File No.: CT 2005-006
Registry Document No.:

COMPETITION TRIBUNAL

IN THE MATTER OF the *Competition Act*, R.S.C. 1985, c. C-34, as amended;

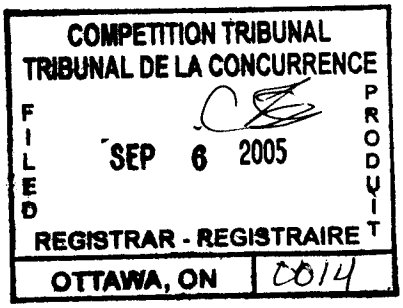
IN THE MATTER OF an application by B-Filer Inc., B-Filer Inc. doing business as GPAY GuaranteedPayment and Npay Inc. for an order pursuant to section 103.1 granting leave to make application under sections 75 and 77 of the *Competition Act*;

AND IN THE MATTER OF an application by B-Filer Inc., B-Filer Inc. doing business as GPAY GuaranteedPayment and Npay Inc. for an interim order pursuant to section 104 of the *Competition Act*.

BETWEEN:

B-FILER INC., B-FILER INC. doing business as GPAY GUARANTEEDPAYMENT and NPAY INC.

Applicants



THE BANK OF NOVA SCOTIA

Respondent

NOTICE OF REPLY BY APPLICANTS TO REPRESENTATIONS BY THE RESPONDENT FOLLOWING APPLICATION BY THE APPLICANTS FOR LEAVE PURSUANT TO SECTION 103.1 OF THE *COMPETITION ACT*

TAKE NOTICE THAT:

1. Whereas the Applicants, B-Filer Inc. B-Filer Inc. doing business as GPAY GuaranteedPayment and Npay Inc. (collectively, "**GPAY**"), have made an application, dated June 17, 2005 (the "**Application**"), to the Competition Tribunal (the "**Tribunal**")

dated June 17, 2005 (the "**Application**"), to the Competition Tribunal (the "**Tribunal**") pursuant to section 103.1 of the *Competition Act*, R.S.C. 1985, c. C-34, as amended (the "**Act**") seeking leave to bring an application for:

(a) an order under subsection 75(1) of the Act directing the Respondent, The Bank of Nova Scotia (hereinafter referred to as "**Scotiabank**"), to accept the Applicants as customers and to provide bank account services, including, without limitation, unlimited E-mail Money Transfer deposit services, to them on usual trade terms; and

(b) an order under subsection 77(2) of the Act prohibiting the Respondent from engaging in exclusive dealing whereby it is withholding its services to the Applicants thereby making banks the only participants in the internet debit payments market in Canada.

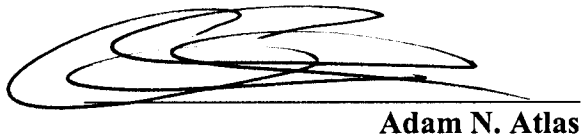
2. Whereas the Respondent has filed a response to the Application, dated July 13, 2005 (the "**Response**").

3. Whereas the Tribunal issued a Direction, dated July 19, 2005, permitting the Applicants to serve and file a reply (the "**Reply**") to the Response on or before noon on Tuesday, September 6, 2005.

AND TAKE NOTICE THAT:

4. In its Reply, GPAY will rely on:
   (a) a Second Statement of Grounds and Material Facts attached hereto;
   (b) the Second Affidavit of Raymond F. Grace ("**Grace**") duly sworn before a lawyer of the Province of Alberta on September 1, 2005 (the "**Grace Affidavit**"); and
   (c) an Affidavit of Joseph Iuso ("**Iuso**") duly sworn before a notary public of the Province of Ontario on August 29, 2005 (the "**Iuso Affidavit**").

DATED at Montreal, Quebec, this 2nd day of September, 2005.



Adam N. Atlas
Adam Atlas Attorney at Law
2000 Mansfield Street, Suite 1400
Montreal, Quebec H3A 3A2
Tel: 514-842-0886
Fax: 514-842-9371
E-mail: atlas@adamatlas.com
Barreau du Québec No.: 201211-1

Counsel for the Applicants

TO:

The Registrar
Competition Tribunal
The Thomas D'Arcy McGee Building
90 Sparks Street, Suite 600
Ottawa, Ontario K1P 5B4
Tel: 613-957-7851
Fax: 613-952-1123

AND TO:

Sheridan Scott
Commissioner of Competition
50 Victoria Street
Gatineau, Quebec K1A 0C9
K1A 0C9
Tel: 819-997-3301
Fax: 819-997-0324

AND TO:

F. Paul Morrison
McCarthy Tétrault LLP
Box 48, Suite 4700
Toronto Dominion Bank Tower
Toronto, Ontario M5K 1E6
Tel: 416-362-1812
Fax: 416-868-0673

A. SECOND STATEMENT OF GROUNDS AND MATERIAL FACTS

1. Raymond F. Grace ("**Grace**") is the President of all the Applicants, B-Filer Inc., B-Filer Inc. doing business as GPAY GuaranteedPayment and Npay Inc. (collectively, "**GPAY**"), and as such has knowledge of the facts set out in his affidavit, dated September 1, 2005 (the "**Grace Affidavit**").

2. The Grace Affidavit was made in support of: (i) an application (the "**Application**") by the Applicants, GPAY, for an order pursuant to section 103.1 of the *Competition Act*, R.S.C. 1985, c. C-34, as amended (the "**Act**") granting leave to the Applicants to make an application pursuant to sections 75 and 77 of the Act; (ii) an application for an interim order pursuant to section 104 of the Act and (iii) an application pursuant to sections 75 and 77 of the Act all against the Respondent, The Bank of Nova Scotia ("**Scotiabank**"); and (iii) a reply (the "**Reply**").by the Applicants to Representations of Scotiabank in Response to Application for Leave Pursuant to Section 103.1 of the Act, filed with the Competition Tribunal (the "**Tribunal**") on July 13, 2005 (the "**Response**").

3. The Grace Affidavit was made to generally respond to the issues and allegations made in the Affidavit of Robert Rosatelli, sworn July 12, 2005 ("**Rosatelli**") and to the Affidavit of David Metcalfe sworn July 12, 2005 ("**Metcalfe**"). The Applicants attempt to refer to specific paragraph numbers in the Rosatelli addifavit, however, owing to the repetitive nature of thereof, specified paragraph referencs may not be all inclusive. The paragraph numbering on the first 233 paragraphs of this Reply is the same as that and corresponds directly to that in the Grace Affidavit.

