister of Justice to present a new or draft—however you want to characterize it—access to information law for consideration by this committee. We asked the minister to do this by December 15, and that did not happen, nor did we receive any correspondence from the Minister of Justice in regard to why that didn't happen.

In the interim, over the break, a new Minister of Justice was appointed. In her motion, Madame Lavallée asked the committee to give guidance to the chair—I'll put it this way—so the chair could write to the Minister of Justice—that's all—on behalf of the committee, inquiring about what was going on from the minister's point of view in response to our first report.

We talked out the clock on that simple issue, twice, and we're back at it again. I believe what Madame Lavallée is asking for, and no more, is that the committee instruct the chair to write to the new Minister of Justice to inquire about what the Minster of Justice's position is in respect of our first report, or words to that effect. That's, in a nutshell, where we are, and I give the floor to Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: That is in fact what I was asking for last fall, when the situation was not complicated. It would have been very simple to pass such a motion. You would have written a letter, and so forth.

That being said, a new factor is now in play. The new factor is that we now have a new Minister of Justice. First and foremost, we should perhaps seriously think about inviting him to appear before us and simply tell us what his intentions are as far as a new Access to Information Act is concerned.

[*English*]

The Chair: So does that mean you're no longer pursuing your initial motion to have the chair write to the minister, and you're now suggesting that we consider inviting the minister here? Am I understanding you correctly?

[*Translation*]

Mrs. Carole Lavallée: I will set aside the proposed letter because there is a new minister. We therefore cannot hold him responsible for requests that we made of the former minister, and perhaps he has somewhat different ideas on the Access to Information Act. Of course, I still want the Minister of Justice, the person responsible for the Department of Justice, to come here and table a new access to information bill, but I would agree that we begin by meeting with the minister and seeing what his plans are. I'm not against the idea of a new Access to Information Act.

[*English*]

The Chair: Okay. Thank you.

Just so the committee members know, the committee has agreed to a work plan. That work plan has taken care of each and every day between now and the end of February, when we have our break. If we have the Minister of Justice, there's no problem. We can call an extra ordinary meeting at a time that is convenient for all the members, but I'm not suggesting that the committee change its work plan under the statutory mandate that we have to review PIPEDA.

So I guess there will be two questions. The first question would be whether the committee is of the view that we invite the new Minister of Justice to appear before the committee to talk about his plans with respect to access to information. If the committee is of such a view, can I then have the committee's permission to call an extra ordinary meeting at a time and place to be agreed upon by the members?

Mr. Tilson.

● (1040)

Mr. David Tilson: Mr. Chairman, I don't disagree with a lot of what Madame Lavallée is talking about. We have a new minister who's been in that position for less than a month. We have a new Information Commissioner—I don't know when that formally took place. Just before the break? He's been in his position for a little over a month, perhaps. Both those individuals may or may not agree with the proposed information legislation that was prepared by former Commissioner Reid. We don't know that. We've got a whole bunch of new players and I can't believe they're not going to want to talk to themselves and to the commissioner before they even come here. Before they talk to themselves, they're going to want to talk to other stakeholders before they come here—in other words, get briefed on the topic. They're going to want to talk to other people, such as the Privacy Commissioner, people like that.

As well, there's the issue of the discussion paper the former minister tabled last April, I think it was. We've had a copy of it; I read sections of it, which deal with the issue of the cost and that sort of thing. We've received it, but we've never debated it or ever talked about it or ever asked for opinions about it. I have no problem—I don't know what others think—with the minister being invited to come, but because of all the things I'm saying, and because of our work plan—which was agreed to by all parties, I might add—I'm suggesting that perhaps the chair or the clerk ask the minister if he'd be available to come perhaps after the March break.

The Chair: Thank you, Mr. Tilson.

On the issue of the consideration of the draft you mentioned, the committee's decision was not to do that but to ask the minister to provide us with a bill that we could look at section by section. That was the decision of the committee and that's why we haven't looked at it.

Mr. David Tilson: I appreciate that, and I didn't mean anything derogatory toward the committee. It's just that it's an issue dealing with information legislation. I can't believe the minister isn't going to come here and ask us what we think about that paper.

The Chair: Would we have consensus then, as the first issue, that the committee would invite the minister here to discuss his views on access to information? That's number one.

Number two is when. We've heard one suggestion from Mr. Tilson and the reasons for it—i.e., to let the minister get up to speed, that we deal with this after the March break. If we do that, the March break takes place for two weeks in March, so I presume we're talking about, depending on the minister's schedule, the first or second meeting after the March break. That's one suggestion. I'm looking for others, if any.

Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: If you are talking about the first or second meeting after the March break, I agree with you. As we are now meeting on Tuesdays and Thursdays, that would be either the 20th or the 22nd of March. If we said March 22nd at the latest, I think that would be reasonable.

[*English*]

The Chair: Okay. I see consensus here. I'll write a letter on behalf of the committee inviting the minister to appear here on the Tuesday, or the Thursday at the latest, of the week after the March break. Are we in agreement? Excellent. Okay, so on or before March 22, which is the first week back.

Any other business?

[*Translation*]

Mrs. Carole Lavallée: All right.

[*English*]

Hon. Jim Peterson: That must be the new minister's major concern.

The Chair: If there's no other business, I'll adjourn the meeting.

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
