Questions for TELUS Communications Inc. (TELUS)[1]

A. Details of Incident

1. Please refer to page 2, third full paragraph of your letter dated 28 November 2005 in which you indicate that the "impostor" ## provided the Client Care Representative (CCR) with three separate phone numbers before one was found that was associated with TELUS Mobility. Discuss what safeguards a) were in place at the time of the alleged incident and b) are now in place, to ensure that confidential customer information is protected by such forms of "number" shopping. ##

   The paragraph referenced above does not indicate that three separate phone numbers were provided to the CCR. It indicates that the IVR was presented with a phone number #
   #
   #
   #
   #
   #
   #
   #
   #
   #
   #
   #
   #

   The following provides a summary of the safeguards in place for authentication practices at the time of the call.

   At the time of the incident, an authentication process to validate a client's identity was in place. However, this incident involved the impersonation of a TELUS employee. #
   #
   #
   #
   #
   #
   #
   #
   #
   #
   #
   #
   #
   #

[1] For ease of reference the headings are those used by TELUS in its 28 November 2005 letter to the CRTC except for the heading entitled Other.

#
#
#

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

B. After the incident, a reminder was circulated to all front line representatives about the importance of client authentication. #
#
#
#

The following is the content of the front-line communication. This information was also used for on the job training for all CCRs.

#
#
#
#
#
#
#

#

#
#
#

a) ## Please explain the discrepancy in the above quoted statements. That is, if the CCR thought that the caller was disguising his/her voice, why was the CCR not suspicious of the call? ##

#
#
#

There is no discrepancy in the statements provided in the November 28 letter.

#
#
#
#
#
#
#

b) ## Comment on the appropriateness of instituting safeguards or policies which would allow CCRs to flag (or elevate to a supervisor) calls where requests to divulge customer confidential information are deemed suspicious. ##

#
#
#
#
#
#
#
#

Further, TELUS requires our CCRs to terminate the call if the client cannot provide authentication information. Clients are instructed to call back when they have the correct authentication information. #
#
#

TELUS followed up with training of all CCRs to reinforce this requirement.

B. Safeguards in place at the time of the incident

3. Refer to page 3, sixth paragraph of your letter dated 28 November 2005.

   Explain how TELUS Mobility reached the conclusion that there was no external electronic access to the cell phone records in question.

#
#

4. Provide copies of the three e.learning programs referred to in page 3, last paragraph of your letter dated 28 November 2005.

Unfortunately, it is not possible to provide copies of the three e.learning programs. These programs are interactive and require the appropriate underlying software modules in order to run. They cannot be printed. However, should CRTC staff require, TELUS can make arrangements for access to these training programs.

C. How TELUS Mobility validates the identity of a party requesting customer Information

A CCR must use the authentication process to validate the identity of a party requesting customer information. #
#

5. Confirm whether the measures listed under this heading refer to what is currently in place. If so, please indicate whether these same measures were in place at the time of the alleged incident. If the measures differ indicate how they differ.

#
#
#
#
#
#

D. The means by which confidential customer information is provided

#
#
#

6. Confirm whether the measures listed under this heading refer to what is currently in place. If so, please indicate whether these same measures were in place at the time of the alleged incident. If the measures differ indicate how they differ.

#
#
#
#

E. Description of additional safeguards TELUS Mobility has taken and will be taking

7. ## Please provide a copy of the information package regarding "social engineering" sent to TELUS CCRs and the updated training material provided to all new CCRs. ##

The following is the content of the information package on "social engineering". This information was also used for training of all CCRs.

#

#
#
#

#

#
#
#

#

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

8. Please refer to page 5, second to last paragraph of your letter dated 28 November 2005 in which you indicate that TELUS ## will use "mystery shopper" calls. Please provide full details, including when and what was done and the results, analysis and recommendations, if any, with respect to such calls. Provide copies of all related documentary reports. ##

#
#
#

#
#
#
#
#

#
#
#
#
#

It appears from the foregoing that the revised authentication procedures and CCR education have been effective.

9. ## What changes, if any, were made to TELUS Mobility's processes and practices as a result of such "mystery shopper" calls. ##

#
#
#
#
#
#

#
#
#
#
#

Other –

10. If your company does not prohibit CSRs from volunteering any confidential customer information, comment on the appropriateness of establishing such a safeguard. If your company does prohibit CSRs from volunteering confidential customer information, provide a copy of any written guidelines outlining this procedure.