4. The Applicants have reviewed the Response. The Response contains a number of false statements concerning facts and legal status of the business of the Applicants. The Applicants intend that the Reply should serve two principal purposes. They are: (i) to correct those errors of fact and law in the Response; and (ii) draw the attention of the Tribunal to the questions of competition law at issue in the Application under the Act and

away from the irrelevant and unfounded allegations concerning terrorism, money laundering, security and gambling that form the bulk of the Response.

5. References in this Affidavit to paragraph numbers in Rosatelli or Metcalf, are to corresponding paragraph numbers in those affidavits.

I. THE SCOTIABANK REFUSES TO COMPLY WITH PLAINTIFF'S APRIL 2005, REQUEST FOR COPY OF HIS FILE, CONTRARY TO PIPEDA

6. **Rosatelli: para 7** – The Respondent expresses particular concern over compliance with laws, and invokes alleged non-compliance as grounds to deny its services (the "**Scotia Services**") to the Applicants. In addition to being in breach of the Act, the Respondent is in breach of the *Personal Information Protection and Electronic Document Act*, 2000, c. 5 (Canada) ("**PIPEDA**").

7. The breach by the Respondent of PIPEDA is resulting in the exclusion from this Affidavit of information that would produce a material effect on the Reply.

8. Attached marked **Exhibit "A"** to the Grace Affidavit are copies of two Emails that sent by Grace to Letty Snethan, of the Office of President of the Respondent bank, dated April 4 and 18, 2005, requesting a copy of the Applicants' files and the personal file of Grace.

9. The Respondent has failed to provide the documents requested and that PIPEDA obliges the Respondent to divulge. What is more, a solicitor to the Respondent has advised a solicitor to the Applicants that the Respondent has no intention of responding to the PIPEDA request.

10. The Applicants pray that the Tribunal will take the failure of the Respondent to comply with PIPEDA into consideration when reflecting on the Reply.

II. RESPONDENT'S ALLEGATIONS OF THEIR VARIOUS REASONS FOR TERMINATING THE BANKING RELATIONSHIP:

A. THE APPLICANTS DID FIT THE CUSTOMER PROFILE

11. **APPLICANTS WERE A SMALL BUSINESS CUSTOMER WHEN THEY OPENED THEIR BUSINESS ACCOUNTS: Rosatelli: paragraphs 89-96** – The Respondent states that the Applicants cannot meet the usual trade terms the Respondent. The Applicants believe that the Respondent is, retroactively, interpreting their own trade terms so as to exclude service to a competitor.

12. At the beginning of the business relationship between the Applicants and the Respondent, the Applicants were, without a doubt, within the category of a 'small business customer' of the Respondent, meaning the Applicants processed less than five (5) million dollars per year.

13. Over time, as is the case with many businesses in Canada, including, no doubt, other clients of the Respondent, the business of the Applicants grew.

14. In early 2005, Mr. Ryan Woodrow ("**Woodrow**"), an officer of the Respondent at the local branch of the Respondent servicing the Applicants, informed Grace that his superiors, and Grace took it to mean parties outside the branch, had informed Woodrow was ***"was taking up too much of his time"***.

15. Woodrow had been instructed to refer Grace to a commercial account manager. The only branch with commercial account managers in Edmonton is the Edmonton main branch in down town Edmonton.

16. When Grace asked for the name and number of the commercial account manager Woodrow advised that he did not have a name and number that he could give me.

17. Woodrow offered to make a call and set up an appointment for Grace with a commercial account manager. Despite the offer, neither Woodrow nor any other officer of the Respondent, was able to provide the Applicants with a name or a scheduled appointment, despite Grace raising this with Woodrow on a number of occasions.

18. Attached and collectively marked as **Exhibit B** to the Grace Affidavit is a copy of a letter emailed from Woodrow to Grace, dated March 22, 2005, indicating Woodrow

would arrange for a commercial account manager and a letter from Grace to Woodrow, dated March 24, 2005, requesting such an appointment.

19. Grace called the Edmonton main Scotiabank branch to make an appointment with a commercial account manager at main branch of the Respondent in Edmonton.

20. This person with whom the appointment was made (whose name Grace do not recall) telephoned Grace later that day and left a message canceling the appointment. Grace called the lady back and was advised that she could not deal with Grace and referred Graceback to his local branch.

21. Grace subsequently received an email from the Office of the President of the bank advising me not to speak to any Scotiabank personnel.

22. The Applicants do not see any merit in the argument of the Respondent that because their business grew, the Respondent could not longer serve the Applicants on usual trade termsSurely the Respondent serves clients that process more that five (5) million dollars per year.

B. THE APPLICANTS DID NOT MISPRESENT THEMSELVES TO THE RESPONDENT AT THE TIME OF OPENING THEIR ACCOUNTS

(i) THREE SEPARATE PROFILES: Rosatelli: paragraphs 11, 35-40.

23. Rosatelli appears to suggest that something is wrong or illegal in so far as the representations of the Applicants made upon the opening of the various profiles of the Applicants with the Respondent.

24. In every dealing with the Respondent, Grace and the Applicants have been forthright and direct and have responded to all requests for information and documents in conformity with all policies and procedures of the Respondent known to the Applicants.

25. When the Applicants opened their first account at the Respondent bank in 1999, Grace met Woodrow in person. Woodrow was the branch small business banker and be the account manager of the Applicants.

26. Grace provided to Woodrow documentation showing that GuaranteedPayment, a division of B-Filer Inc. was a registered trade name of B-Filer Inc., which met the criterion of the Respondent for a customer profile distinct from that of B-Filer Inc. (a federally incorporated incorporation, registered extra provincially in Alberta).

27. When Grace later met with Woodrow to open the NPAY Inc. and B-Filer Inc. business accounts, Grace believes that he gave Woodrow copies of the Certificates of Incorporation, Articles of Incorporation and extra provincial registration in Alberta of those two companies.

28. Supply of these documents was the criterion to allow these two (2) corporations to each have a distinct profile with the Respondent Scotiabank. These documents were the only information that Woodrow requested from Grace in respect of the B-Filer Inc. and NPAY Inc. profiles.

