QUESTIONS FOR ROGERS WIRELESS PARTNERSHIP (RWP)/FIDO INC. (FIDO) (COLLECTIVELY ROGERS)[1]

QUESTION:

B) FIDO INVESTIGATION

1. REFER TO THE REPORT ATTACHED TO YOUR LETTER DATED 28 NOVEMBER 2005, PAGE 1,

   THIRD PARAGRAPH. EXPLAIN WHY FIDO DID NOT PERFORM A QUERY WITH THE NAMES OF ALL OF THE EDITORIAL STAFF AT MACLEAN'S IN ALL AREA CODES (I.E., NOT LIMITED TO 416, 647 AND 613) WHERE FIDO IS PROVIDING SERVICE, IN ORDER TO IDENTIFY THE SENIOR MACLEAN'S EDITOR IN QUESTION.

ANSWER:

1. FIDO targeted its search to the 416, 647 and 613 area codes #C

#C

#C

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

#C – Filed in Confidence with the CRTC

QUESTION:

D) RWP'S INVESTIGATION

2. PLEASE PROVIDE ANY ADDITIONAL MEMORANDA, OR OTHER WRITTEN INFORMATION, SENT TO ROGERS' EMPLOYEES CONCERNING THE CONFIDENTIALITY OF CUSTOMER INFORMATION SINCE THE AUDIT OF ROGERS' VALIDATION PROCESSES.

3. PROVIDE A COPY OF ALL DOCUMENTED INFORMATION RELATING TO THE INVESTIGATION CONDUCTED BY RWP AS REFERENCED IN SUBSECTION D) OF THE REPORT ATTACHED TO YOUR LETTER DATED 28 NOVEMBER 2005.

ANSWER:

2. See Schedule A for additional information sent to FIDO employees since the audit of validation processes. #C

#C

See Schedule B, C and D for additional information made available to Rogers employees #C

#C

3. See Schedule E for a copy of all documented information relating to the investigation conducted by Rogers Corporate Security Group. #C

#C

#C

#C

#C – Filed in Confidence with the CRTC

QUESTION:

E) ACCESSED INFORMATION

4. ROGERS INDICATES THAT IN MOST CASES CREDIT CARD NUMBERS, SOCIAL INSURANCE NUMBERS, DRIVER LICENSE NUMBERS AND BANK ACCOUNT NUMBERS ARE FULLY OR PARTIALLY MASKED ON THE SYSTEM THAT CSRS USE SO THAT CSRS MAY NOT READILY ACCESS THAT INFORMATION. IN WHAT CASES, AND TO WHAT EXTENT, ARE EACH OF THE ABOVE NUMBERS FULLY MASKED, PARTIALLY MASKED, AND NOT MASKED AT ALL?

5. WHERE SUCH NUMBERS ARE FULLY OR PARTIALLY MASKED HOW DOES THE CSR VALIDATE CALLER IDENTIFICATION WHEN THE CALLER PRESENTS SUCH NUMBERS?

ANSWER:

4. When a first time customer signs up for service by phone, an activation CSR has full visibility of the customer's personal information. However, from that point onward CSRs servicing the account do not have visibility to this information as it is masked to some extent. #C #C #C

Note that individuals who work in have the ability to unmask all information as it may be required for However, the information is unmasked only on an as needed basis (see Schedule F). #C #C #C

5. Where numbers are partially masked a CSR validates caller identification by paying attention to those numbers that are visible as the caller articulates the entire number associated with a piece of identification. At no time does a CSR ask a customer for only those digits they can see. #C #C

#C – Filed in Confidence with the CRTC

QUESTION:

F) AUDIT OF ROGERS' ID VALIDATION PROCESSES

6. PROVIDE FULL DETAILS, INCLUDING THE TERMS OF REFERENCE, WHEN AND WHAT WAS DONE AND THE RESULTS, ANALYSIS AND RECOMMENDATIONS, IF ANY, WITH RESPECT TO ROGERS' AUDIT OF ITS ID VALIDATION PROCESSES FOR EACH OF THE POINTS OF CUSTOMER CONTACT (CSR, IVR AND WEBSITE) ## REFERRED TO IN SUBSECTION F) OF THE REPORT ATTACHED TO YOUR LETTER DATED 28 NOVEMBER 2005. PROVIDE COPIES OF ALL RELATED DOCUMENTARY REPORTS.