CCRs do not volunteer any confidential information. They must always follow the authentication process. #
#

11. Consider a situation where an individual identifies himself/herself as an employee of the company or an agent of the company, prior to requesting confidential information from a CSR.

a) Describe the procedures in place for CSRs, at the time the alleged incident took place, to safeguard against an individual falsely identifying himself/herself as an employee of the company or an agent of the company.

#
#
#
#
#

b) Describe the procedures currently in place for CSRs to safeguard against an individual falsely identifying himself/herself as an employee of the company or an agent of the company.

#
#

c) Describe the circumstances, before and since the alleged incident, in which CSRs are required to re-validate the identity of a customer and what this entails.

#
#
#
#
#

d) If CSRs rely on information provided by call display service, describe whether identification by that methodology may be inaccurate and therefore unreliable.

#

12. In the 28 November 2005 issue of Maclean's, it was reported that there exists a computer software that enables a caller to assume another person's identity by making that person's telephone number appear on call display, regardless of where the call is really coming from. Provide your company's view as to whether this is possible. If it is possible, indicate the appropriateness of relying on call display information to validate a customer's identity.

TELUS is aware that "caller ID spoofing" can occur; #
#

13. Describe the safeguards in place to protect against unauthorized electronic access to your company's information technology systems (internal databases, communications networks, web-enabled customer interfaces, etc.) at the time the

alleged incident took place. Identify any changes made to the safeguards subsequent to the alleged incident.

As noted previously, there was no evidence of any unauthorized electronic access.

14. Please explain why the safeguards in place to protect against unauthorized electronic access are considered appropriate. Include in your answer a description of what your company a) has done and b) is doing on an ongoing basis to verify the adequacy of the safeguards and to ensure adequate protection against evolving methods of unauthorized electronic access.

As noted previously, there was no evidence of any unauthorized electronic access.

15. For each acceptable piece of identification required to validate the identity of a customer, listed in the chart contained in Attachment 2, indicate to what extent that information is publicly available. For example, name, address and postal codes are readily available on the Internet. In addition, the Maclean's article dated 21 November 2005 stated that the Privacy Commissioner of Canada's date of birth was obtained from publicly available property deed and mortgage papers in Montreal. To the extent that any of the pieces of identification is publicly available, explain and justify the appropriateness of using such identification to validate the identity of a calling party.

#
#
#
#

TELUS continuously encourages our customers to create a PIN for their account.
#
#

#
#
#
#
#
#

16. Provide your view as to whether customers should be allowed to request that their confidential customer information not be disclosed by specified methods, such as over the phone, by facsimile, etc.

#
#
#
#
#
#

17. Apart from what is referred to in other questions, since the alleged incident, has your company or any third party engaged by your company done any investigations, mystery shopper calls, audits, reports, etc. related to the accessibility of confidential customer information? If so, provide full details, including the terms of reference, when and what was done and the results, analysis and recommendations, if any. Provide copies of all related documentary reports.

#

#
#
#
#
#
#
#

It is important to note that the risk of unauthorized access by U.S. data brokers has been significantly reduced through the legal actions of carriers in the U.S. and Canada, as well as proposed legislation in the U.S.

18. If your company has undertaken any of the activities referred to in question 17, what changes, if any, were made to the company's processes and practices as a result?

#
#
#
#

19. Please provide any and all written policies and procedures with respect to the confidentiality of customer information that a) were in force at the time of the alleged incident and b) which are currently in force.

All wireless account details are classified as confidential information and are only discussed after the client authentication process is successful. Additionally, our employees are fully aware of the CRTC-prescribed confidentiality obligations in our client service contracts.
Further, TELUS has three key written policies related to confidentiality of customer information, each with associated e.learning training modules. For

your convenience, two of these policies are available on-line through our telus.com website. Our Ethics Policy is posted at the following link on telus.com: http://about.telus.com/governance/ethics.html. Our Privacy Code is available on telus.com by clicking on the word "privacy" at the bottom of any page. #
#
#

20. On 10 February 2006, the Federal Communications Commission (FCC) launched a proceeding, with a Notice of Proposed Rulemaking (NPRM)[2], to examine whether additional security measures could prevent the unauthorized disclosure of sensitive customer information held by telecommunications companies. Among other items, the FCC seeks comment on the feasibility and advisability of: 1) requiring carriers to adopt a consumer-set password system to protect access to confidential customer information; 2) requiring carriers to establish audit trails that record all instances when a customer's records have been accessed, whether information was disclosed, and to whom; 3) data stored by the carrier being encrypted; 4) whether confidential customer information should be deleted when it is no longer needed and, if so, how long it should be kept; 5) whether certain types of requests for the release of confidential customer information should trigger an advance notification requirement; 6) whether customers should be notified after the release of their confidential customer information; 7) requiring carriers to permit customers to put an absolute 'no release' order on their confidential customer information.