29. There we no issues as to any outstanding document during 2004 of which the Applicants were aware. Prior to the Rosatelli Affidavit, the Respondent bank never raised with the Applicants the issue that the Applicants were (or were not) operating as a single business enterprise.

30. The Applicants were each granted a separate profile at the Respondent Scotiabank which was (and is) extremely important to the growth of their business. Woodrow and the Respondent knew that they were related companies.

31. The level of knowledge of the Respondent in the affairs of the Applicants was such that Woodrow often transferred funds between the various accounts of the Applicants on oral instructions by telephone from Grace.

32. The argument of the Respondent that something was not correct with the profiles of the Applicants is wrong and runs against years of friendly enlightened service rendered by Woodrow and other officers of the Respondent.

(ii) DESCRIPTION OF BUSINESS: Rosatelli: paragraphs 19 – 30.

33. Rosatelli states that Grace opened the B-Filer Inc. account on August 6, 1999, describing his business as a "financial collection" business.

34. The business of Grace in August 6, 1999 was indeed to provide services to the collection industry to process payments from debtors through telephone and internet banking.

35. The service delivered by Grace was a certified form of payment that was and is treated by the banks as if it was a cash transaction, that was not subject to chargeback.

36. In 1999, internet banking was in its fledging stage. Woodrow referred Grace to a Scotiabank internet manager with whom Grace met to discuss the proposed business and ask advice about obtaining reports from the Scotiabank and the cost of these services.

37. Grace had incorporated B-Filer Inc. in 1997 for the purpose of filing Bankruptcy Proof of Claim forms on behalf of large financial institutions. Grace had worked in the credit collection industry for about twenty-five (25) years and wanted to be in business on his own.

38. At no time, did the Respondent ever ask Grace for an update of the description of the B-Filer Inc. business when he opened the NPAY and B-Filer business accounts.

39. The average balance in the GPAY Guaranteed Payment A Division B-Filer Inc. account in 1999 was probably $100.00 increasing to maybe a few thousand dollars in 2000.

40. It wasn't until in or about late 2003 or early 2004, that the Applicants' business collectively began to expand with its relationship with UseMyBank Services Inc.

41. As with many businesses in Canada, the business of the Applicant changed. Specifically, the business of the Applicants changed from being a financial collection business to being an internet debit payment facilitation business.

42. Growing a business and changing its nature is not illegal in Canada.

43. At all relevant times, the Respondent was well aware of the nature of the business of the Applicants.

44. Lest there be any doubt as to the full knowledge of the business of the Applicants in the minds of the Respondent at all relevant times, the Applicants are submitting, concurrently herewith, an affidavit by Joseph Iuso ("**Iuso**"), President of UseMyBank Services, Inc., dated August 29, 2005 (the "**Iuso Affidavit**").

45. As stated in the Iuso Affidavit, on or about October 22, 2003, Iuso, was invited by the Canadian Payments Association ("**CPA**") to make a presentation to its members regarding the business of UseMyBank and GPAY.

46. Attached and marked Exhibit B to the Iuso Affidavit is a copy of the list of attendees at the CPA presentation, as provided by an officer of the CPA to Iuso. The lists includes two (2) representatives of Scotiabank, namely: Beth Bailey and Tom Provencher.

47. Attached and marked Exhibit A to the same affidavit of Joseph Iuso, filed in these proceedings, is a copy of the actual presentation made by Iuso to the CPA and the Scotiabank representatives present. The presentation clearly demonstrates that the Customer types in heir confidential bank password and bank card number during the encrypted browser session, and then, acting as the agent of the Customer, GPAY enters the Customer's account in order to complete the Customer's payment instructions for the future goods or services being acquired by the Customer from the Applicants' merchant client (each a "Merchant").

48. In the numerous conversations and meetings between Grace and Scotiabank account manager, Woodrow, Grace never disguised the manner of operation of the

Applicants although, in so far as Grace recalls, Woodrow never made specific inquiries as to the manner and source of the transactions being processed through the Applicants' accounts.

49. Scotiabank is on the record as being fully educated as to the business model of the Applicants. Stating today, that the business of the Applicants is incongruous with a 1999 account application form is no violation of any law or policy, and is certainly not grounds to deny service to the Applicants. Denying services on these grounds is illegal under the Act.

(iii) BANK POLICIES DO NOT JUSTIFY EXCLUSIVE DEALING: Rosatelli: paragraphs 15-30

50. Rosatelli is astonished (at paragraph 21of his affidavit) that Grace caused approximately one hundred (100) accounts to be opened with the Respondent. As will be discussed later in this affidavit, that number of accounts was required in order to avoid computer malfunctions in the internet baking system of the Respondent.

51. While it may be unusual for an individual to open a hundred accounts at a bank, the reasons for opening these accounts were discussed with Woodrow. Woodrow checked with officers in the bank outside of the branch and found that there was no restriction on the number of Money Manger for Business accounts that a business could open.

52. The reasons for opening the one hundred (100) accounts were stated in writing in Grace's letter dated March 24, 2005 to Woodrow included in Exhibit "**B**" hereto. The Scotiabank only provided paperless statements for the Money Manager for Business accounts. A paper statement was not an option. When more than one hundred (100) transaction have gone through the account in a one (1) month period subsequent transactions need to be posted manually.

53. One of the problems with this Scotiabank system is that the online balance is sometimes incorrect or out dated. The other problem is that customers cannot see their transactions online for previous days and months

54. The only reason that we had multiple accounts instead of say only two (2) accounts per profile was to protect the Scotiabank. There were no sinister reasons. We limited the number of deposits to twenty (20) per day and ceased deposits at ninety (90) per month for each account. We were depositing nine thousand (9000) EMT's per month in January 2005 and needed additional accounts to take the load.

55. Rosetelli read the letter, Exhibit "B", and is aware of the Scotiabank online banking system shortcomings. Non the less Rosetelli suggested in his affidavit that there was some sinister reason for Grace to open the 100 accounts. One must think about his real motivation.

56. Indeed it was the great success of the business of the Applicants, coupled with the specifications of the computer systems of the Respondent that required a large number of accounts to be opened by the Applicants.

57. The Applicants take the position that the number of accounts and the period of time over which they were opened give no reason what so ever for the Respondent to deny service to the Applicants. Indeed, the Applicants believe that it is the success of the Applicants, as evidenced by the numerous and active accounts, that drew the attention of the Respondent to try to put an end to the business of the Applicants and concurrently launch its own competing business, Interac Online.

