TELUS®

TELUS Communications Inc.
5-3777 Kingsway Avenue
Burnaby, B.C.
V5H 3Z7

604 432-5053 Telephone
604 430-4258 Facsimile

SECRETARIAT
IM / TELECOM

DEC 09 2005

8665-C12-20051/3483
GI / TELECOM
SECRETARIAT

By Facsimile

December 9, 2005

Mr. Gerry Lylyk
Director, Consumer Affairs
Telecommunications Branch
Canadian Radio-television and Telecommunications Commission
Ottawa, Ontario
K1A 0N2

Dear Mr. Lylyk:

Re: *Maclean's* Magazine article re disclosure of phone records

TELUS Communications Inc. (TELUS) is in receipt of your letter dated 2 December 2005 wherein TELUS was requested to file with the Commission a public claim of confidentiality along with an abridged version of our letter dated 28 November 2005 in relation to the above-captioned matter. The following constitutes TELUS' reply to this request. TELUS has also attached an abridged and amended version of our letter dated 28 November 2005.

TELUS continues to maintain its claim of confidentiality pursuant Section 39 of the *Telecommunications Act* and Section 19 of the *CRTC Telecommunications Rules of Procedure* in relation to portions of the letter dated 28 November 2005, on the basis that the letter contains confidential customer information as well as confidential and sensitive information as to TELUS Mobility's processes regarding security and fraud management practices (and, possibly, vulnerabilities therein). As explained in the letter dated 28 November 2005, and more fully explained below, disclosure of these security and fraud management practices would assist fraudsters by identifying and explaining the very systems and practices designed and put in place to protect confidential customer information, and thereby cause specific and direct harm to TELUS, TELUS Mobility, and their customers by significantly impairing their ability to prevent unauthorized access to customer confidential information.

In relation to the customer confidential information redacted from the 28 November 2005 letter, TELUS notes that this information includes information about the telephone numbers that were involved in this incident, to whom those telephone numbers were assigned (i.e., the name of or identifying information about the customer) along with the details of the equipment and services used or belonging to the various customers affected by this incident. TELUS submits that there is no public interest to be served in disclosing on the public record this confidential information relating to identifiable customers. TELUS requests therefore that, absent express customer consent to disclose this information publicly, the Commission keep this information confidential.

In relation to the processes and safeguards put in place to prevent unauthorized disclosure, TELUS observes that public disclosure of both the processes themselves (including the discussion of potential vulnerabilities) and the security measures and/or safeguards put in place, will undermine TELUS and TELUS Mobility's ability to prevent unauthorized disclosure in the future, and thereby cause specific and direct harm to TELUS, TELUS Mobility, and potentially our customers. Indeed, disclosure of the processes would likely cause specific and direct harm to other telecommunications service providers. If, for example, TELUS were to disclose information regarding the processes used by TELUS Mobility's Client Care Representatives for customer authentication, then this would potentially expose other telecommunications service providers (as fraudsters may say to themselves: "Okay. TELUS has remedied its processes, but I wonder if I can try the same tactic on a different service providers. If it worked once at TELUS, maybe it will work on another service provider who has similar processes to those that TELUS had implemented or amended.") TELUS also observes the specific details around the circumstances leading to the unauthorized disclosure provide information to fraudsters as to where and when validations, etc. took place, thereby indirectly identifying communications channels and/or means of entry into the company that are likely more susceptible to fraudulent activities.

In relation to disclosure of the security measures and/or safeguards, TELUS submits that disclosure of these measures and safeguards undermines their effectiveness, thereby causing specific and direct harm to TELUS, TELUS Mobility, their customers and any of the other TELUS affiliates relying on these same measures and safeguards. It is analogous to disclosing to a jewel thief a list of the various security measures put in place intended to foil a robbery or burglary.

Finally, TELUS submits the public interest in disclosure of the redacted portions of the letter dated 28 November 2006 do not outweigh the specific and direct harm to TELUS and its affiliates likely to be caused by their disclosure. TELUS respectfully submits that the Commission has before it the information that it needs to assure itself that appropriate measures have been implemented to ensure that similar unauthorized disclosure does not occur in the future.

For all of these reasons, TELUS respectfully submits that the information redacted from the letter dated 28 November 2006 should continue to be held in confidence and not placed on the public record.