ANSWER:

6. No formal terms of reference were developed for the audit of Rogers' ID validation processes as internal resources were dedicated to the completion this task. A cross-functional team was immediately formed to review the ID validation processes and procedures in place at both Rogers Wireless and of FIDO. #C #C

These changes included: #C

a) Discontinuing the faxing of call detail records #C #C #C

b) Tightening up existing authentication methods when customers called a live CSR #C #C

c) Communicating with the CSR's informing them of the new validation methods and reaffirming the importance of protecting our customer's personal information.

Note that changes were not required to be made to Rogers' or FIDO's website as the methods of authenticating a customer through the respective web portals proved secure.

#C

#C

#C – Filed in Confidence with the CRTC

QUESTION:

G) COUNTERMEASURES

7. COMMENT ON WHY THE FOLLOWING COUNTERMEASURES LISTED IN SUBSECTION G) OF THE REPORT ATTACHED TO YOUR LETTER DATED 28 NOVEMBER 2005 ARE NOT REFLECTED EXPLICITLY IN SCHEDULES "E", A MEMORANDUM DATED 11 NOVEMBER 2005 TO ALL WIRELESS AND COMMON CUSTOMER CARE EMPLOYEES AND "F", A MEMORANDUM DATED NOVEMBER 25, 2005 TO ALL ACCOUNTS RECEIVABLE EMPLOYEES: ROGERS' NEW RULE LIMITING THE AMOUNT OF CALL DETAILS A CSR MAY DISCUSS WITH A CUSTOMER OVER THE PHONE; THE EXPLICIT PROHIBITION ON CSRS VOLUNTEERING A CUSTOMER'S ADDRESS, CELLULAR PHONE NUMBER OR ACCOUNT NUMBER; AND THE REQUIREMENT TO PROVIDE TWO ADDITIONAL PIECES OF IDENTIFICATION IN ORDER TO CHANGE A CUSTOMER'S MAILING ADDRESS.

8. COMMENT ON WHY IT IS APPROPRIATE THAT A CUSTOMER WANTING TO ESTABLISH A NEW PASSWORD/PIN (HEREAFTER PASSWORD) CAN DO SO THROUGH A CSR, IVR OR WEBSITE WHILE A CUSTOMER IS REQUIRED TO VISIT A ROGERS RETAIL OUTLET IN PERSON WITH A PHOTO ID TO ESTABLISH A REPLACEMENT PASSWORD WHEN A PASSWORD HAS BEEN FORGOTTEN.

ANSWER:

7. The new rule on limiting the amount of call details a CSR may discuss with a customer over the phone was not included in the November 11th memo. However, the rule was included in #C

#C

#C

The explicit prohibition on CSRs volunteering a customer's address, cellular phone number or account number is not absent from the memos. Under the heading it states: #C

#C – Filed in Confidence with the CRTC

…"Please do not provide any information to the person on the phone until you have verified that your are speaking to the correct customer (i.e., the customer should say "I am John Smith". Do not ask the customer "Are you John Smith?")."

#C

#C

The requirement to provide additional pieces of identification in order to change a customer's mailing address is absent from the memos. However, direction was given to the CSRs to ask for an additional piece of information in (see Schedule B). #C

8. Rogers believes there is an important difference between establishing a new password and replacing a forgotten one. Rogers wishes the process to set up a password be as easy as possible in order to provide our customers with increased security. However, Rogers considers the fact that the customer established a password in the first place as an indication that they have heightened privacy and security concerns. As such, Rogers created a stricter procedure to replace a password in keeping with the customer's desire for a higher level of account security. To date we have not received complaints on our stringent measures to change a password.