58. Concerning the number of bank cards (Rosatelli, paragraph 27), it is apparently Scotiabank policy to give a bankcard to the customer when the customer opens an account at the branch.

59. Grace did not refuse Woodrow, an officer of Scotiabank, when he gave Grace the first batch of 28 bank cards in October or November 2004. Woodrow never remarked on the number of cards, why should Grace have done so and why should the Tribunal?

60. It seemed routine banking to issue a card for each account. Surely, the Respondent does not expect its customers to second guess its officers.

61. It may interest Rosatelli and the Tribunal that, as matter of fact, Grace never did picked up the bank cards for the remaining accounts that he opened. Rosatelli misleads the Tribunal when he omits the fact that his bank is actually in possession of ninety (90) bankcards issued in the names of the Applicants.

62. The Responded alleges breaches by the Applicants of policies of the Respondent. For the record, neither Woodrow nor any other officer of the Respondent ever went through the individual clauses of the Financial Services Agreement between the Applicants and the Respondent with Grace or any other representative of the Applicants. The only discussion Woodrow and Grace had regarded the blanks in the paragraphs that had to be filled on the generic application forms and then Grace signed the last page.

63. Another point is that Scotiabank telephone banking was remiss in opening the 90 or so accounts in 2005 if it was Scotiabank policy for small businesses to be limited to 3 accounts. Is it possible that this was a local policy enacted only for the Sherwood Park branch of the Scotiabank.

64. Grace never read the Financial Services Agreement and never thought it would contain a clause that permitted the bank to cancel the Applicants' banking services without cause or to release the Scotiabank of any liability for damages to the Applicants for terminating the Applicants without cause.

65. While the Applicants maintain that they have not breached any laws or Respondent policies, it is to be noted that none of the numerous policies of The Bank of Nova Scotia that Rosatelli now cites in his affidavit were ever made known to or explained to the Applicants.

66. In the event that the Tribunal concludes that the Applicants breached bank policies, the Applicants pray that the Tribunal will consider the belief of the Applicants that those policies are drafted so as to preclude Scotiabank officers from servicing competitors of Scotiabank.

67. Scotiabank policies are not law. They serve the interests of the bank.

68. A policy to deny service to competitors is not grounds for exclusive dealing; it is an illegal and brazen example of it.

(iv) "FLURRY OF ACTIVITY" BY APPLICANTS CAUSED BY SCOTIABANK SOFTWARE DEFICIENCY Rosatelli: paragraphs 23-30

69. Grace accepts the dates that Rosatelli cites in these paragraphs as to when the majority of the Money Manager for Business Accounts ("**MMfb**") were opened.

70. The Applicants do not, however, accept any suggestion that the opening of these accounts, or the number thereof, provides the Respondent with any legal basis on which to deny service to the Applicants.

71. The following, as stated by Grace at paragraph 51 of the Grace Affidavit, is a summary of the chronological events that arose, that forced the Applicants to open more than one hundred (100) MMfb accounts - at great inconvenience to the Applicants.

a. In or about the week of September 20, 2004, I transferred funds from my Scotiabank MMfb accounts to my Scotiabank current account.

b. At or about 7:45 p.m. on Friday, September 24, 2004, I saw that our main Scotiabank account, the GPAY account, was in overdraft, for approximately $95,000.00.

c. On Monday, September 27, 2004, I went into the Scotiabank branch at 9:45 a.m. to speak with Woodrow about the overdraft. Woodrow told me was aware of it but could not tell me the cause nor was he able to look up the previous transactions on his bank computer terminal to show what happened to cause the account to go into overdraft. He offered to investigate it and let me know.

d. I wanted to remedy the overdraft as soon as possible.

e. In the interest of maintaining my good relationship with the Scotiabank and because, if it was my fault, I wanted to correct it immediately, and if it

was a bank error, I knew I would get the money back sooner or later, I immediately transferred $20,000.00 from one of my Scotiabank MMfb accounts to the overdrawn account.

f. I also and gave Woodrow a cheque drawn on my Bank of Montreal account for $75,000.00, which I offered to have certified but Woodrow indicated was not necessary.

g. Woodrow's acceptance of a $75,000.00 uncertified cheque exemplifies the well informed and trusting relationship to which I have been accustomed at Scotiabank.

h. A week later, after Woodrow had done some investigating, he advised me that he could only conclude the Calgary accounting department of Scotiabank was responsible for the over draft.

i. There were two recent $87,000.00 transactions through the account. One was a debit reducing the balance. The other was an offsetting credit that was negative and consequently reduced the account balance again, perhaps because my maximum electronic transaction size was $49,999.99.

j. The Scotiabank Calgary accounting department insisted that the account was balanced and no refund was due. I had done some reconciling and determined that there was a possibility that we were balanced. I dropped the issue to preserve my relationship with the Scotiabank. At this time Woodrow told me to wait until the end of the month and the branch would order a paper statement.

k. As it happens, the Scotiabank has never been able to provide me with a bank statement for that month, even to the present date.

l. Woodrow was able to find out and advise me that a scotiabank officer outside of the branch, and I assumed that they were in Scotiabank's IT (information technology) department told him their online system for

MMfb accounts could handle a maximum of approximately 30 transactions per day and 100 per month.

m. The problem with exceeding 100 transactions a month was that the statement of previous transactions for the current month and, in some cases, previous months became unavailable. Our MMfb statements are paperless so the statement was available online only.

n. A paper statement was unavailable but the branch could print a transaction history at the end of the month.

o. **In an effort to PROTECT the BANK from ITS OWN SOFTWARE shortcomings**, and out of an abundance of caution, I began to limit the number of transactions into each MMfb account to 20 per day or 90 per month.

p. I advised Woodrow about my new self-imposed limitation.

q. Woodrow checked Scotiabank policy in October 2004 and informed me that I could open as many MMfb accounts as I needed.

r. I asked Woodrow to open up the NPAY Inc.'s business accounts and B-Filer Inc.'s business accounts in October and November 2004, respectively, to handle the existing volume and the anticipated increased volume of the Applicants' businesses.

s. I needed one (1) current account to transfer funds out of the Scotia bank. The current account was linked to the MMfb accounts that were receiving funds from our customers. The current account bank card was linked to the MMfb accounts.