If it is not your company's policy to a) require all customers to password-protect their account; b) establish an audit trail that records all instances when a customer's records have been accessed, whether information was disclosed, and to whom; c) encrypt stored data; d) delete confidential customer information when it is no longer needed; e) notify the affected customer if a request for the release of that customer's confidential customer information has been received; f) notify customers after release of their confidential customer information; and g) permit customers to put an absolute 'no release' order on their confidential customer information, address the feasibility and appropriateness of establishing such a policy for each of a) – g).

As a general comment, the feasibility and appropriateness of establishing each of these policies must be considered in light of the following:

1. the extent of the risk of unauthorized disclosure of confidential customer information by TELUS CCRs. (Considering the millions of client inquiries that are handled by TELUS CCRs each year, and the number of reports of unauthorized disclosure, it is evident that the risk is very low.);
2. the cost of implementing the policy;
3. its likely effectiveness in mitigating the risk;

[2] Federal Communications Commission, Notice of Proposed Rulemaking, CC Docket No. 96-115; RM-11277, FCC 06-10, adopted February 10, 2006 (RM-11277).

4. the impact that implementing the policy will have on customers' ability to access their account information and manage their accounts;
5. the relative sensitivity of the customer information at issue; and
6. the adequacy of TELUS' current policies and safeguards.

It might be feasible for TELUS to implement policies that would reduce to zero the risk of an unauthorized disclosure ever occurring. However, it would be inappropriate to do so given the costs and the negative impact on our customers.

Instead, TELUS identifies and evaluates risks as they arise and takes appropriate steps to mitigate those risks. #
#
#

With reference to items (a) to (g) above:

a) Password protection is a best practice and should be a goal of authentication mechanisms. However, password protection may not be feasible for all accounts in all circumstances. Implementation of such systems in a wireline environment, for instance, would be a lengthy and time consuming process that would require customer contact and authentication.
b) Again, audit trails would be a best practice, but may not be financially feasible for all business models of common carriers. #
#

c) Encryption of stored data is a best practice for certain types of information. It may not be feasible for all systems and all data elements; however, it may be appropriate for certain financial information such as credit card numbers. Having encrypted data would not have altered the events surrounding the incident and therefore not have added any value.
d) Deleting personal information when no longer required to fulfill the purposes for which it was collected is already a requirements under the "Personal Information Protection and Electronic Documents Act" (PIPEDA), and therefore all organizations in Canada subject to PIPEDA, or to substantially similar legislation, are required to have such a policy.
#
#
e)
f) While this may be a best practice in some circumstances, it may not be practical or feasible for some customers.
#
#
g)

#
#

21. With respect to d) in question 20 above, list by item the company's retention periods for confidential customer information.

    TELUS has established a Records Retention Policy which includes a retention schedule with over 200 classifications, many of which relate to confidential customer information. We can provide a copy of the retention schedule associated with the Policy on request, but submit that this is not relevant to the circumstances at hand. Suffice to say we have developed a comprehensive Policy based on legal and business requirements for all records kept by the organization.

22. If it is not your company's policy to notify customers when their account information has been modified, comment on the feasibility and appropriateness of establishing such a policy.

#
#
#
#
#
#
#
#

23. If it is not your company's policy to encourage customers to password-protect their accounts, comment on the feasibility and appropriateness of establishing such a policy.

    Clients are encouraged to password-protect their accounts at the time of activation.

24. If it is not your company's policy to notify customers when their password has been changed, comment on the feasibility and appropriateness of establishing such a policy.

    Only a client that has been authenticated can change the password. Therefore, the client already knows that his or her password has been changed.

25. If it is not your company's policy to place a limit on the amount of confidential customer information, such as the number of calls for which call detail is provided, that may be distributed a) during one session, b) in total, comment on the appropriateness of establishing such a policy.

    A CCR needs to the ability to discuss the invoice to resolve various billing issues on behalf of the client. The call records that appear on a client's invoice are the client's billing transaction records. As such, the client has the right to question, dispute and discuss these records with a TELUS CCR. #

#

26. For each type of confidential customer information that is allowed to be divulged, address why each method (e.g. mail, fax, etc.) chosen to distribute confidential customer information ensures that such information is likely to reach the real customer.

#
#
#
#
#
#
#
#

27. If your company faxes copies of customer bills on request, please comment on the appropriateness of establishing a safeguard that would require such information to only be mailed to the listed mailing address.

#

28. Please fill in the chart contained in Attachment 2.

#
#
#
#
#
#