QUESTION:

H) ADDITIONAL INFORMATION

9. WITH RESPECT TO THE EXTERNAL CONSULTANT HIRED BY RWP REFERRED TO IN SUBSECTION H) OF THE REPORT ATTACHED TO YOUR LETTER DATED 28 NOVEMBER 2005, PROVIDE FULL DETAILS, WITH REGARD TO ROGERS, INCLUDING THE TERMS OF REFERENCE, WHEN AND WHAT WAS DONE, RESULTS, ANALYSIS AND RECOMMENDATIONS, IF ANY. PROVIDE COPIES OF ALL RELATED DOCUMENTARY REPORTS.

10. INDICATE WHAT CHANGES, IF ANY, HAVE BEEN MADE TO ROGERS' PRACTICES AND SAFEGUARDS WITH RESPECT TO CUSTOMER CONFIDENTIAL INFORMATION AS A RESULT OF THAT REVIEW.

ANSWER:

9. After the alleged incident in the Maclean's article, Rogers contracted to identify opportunities to reduce the #C
risks associated with customer identification validation. was brought #C
in after our internal audit was complete and was mandated to review Rogers' privacy and ID validation policies and processes. #C
The work performed by #C
entailed the following scope: #C
    1. Review and document Rogers' current practices for validation of customer identification at points of entry (i.e. call centre, IVR, website) for Rogers Wireless, FIDO, Rogers Cable, and Rogers Telecom.
    2. Research best practices for authentication methods by industry (i.e. telecom, banking, ISP, etc.) in North America and Europe.
    3. Provide recommendations focusing on a unified and standard approach for customer identification applicable to Rogers' environment and customer service culture that comply with PIPEDA and the CRTC privacy rules

completed their assessment, as per the aforementioned scope, and #C
provided recommendations in their report dated #C
Limitations in the contract between Rogers and prevent the release #C
of the entire report to third parties. agreed to release the following #C
excerpt from their Executive Summary titled Next Steps. #C

#C

#C

#C

#C

#C

#C

#C

#C

#C

#C

10. Subsequent to the recommendations presented by ,Rogers immediately set up a working group mandated to review the recommendations and assess the feasibility of their implementation. This working group is comprised of representatives from departments. The scope of this working group is: #C #C

#C

#C

#C

#C

#C

#C

Rogers will be also be #C

#C

#C

#C

#C

#C

#C

Rogers has #C
#C
This has resulted in an elimination of ambiguity for #C
CSRs with simplified and concise call handling rules while reinforcing
more stringent authentication methods. #C
#C

QUESTION:

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.

ANSWER:

11. a) #C

#C

#C

#C

#C – Filed in Confidence with the CRTC

b) Rogers' current procedures prohibit a CSR from disclosing a customer's account information to an individual identifying himself/herself as an employee/agent of Rogers and attempting to administer an account that is not their own. #C

#C

#C

c) In instances where a customer's call is transferred from one CSR to another, the second CSR is required to revalidate the identity of a customer. This has always been the practice at Rogers and continues to be the case.

d) CSRs do not rely on call display information to authenticate a customer.

#C
#C

QUESTION:

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.

ANSWER:

12. It is technologically possible for a caller to display the telephone number of another individual on call display. This is called "caller ID spoofing" or "call display spoofing" and masks the true originating telephone number from which a call is placed. Through the use of a web interface a spoofing system lets unscrupulous companies or individuals appear to be calling from any phone number and organization they choose. #C

#C

#C

To the best of our knowledge, spoofing technology is IP-related and has become available with the onset of VoIP. We are not aware of technology that permits spoofing when both the individual calling and the individual being called reside on the PSTN.

Rogers does not believe it to be appropriate to rely on call display information to validate a customer's identity. The reasons are twofold. First, customers often phone in from phone numbers not associated with their account. Therefore, call display can never be used to authenticate customers in cases where phone numbers are not associated with a customer's account. Second, because of the aforementioned technology, #C

#C

QUESTION:

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.

ANSWER:

13. Unauthorized electronic access to Rogers' information technology systems was not a deficiency found during the alleged incident captured in the Maclean's article.

Rogers has in place #C
#C
at #C
the time of the alleged incident, safeguards were reviewed to ensure containment and adherence to security policies and procedures by Rogers Call Centre employees. Our investigations conducted by both internal staff and external consultants showed that all employees were compliant with existing security policies and procedures. Therefore, no changes to these safeguards were required.