t. My practice, which was well known to the Scotiabank, was to deposit a maximum of 10-20 payments a day into each of the MMfb accounts. Once 90 payments were reached, we ceased to use that account for deposits for the rest of the month and moved on to the next MMfb account. This

limited the total number of transactions in any one account to 20 per day or 90 per month. This was an amount that the Scotiabank software could handle and still provide a transaction history online without crashing.

u. I explained to Woodrow in October and November of 2004 why I needed to open more MMfb accounts. Understanding our need, he kindly opened approximately 28 of the accounts for me.

v. The accounts were all linked to the bankcard of the current account for each Plaintiff. We only needed one card to access all of the accounts for each Plaintiff.

w. The approximately 90 accounts that I opened online in 2005 were to respond to the increased volume of our business.

x. We were now processing more than 9000 EMT's a month.

y. **Our one hundred (100) or so accounts were opened for the sole purpose of PROTECTING the BANK from ITS OWN SOFTWEAR deficiencies.**

z. The Applicants actually underestimated their growth rate because on or about January 4, 2005, three (3) of the Bfiler accounts of the Applicants again went into overdraft for approximately $14,000.00 each. Responding promptly to the problem, the Applicants opened additional MMfb accounts to ensure the Scotiabank software program limitations were averted.

aa. I discussed our expansion plans with Margaret Parsons, the Scotiabank branch manager at the branch serving the Applicants, from time to time.

bb. The Applicants and Grace hid nothing from Scotiabank.

72. Rosatelli (at paragraph 30 of his Affidavit and elsewhere therein) appears to be surprised by the enlightened services rendered by his own bank to the Applicants. The

Applicants assure the Tribunal that nothing in the affairs of the Applicants with the Respondent was a surprise to the Respondent. On the contrary, the Respondent was helpfully involved in the day to day substantial banking requirements of the Applicants.

73. The Respondent appears to wish to deny service to the Applicants because it claims to have been ignorant of the workings of the Applicants. The claim of ignorance by the Respondent in this regard is simply false.

74. Indeed, being all too familiar with the business of the Applicants, the Respondent conspired to both extinguish the business of the Applicants and launch its own identical and competing substitute service, Interac Online.

(vi) ANOTHER EXAMPLE OF THE APPLICANTS' GOOD RELATIONSHIP WITH SCOTIABANK

75. From reading Rosatelli and the Response, one might have thought that the Applicants did not have a good, healthy, mutually informed baking relationship with Scotiabank. Actually, they did.

76. As an example of this good relationship, Grace went into the Sherwood Park Scotiabank branch on or about January 7, 2005 and asked them do make up a bank draft on a GPAY account for $154,000.00.

77. The bank draft should have been made payable to GPAY but, in error, the teller made it payable to Ray Grace, personally. When Grace pointed out the mistake, the teller called the bank manager, Margaret Parsons, over.

78. Mrs. Parsons initialed the draft and assured Grace there was no need to change it into the company name as he could simply endorse it and deposit it.

79. Grace pointed out a $45,000.00 overdraft that would follow from cashing the cheque and said that he was leaving $50,000.00 in another one of the accounts to cover the apparent overdraft "just in case".

80. It should be noted that this overdraft was caused again by an error in the software of Scotiabank that failed to record all of the transactions correctly and display the correct online account balance.

81. Grace was left with the impression from Mrs. Parsons, his Scotiabank branch manager, that these events were: (a) no big deal for her and the Scotiabank, and (b) that this happens from time to time and Scotiabank's Calgary accounting department would sort it out eventually.

III. THE APPLICANTS DO NOT CAUSE THE SCOTIABANK CUSTOMERS TO BREACH THEIR CARDHOLDER AGREEMENT

82. **Rosatelli: paragraphs 12, 61-88** – The Respondent argues in the Response that it is justified in denying service to the Applicants because the Applicants allegedly cause customers to breach their cardholder agreements with Scotiabank.

83. First, it is a question of law as to whether the Applicants' manner of carrying on business causes Scotiabank customers to breach their Cardholder Agreement with the Scotiabank.

84. Attached and marked **Exhibit C** to the Grace Affidavit is a copy of the GPAY and UseMyBank Services Inc. Terms and Conditions. These terms (the "**GPAY Customer Terms**") constitute the agreement between each of the approximately 20,000 individuals who retain the services of the Applicants (each a "**Customer**") and the Applicants.

85. Section 4 of the GPAY Customer Terms states:

> "**Your authorization of UseMyBank services.** Online accounts access is provided by you from the Transaction Providers. By providing Login Information, you authorize UseMyBank and its facilitation service to act as your agent to access, retrieve your Account Information, and make bill payments or email money transfer from the web sites of your Transaction Provider site on your behalf. You hereby grant UseMyBank and its facilitation service a limited power of attorney, and you hereby appoint UseMyBank and its facilitation service as your true and lawful attorney-in-fact and agent, with full power of substitution and resubstitution, for you and in your name, place and stead, in any and all capacities, to access Transaction Provider sites, retrieve information, and use your information, all as described above, with the full power and authority to do and perform

> each and every act and thing requisite and necessary to be done in connection with such activities, as fully to all intents and purposes as you might or could do in person. YOU ACKNOWLEDGE AND AGREE THAT WHEN USEMYBANK AND ITS FACILITATION SERVICE ACCESSES AND RETRIEVES INFORMATION FROM THE TRANSACTION PROVIDER, USEMYBANK AND ITS FACILITATION SERVICE ARE ACTING AS YOUR AGENT, AND NOT THE AGENT OR ON BEHALF OF SUCH TRANSACTION PROVIDER. You agree that the Transaction Providers will be entitled to rely on the foregoing authorization, agency and power of attorney granted by you to UseMyBank. You also authorize UseMyBank and its respective authorized agents and assignee's to receive your Information, to provide that information to its facilitation service in accordance with the terms of the UseMyBank Privacy Policy Statement. UseMyBank is not responsible for any fees that are associated with the facilitation of this services as it relates to Bill Payment or email money transfer through the Transaction Provider and/or third parties."

86. By operation of the GPAY Customer Terms, the Applicants, at law and in fact, become the agents on behalf of the Customer for the purposes of carrying out Customer instructions.

87. The 20,000 or so Customers of the Applicants appoint the Applicants to assist in instructing their respective banks to effect transactions.

88. In so far as the Applicants are aware, the law of agency is alive and well in Canada, and does not end at the Scotiabank doorstep.