Sincerely,

Drew McArthur
Vice President Corporate Affairs and Compliance Officer

c. Willie Grieve
Renée Gauthier, CRTC (819) 994-5174

Attachment

TELUS®

TELUS Communications Inc.
5-3777 Kingsway Avenue
Burnaby, B.C.
V5H 3Z7

604 432-5053 Telephone
604 430-4258 Facsimile

By Facsimile

AMENDED AND ABRIDGED

November 28, 2005

Mr. Gerry Lylyk
Director, Consumer Affairs
Telecommunications Branch
Canadian Radio-television and Telecommunications Commission
Ottawa, Ontario
K1A 0N2

Dear Mr. Lylyk:

Re: *Maclean's* Magazine article re disclosure of phone records

We refer to your letter of November 18, 2005 and to the *Maclean's* Magazine article of November 21, 2005 referred to therein. According to that article, a U.S.-based databroker doing business as *Locatecell.com* obtained confidential telephone records of Ms. Jennifer Stoddart, the Privacy Commissioner of Canada, from Bell Canada and TELUS Mobility and also obtained the confidential telephone records of another individual from the Fido division of Rogers Wireless.

The purpose of this letter is to respond to the Commission's request that TELUS investigate and report to the Commission on this incident as it relates to TELUS Mobility. In particular, as requested, this letter will provide the following:

A. an outline of the specific details of what occurred;

B. a description of the safeguards that were in place at the time the incident took place;

C. details as to how TELUS Mobility validates the identity of a party requesting confidential customer information;

D. the means by which confidential customer information is provided; and

E. a description of additional safeguards that have been or will be implemented.

Before proceeding further, however, we wish to note that some of the facts in the *Maclean's* article are incorrect. For example, we have determined that the cell phone logs that were disclosed by TELUS Mobility to *Locatecell.com* were not associated with the Privacy Commissioner, but rather with another individual in her office. We also wish to note that the writer has spoken with both Ms. Stoddart and the other individual and has apologized to

both on behalf of TELUS. As indicated to them, TELUS takes this matter very seriously and is taking all reasonable steps to prevent further such incidents.

We also wish to note that this letter contains confidential customer information as well as confidential and sensitive information as to TELUS Mobility's security and fraud management practices. If these security and fraud management practices were made public, it would assist fraudsters by identifying the very systems and practices designed and put in place to protect confidential customer information (and which the fraudster needs to thwart) and thereby cause specific and direct harm to the company by significantly impairing our ability to prevent unauthorized access to confidential customer information. Accordingly, TELUS is filing portions of this letter in confidence pursuant to section 39 of the *Telecommunications Act* and section 19 of the *CRTC Telecommunications Rules of Procedure.*

A. Details of Incident

We have determined that an impostor called into TELUS Mobility's customer care Interactive Voice Response ("IVR") system on November 3, 2005, and entered the number # into the system. #

#

When the CCR received the transferred call, the impostor apparently gave her a different number #

#

#

During the call, although the team member felt rushed, she did not feel suspicious about the call. However, after the call was terminated, she began to be suspicious and mentioned this to her manager.

On reviewing the cell phone records provided to the OPC by the *Maclean's* reporter, we have determined that they are not associated with the cell phone used by Ms. Stoddart, but rather with the cell phone used by another staff member, which is covered by the same government account. Further, the information provided was not accurate, as there were many errors and omissions in the records. The records provided by *Maclean's* also show indications of outbound and inbound calls, #

The records made available to *Maclean's* by *Locatecell.com* list approximately 75 calls made between September 28 and October 27, 2005. The list shows dates, telephone numbers, and whether the call was outbound or inbound. However, as noted above, the "inbound" notations are incorrect. There are no names or other identifiers associated with the numbers on the report.

It is important to note that this is the first time that we have heard of a TELUS company and its customer being victimized by one of these U.S. data brokers.

B. Safeguards in place at the time of the incident

TELUS Mobility has security provisions in place to ensure that its internal electronic information systems are protected from external access, and its on-line access mechanisms are secure as well. There was no external electronic access to the cell phone records referred to in this letter. #

There is no evidence of a breach of any of TELUS Mobility's electronic safeguards.

#

#

Included in CCR training is the requirement to complete three e.learning programs: e.ethics, e.privacy, and e.security. Each of these programs has references to confidential customer information and the requirements from a regulatory and privacy perspective to protect confidential customer information.

Also, TELUS Mobility provides periodic reminders to CCRs at their workstations by electronic means to ensure that CCRs are following appropriate authentication procedures as outlined in their procedural guides. #

.#

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

TELUS Mobility uses the following procedures to verify and validate the identities of parties requesting customer information. Similar processes are used for TELUS Communications Inc., but are not detailed here as the incident described in Section A above involves TELUS Mobility.

#

#

D. The means by which confidential customer information is provided

#

#

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

As soon as TELUS Mobility became aware of this incident, TELUS Mobility immediately took steps #

#

We believe we are taking all reasonable steps to prevent this type of unauthorized access to customer confidential information, while at the same time recognizing our customers' legitimate need to access their information as required. To put this in context, TELUS Mobility handles over 14 million customer calls in a typical year, and this is the first instance

of which we are aware of unauthorized access to TELUS Mobility customer information by either *Locatecell.com* or other U.S. data brokers.

Sincerely,

Drew McArthur
Vice President Corporate Affairs and Compliance Officer

c. Willie Grieve