QUESTION:

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.

ANSWER:

14. Rogers Group of Companies has in place #C

#C

#C

#C

#C

In Rogers IT and Engineering departments, information systems are under the constant security scrutiny of qualified information security #C specialists that oversee network security as well. The operations groups keep abreast of all new vulnerabilities and apply appropriate counter measures. Rogers IT infrastructures constitute of a vast array of the latest security tools found in the industry such as #C

#C
#C

All of the above ensure that Rogers meets its regulatory requirements as it relates to protecting information for its customers and its information holdings.

QUESTION:

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.

ANSWER:

15. The following chart outlines the pieces of identification that Rogers uses in order to authenticate a customer. For each form of identification we have stated whether it is publicly available and the appropriateness of its use.

FORM OF IDENTIFICATION	IS IDENTIFICATION PUBLICLY AVAILABLE?	APPROPRIATENESS OF USE
#	Yes	In combination with other forms of identification not publicly available, it is appropriate to use.
#	Yes	In combination with other forms of identification not publicly available, it is appropriate to use.
#	Yes	In combination with other forms of identification not publicly available, it is appropriate to use.
#	Sometimes. # #	In combination with other forms of identification not publicly available, it is appropriate to use.
#	No. # #	Not publicly available and therefore appropriate to use.

- filed in confidence with the CRTC

#	Limited public availability. # #	Public availability is limited and significant effort must be made to obtain this information. Therefore appropriate to use.
#	No	Not publicly available and therefore appropriate to use.
#	No	Not publicly available and therefore appropriate to use.
#	No	Not publicly available and therefore appropriate to use.
#	No	Not publicly available and therefore appropriate to use.
#	No	Not publicly available and therefore appropriate to use.
#	No	Not publicly available and therefore appropriate to use.
#	No	Not publicly available and therefore appropriate to use.
#	No	Not publicly available and therefore appropriate to use.

- filed in confidence with the CRTC

QUESTION:

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.

ANSWER:

16. Rogers does not allow customers to customize the ways in which their confidential customer information is disclosed. However, Rogers does offer customers the option to use account passwords which limits the disclosure to users of the password and accomplishes the same objective as customized disclosure.

QUESTION:

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.

ANSWER:

17. Rogers participates in ongoing monitoring of CSR call handling both with in-house CSRs and those employed by third parties. #C

#C

#C

Managers use these calls to consistently #C
monitor the performance and compliance of their CSRs. #C

#C

QUESTION:

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?

ANSWER:

18. The consistent monitoring of CSR calls previously mentioned resulted in some changes in how Rogers validates our customers. #C

#C

#C

#C

#C

#C

#C – Filed in Confidence with the CRTC

QUESTION:

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.

ANSWER:

19. Please refer to Schedules C, D, G, H for written policies and procedures with respect to the confidentiality of customer information which are currently in force. #C

The Schedules are as follows: #C

Schedule C: #C
Schedule D: #C
Schedule G #C
Schedule H: #C
Schedule I: #C

These are living documents and modified as required. #C

#C

#C

QUESTION:

20. IN 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).

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

ANSWER:

20. The feasibility and appropriateness of establishing policies for a) through g) are outlined as follows.

    a. Implement mandatory passwords

    A working group has been established at Rogers to consider, amongst other items in their mandate, the implementation of mandatory passwords. The working group has not yet formulated recommendations in this regard and the policy remains under consideration.

    b. Establish an audit trail when customer information has been disclosed and to whom

#C
#C
#C
#C
#C
#C

    c. Encrypt stored data

    The methods employed by the data brokers in the alleged incident did not compromise the security of stored customer data.

#C
#C
#C
#C

d. Delete customer information

Rogers already has in place a Document Retention Policy that includes the destruction of customer information. This policy was last updated on January 16, 2006.

e. Notify customers if a request for release of information has been received by Rogers

PIPEDA already contains a requirement for Rogers to obtain knowledge and consent of customers before their personal information is disclosed except in instances stipulated in PIPEDA (i.e. a subpoena, a warrant, enforcing/administering Canadian laws, threat of life, health or security, etc.). Rogers believes that PIPEDA sufficiently addresses this and a specific corporate policy is not required.

f. Notify customers after a release of information

#C

#C

g. Permit customers to place a 'no release' order on their account.