89. Indeed, it is customary in Canada for individuals to instruct others to act for them in all areas of business. Banking is no exception.

90. At law, when an agent acts for a principle, it is as if the principle themselves acted. As such, when the Applicants, *qua* agent for a Customer, deliver instructions to a bank, from the perspective of the bank, it is as if the Customer themselves delivered the instruction.

91. As such, the argument that Customers breach their cardholder agreements by disclosing passwords is false. By mandate from the Customer, the Applicants are the Customer.

92. Rosatelli states, at paragraph 10 of his affidavit, that the agreement between the Bank and the Customer stipulates that if the Customer discloses his PIN or user identification number, then the Customer is responsible. Curiously, Scotiabank takes no

further action to ensure that the Customer does not actually disclose their PIN. In fact, Scotiabank is well aware that Customers routinely disclose PINs and passwords to their children, etc...

93. If keeping a PIN or password is truly so important to the security of the whole Canadian banking system as the Respondent alleges, then why doesn't the Bank have additional security in place to determine who actually is using the customer's bank card? The reality is that the banks knowingly condone their Customer's alleged breaches of this clause and they simply pass the liability for doing so on to their Customers, collectively.

94. Taking this discussion one level deeper, none of the Applicants' employees or contractors ever come into actual knowledge of any confidential information of the Customer. Customer information is inputted into software of the Applicants by the Customer in a secure, encrypted browser session. That same, secure and encrypted information is then relayed to the bank of the Customer where the instructions of the Customer are ultimately carried out.

95. When the browser session is closed, after no longer than 2 minutes, the **confidential Customer information is NOT STORED**. The Customer then deals directly with the Merchant to acquire whatever goods and services they desire.

96. Reading the Response might lead one to conclude wrongly that the cardholder agreement is breached or that security of the cardholder information is somehow compromised. Neither is true.

97. The Applicants method of doing business actually gives greater security to the movement of funds from a bank Customer's account because, in the browser session that instructs the transfer of funds, the Applicants' security systems verifies that the Customer who is giving the instructions is actually the Customer who owns the bank account and can also identify from which computer site the Customer is giving the instructions.

98. For any given interaction with their online banking system, Scotiabank cannot state with much certainty who is actually performing the banking. The Applicant's system is much more secure than that of Scotiabank.

99. If any of this information supplied by a Customer to the Applicants is contradictory, the Applicants attempt to contact the Customer directly by telephone to double check the transaction. The Applicants also contact each of their first time Customers to ensure they intend to open a relationship with the Applicants.

100. Whether or not the Applicants have been successful in contacting the Customer, the funds are flagged by the Applicants, and set aside for refunding, if necessary. If the computer IP (internet protocol) address is different, the Customer could be on holidays (which explains a different computer) or again, it could mean that the Customer's account information has been compromised.

101. The banks, such as the Respondent, have no such security in place and can only detect frauds after a Customer complains, upon review of the activities in their bank statement. The banks have fraud prevention and reporting departments. The Plaintiff's have a real-time fraud detection system that protects the Canadian public. Compromised bank accounts are discovered and reported to the Customer's bank, within hours, sometimes within minutes, instead of days.

102. For a fraudulent transaction to succeed using the Applicants services, the fraudster must evade the fraud prevention systems of the Applicants as well as those of the Respondent. In other words, the Applicants actually enhance the security of banking for the Customer rather than decrease it.

103. The Respondents are self insuring for fraud matters. They have fraud prevention departments and fraud reporting departments. They do not, however, have real-time fraud detection departments or systems in place. The Applicants have these in place. The Applicants do not pretend that they can stop fraud or detect every fraud that is perpetrated against them.

104. The Applicants contend that they have methods to detect possible fraud in place that they do not want to disclose in a public document.

105. The Applicants would be willing to provide a sealed affidavit with the details for the Tribunal and the Respondent to peruse. These systems and procedures allow the

Applicant to detect possible fraud and protect the financial institutions from a loss. Losses not caught by security systems, such as those of the Applicants, are passed on to the Canadian public in increased fees and reduced services.

106. The Applicant contends that they are a benefit to the Canadian public for reducing fraud, reducing the time a bank's Customer's information is at risk, and providing information that allows the various banks' security departments to identify other unreported at-risk accounts sooner.

107. The Response includes a flurry of verbiage about terrorism, money laundering, and security breaches. This flurry will be addressed more fully below, but it is pertinent to mention here, the belief of the Applicants that those lines of argument are intended by the Respondent to be alarmist and to obscure the true pith of this matter, which is one of a monopolistic player eliminating a supplier in a defined market and simultaneously launching its own identical service, Interac Online.

108. In flagrant breach of the Act, having little else on which to argue, the Respondent liens on unfounded and alarmist allegations that the Applicants pray will not divert the attention of the Tribunal from the call of the Act to these facts.

IV. THE APPLICANTS ARE NOT IN BREACH OF CANADIAN PAYMENTS ASSOCIATION (CPA) RULE E2

109. **Rosatelli: paragraphs 97-110** – The Respondent alleges that the Applicants are in breach of CPA Rule E2.

110. CPA Rule E2 specifically prohibits banks from clearing items under that Rule in circumstances where the banking customer's authentication information such as user identification and password have been made available to the payee, during the on-line payment transaction session.

111. Before explaining why the Applicants are not in breach of CPA Rule E2, it must first be stated that CPA Rule E2, as with all CPA Rules, applies to CPA members. The Applicants are not members of the CPA.

112. The Applicants have had several meetings with the CPA. The Applicants are not eligible to join the CPA because they are not a bank or a credit union. Iuso has, nonetheless, attended many of their meetings to keep abreast of recent issues, identify current problems (e.g. CPA admits that fraud is an ongoing problem) and to maintain communication with their members and other attendees.

113. By invoking a rule that does not apply to the Applicants as justification for refusing to serve them, the Response comes up empty, again.