Rogers does not currently permit customers to place a 'no release' order on their account. However, Rogers does offer the use of voluntary passwords which accomplishes the same goal for a customer by using an additional level of security. The use of a password renders the use of a 'no release' order unnecessary.

QUESTION:

21. WITH RESPECT TO D) IN QUESTION 20 ABOVE, LIST BY ITEM THE COMPANY'S RETENTION PERIODS FOR CONFIDENTIAL CUSTOMER INFORMATION.

ANSWER:

21. Rogers' Document Retention Policy (last updated January 16, 2006) was developed considering Canadian legal requirements (i.e. PIPEDA), tax audit requirements and operational requirements. Customer information is typically destroyed years after an individual ceases to be a customer of Rogers #C
However, the records may be held longer than #C
The #C
records will be retained permanently if they are subject to litigation.

#C – Filed in Confidence with the CRTC

QUESTION:

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.

ANSWER:

22. Rogers currently notifies customers of #C

#C

#C

#C

#C

#C

QUESTION:

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.

ANSWER:

23. The use of mandatory passwords is currently under consideration by a working group at Rogers. To date Rogers has utilized a system of voluntary passwords. We encourage those customers that have heightened privacy or security concerns (i.e. participating in divorce proceedings) to place a password on their account. #C

As it stands #C customers that express an interest in additional account security are informed of the password option.

#C – Filed in Confidence with the CRTC

QUESTION:

24. IF IT IS NOT YOUR COMPANY'S POLICY TO NOTIFY CUSTOMERS WHEN THEIR PASSWORDS HAVE BEEN CHANGED, COMMENT ON THE FEASIBILITY AND APPROPRIATENESS OF ESTABLISHING SUCH A POLICY.

ANSWER:

24. The idea of notifying customers when their passwords have been changed is currently under consideration by a working group at Rogers. A recommendation on this matter is forthcoming. Rogers does not currently notify customers when a password is changed. However, we have stringent policies in place with respect to resetting a password when it has been forgotten by a customer. #C

Individuals that place passwords on their #C accounts in the first place appreciate our stringent policies surrounding password resets. To date we are unaware of any customer complaints with #C

#C – Filed in Confidence with the CRTC

QUESTION:

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.

ANSWER:

25. Rogers currently has in place a policy that limits the amount of call detail information that can be provided verbally by a CSR to a customer to a window. If the customer requires information on call details outside of this window a CSR offers to mail them a copy of their bill. Call details will only be sent by mail and only to the billing address on the customer's account. Rogers recognizes that there are legitimate reasons why customers require some call detail information over the phone. However, we believe that our ID validation procedures, together with our limits imposed on the amount of call details that may be disclosed, adequately address the risks presented by the data brokers. #C #C #C

#C – Filed in Confidence with the CRTC

QUESTION:

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.

ANSWER:

26. Rogers has restricted the methods in which it will release customer information. Rogers has prohibited the use of faxes to disclose customer information. We will also not disclose verbally more than worth of call details to a customer. Rogers will only provide full details of a customer account through regular mail. To further protect this distribution method, customers must provide additional pieces of identification when changing their billing address. We believe this policy addresses those instances when fraudsters hijack an account and have the call detail records sent to an alternate address. Web access to confidential information is password protected in all instances. In the case of Rogers IVR system the amount of customer information that is available is limited to that information that is considered less sensitive and excludes information that is used validate a customer . Rogers believes these policies ensure that the information reaches the customer and only the customer. #C #C #C

#C – Filed in Confidence with the CRTC

QUESTION:

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.

ANSWER:

27. Rogers no longer permits customer bills to be sent via fax. #C
#C

#C – Filed in Confidence with the CRTC

QUESTION:

28. PLEASE FILL IN THE CHART CONTAINED IN ATTACHMENT 2.

ANSWER:

28. Completed chart attached.