114. Subsidiarily, the Applicants wish to explain why, even if CPA Rule E2 did apply to them, they would be in perfect conformity with its requirements. The Applicants base this position principally on the following:

a. The Applicants are not the ultimate payee and none of their Merchant clients receive any personal financial information about the Customer. In other words, the Merchants do not receive what CPA Rule E2 forbids them to receive.

b. The Applicants state are agents of the Customer and so are not in violation of this rule, because the Applicants act *qua* agent *qua* Customer.

c. The Applicants specifically deny that the user identification and/or password are made available to them by their Customer. As discussed above, the information is made available to the Applicants' computer software in an encrypted browser session and no live person of the Applicants ever learns the actual confidential information.

d. The procedure employed by the Applicants is to have the customer type in their password and user identification which is sent back to the Applicants' SOFTWARE PROGRAMME (i.e. never to a real person) by way of encrypted code which is then effectively "bounced back" - again in the same secure browser session - to the Customer's bank, to enable the Applicants to watch the Customer's bank debit the Customer's account for the specified amount. In observing the transaction, the Applicants are able

to verify the name and address of the account holder and compare it to their Customer's name and address as an additional security measure for the Customer.

e. **The Customer's user ID and password are NEVER stored on the Applicants' servers or seen by a live person. Once the session is closed, the information is gone. NO PERSON FROM THE APPLICANTS EVER PERSONALLY SEES THE USER IDENTIFICATION NUMBER OR BANK CARD NUMBER OR ANY OTHER AUTHENTICATION INFORMATION.**

f. As a further subsidiary argument, CPA Rule E2 was adopted in February of 2005, long after the implementation of the business of the Applicants. As such the Applicants believe that they have an acquired right to continue operating as they have and not be put out of business by a Rule adopted by CPA members, such as Scotiabank, implementing Interac Online to capture the market now held by the Applicants. The banks can't have it all.

g. The Applicants state that there are several other businesses – for example, Yodlee, CashEdge (which Grace believes is partly owned by The Royal Bank of Canada) and Citadel which all go further than the Applicants and actually RECORD bank card and passwords. These other businesses that are very similar to that of the Applicants are operating without threat of closure by Scotiabank or the CPA for violating CPA Rule E2 or any other rule. Yodlee, in fact, boasts that it has 4 million recorded bank cards and password ON ITS SERVERS. This is a much greater danger to the Canadian Banking industry than the Applicants.

V. THE APPLICANTS DO NOT - AND NEVER HAVE - TRANSFERRED MONEY FROM THEIR SCOTIABANK ACCOUNTS TO OFF-SHORE INTERNET GAMBLING SITE

115. **Rosatelli: paragraph 13** – Rosatelli alleges that the business of the Applicants is to transfer Customer funds to off-shore internet gambling sites. This is false.

116. The Applicants have never transferred money from Customers' Scotiabank accounts to off-shore internet gambling sites. The Applicants require strict proof of this allegation by the Respondent.

117. The Applicants submit that what the Applicants do with the Applicants' Customers' funds from a bank other than Scotiabank is solely between that bank and the Applicants and is not relevant to these proceedings.

118. **Rosatelli: paragraphs 45-49** – As a matter of fact, the Applicants never know exactly what goods or service the Customer is acquiring from the Merchant.

119. When a Customer is dealing with an off-shore internet casino Merchant, the service offered by the Applicants is to ensure that the funds the Customer wishes to pay to that Merchant are removed from the Customer's account and the Merchant is advised of this in virtual real time. Title in those funds and what becomes of them are a matter strictly between the Customer and the Merchant.

120. When a Customer of the Applicants wishes to engage in a transaction with a Merchant, the amount of the transaction is taken from the Customer's bank account only after the Customer has appointed the Applicants as his agent to enter his account and complete the customer's instructions by either emailing (i.e. by EMT) or paying the Applicants as a "bill payee" the authorized amount to the Applicants' account.

121. This EMT is recorded by CertaPay (which is a software company whose business is facilitating email notifications), who virtually instantaneously, notifies the Applicants that the money has been debited from the Customer's account. The CPA is a not for

profit organization created by an Act of Parliament in 1980. It operates the national system for the clearing and settlement of payments. The CPA is the entity that actually "moves" the money from the Customer's account into, Applicants believe, a suspense account of the sending bank.

122. Once the EMT is accepted, into a suspense account at the recipient's bank, which then deposits the funds into the Applicants' designated account. The Applicants, acting as the Customer's agent, merely authorizes the transaction to CertaPay and does NOT physically remove or transmit the funds.

123. The Respondent appears in the Response to tower over Canada, liberally dispensing judgment over what Canadians should or should not do with their money. The Applicants, that pass no judgment over their Customers or any other Canadians, are caught up in this flurry of adjudication which serves as a thin veil for Scotiabank's true intent of extinguishing the business of the Applicants and illegally implementing its own substitute, Interac Online.

VI. THE MONEY LAUNDERING QUESTION

124. **Rosatelli: paragraphs 5-53, 55-59** – The Respondent expresses concerns over money laundering possibly being facilitated by the business of the Applicants. The Applicants will illustrate below how: (a) this is false; and (b) Scotiabank is heavily invested in both off-shore internet and offshore brick and mortar gambling in a way that is an invitation to money laundering.

125. The Financial Transactions and Reports Analysis Centre of Canada ("**FINTRAC**") is Canada's financial intelligence unit, a specialized agency created to collect, analyze and disclose financial information and intelligence on suspected money laundering and terrorist activities financing.

126. Grace spoken to FINTRAC on several occasions during which he explained the payment and fund flow procedures of the Applicants.

127. The Applicants have never been charged or sanctioned by FINTRAC or any other law enforcement agency in Canada or elsewhere.

128. In the course of providing their services, the Applicants do not accept cash, cheques, money orders, wire transfers, deposits, negotiable instruments or credit cards as payment for goods and services.

129. The only way a Customer can make a payment to a Merchant with the Applicants is to make the payment at the Merchant website using a bank debit card.

130. The use of the bank debit card identifies the payor or Customer. Each bank debit card, by its very nature, was issued by a bank that saw picture identification and proof of residency of its holder before it was issued.

131. As agent for the Customer, the Applicants notify the Merchant the payment has been made within seconds of the payment. The Merchant relies on this information and provides the Customer with instant credit to their account for the amount paid.

132. As per our agreement with the Merchant, we instruct a bank to remit funds to the Merchant at a later time. The funds are always deposited into a bank account electronically. We never send a Merchant a cheque, money order, or cash.

133. Pursuant to customary banking security protocol, the onus is on the receiving BANK to know their customer and identify them as a non terrorist, non money launderer and non criminal. The onus is on the receiving BANK to know the source of any large amount of money their customer deposits into their account, but only when the source of the funds is a cash, cheque or money order deposit. Money sent electronically from one Canadian bank customer's account to another Canadian bank customer's account (ie an EMT or online bill payment) DOES **NOT** RAISE CONCERNS OF MONEY LAUNDERING OR FUNDING TERRORISM.

134. FINTRAC informed Grace that the Applicants do not fall into their reporting sphere because they do not deal with cash or any non electronic form of payment. Everything the Applicants do is traceable.

135. The Applicants do accept Scotiabank appointing itself as a Canadian law enforcement agency.

136. As per the Applicants' agreement with our Merchant, if the payment is flagged by the Applicants (because the GPAY security system suspects a fraud), the Applicants notify the Merchant to hold off giving the customer credit. The liability for the funds rests with the Merchant if it allows the customer's business to proceed after the payment is flagged. If the Applicants subsequently discover the payment was fraudulent, the Applicants reimburse the Customer's bank (who refunds it to the Customer) and notify the bank's security department (and occasionally the police) with the details of the fraud.

137. Indeed, to facilitate in this kind of reporting, the Applicants are very much in need of the Respondent appointing an account manager, so that the Applicants can speak to Scotiabank and find out what information they have regarding any alleged fraud.

138. The Applicants have detected about no less than twenty (20) frauds in 2005 totaling approximately $7,000.00. In each case, the fraud would not have been detected by the Customers' banks but for the Applicants. In each case, the Applicants refunded the sending bank.

139. The Applicants have a cutting edge fraud detection system.

140. The Applicants are have offered to fully indemnify the Scotiabank from any loss arising from any reported fraud. The Scotiabank has rejected this offer to date.

(a) SCOTIABANK IS ALSO IN THE BUSINESS OF DEALING WITH OFF-SHORE CASINOS - The Pot Calling the Kettle Black – Part One

141. More than half of the argument of the Respondent rests on the fact that certain of the Merchants procuring the Applicants' services are off-shore casinos.

142. However, the right of a person in Canada to provide information services and to facilitate payments by a Canadian to a casino is not at issue before the Tribiunal in this case. The right of the Respondent to terminate the banking services of the Applicants because of their alleged payments to casinos is very much at issue before the Tribunal.

143. More specifically, the right of the Respondent to exclude the Applicants from dealing with the Respondent on account of the Applicants' supply of services to certain casinos is open for judgment under the Act in this case.

144. The Applicants do not argue that two wrongs make a right. However, if the involvement of some of the Applicants' Merchants in gambling is the basis for the refusal of the Respondent to supply banking services to the Applicants, then, in making that argument, the Respondent is in breach of the very same complaint.

145. The Respondent owns or has invested material funds in the following offshore and domestic casinos (collectively, the "**Scotiabank Casinos**"):

a. Caesars Palace – Las Vegas

b. Caesars Palace – Lake Tahoe

c. Caesars Atlantic City

d. Aladdin resort & Casino – Las Vegas

e. MGM Grand – Las Vegas

f. St Kitts Marriott Resort & The Royal Beach Casino – **British West Indies**

g. Lima Marriott Hotel and Stellaris' Casino – **Lima, Peru**

h. Resort & Casino at Bahamia – **Freeport, Bahamas**

i. Harrah's Cherokee Casino – North Carolina

j. Atlantis Paradise Island - **Bahamas**

146. Attached and marked **Exhibit "D"** to the Grace Affidavit is a page summarizing the Scotiabank's involvement with each of the Scotiabank casinos.

147. In contrast, none of the Applicants, or any of their affiliates, have invested in or own any casinos. As such, if participation in casinos is a matter of such great concern to the Respondent, the Respondent should, perhaps, turn its gaze inward.

148. The Applicants submit that the Scotiabank Casinos generate material (and welcome) revenue for the Respondent.

149. Earning revenue from offshore and other casinos and arguing that earning that very kind of revenue is valid grounds for refusal to supply banking services to the Applicants is, perhaps, the perfect proof of the malevolent motivation of the Respondent. The position of the Respondent on this point is strikingly contradictory and abundantly hypocritical.

150. These facts make the case of the Applicants under the Act.

(b) Scotia Visa Internet Gambling: The Pot Calling the Kettle Black – Part Two

151. The Respondent is a member of the Visa credit card bank association.

152. The Respondent issues Visa credit cards to certain of its customers (each a **"Scotia Cardholder"**).

153. There are millions of Scotia Cardholders in Canada and elsewhere in the world.

154. Whenever Scotia Cardholders use their Scotiabank Visa card to purchase goods or services, the Respondent earns a majority of the fees charged to the merchant where the card is used.

155. For example, if a Scotia Cardholder buys a $20.00 book at Chapter's, Chapter's will receive something less than $20.00, perhaps, $19.50. The $0.50 difference between the amount paid by the Scotia Cardholder and the amount received by Chapter's

represents a fee (the "**Scotia Visa Fee**") charged by the Respondent and the bank assisting Chapter's in receiving funds from the Scotia Cardholder.

156. The general practice among Visa member banks is to share the Scotia Visa Fee, paying approximately eighty percent (80%) thereof ($0.40 in the example set out above) to the Respondent, as an issuing bank, and approximately twenty percent (20%) thereof ($0.20 in the example set out above) to the acquiring bank, being the bank assisting Chapter's in the example above.

157. It may come as a surprise to the diligent Scotia Cardholder that, even if they pay every monthly Visa bill on time, the Respondent is actually still earning approximately eighty percent (80%) of all Scotia Visa Fees incurred in the use of the card.

158. As such, the Respondent earns Scotia Visa Fees on millions of Visa cards in circulation. The aggregate amount of Scotia Visa Fees earned by the Respondent on an annual basis is not public information, but is estimated to be in the tens of millions of dollars per year. The Applicants believe a substantial portion of that revenue is from online off-shore internet gambling purchases by Scotiabank Visa cardholders.

159. Among the millions of Scotia Cardholders, there are, perhaps, a few hundred thousand, or a million, Scotia Cardholders who enjoy online offshore gambling by using their Visa cards issued by the Respondent.

160. As with all Scotia Cardholder transactions, such as the purchase of a book at Chapter's, the Respondent earns eighty percent (80%) of all Scotia Visa Fees levied on online offshore internet casinos (the "**Scotiabank Online Casino Revenue**").

161. The Applicants believe the Scotiabank Online Casino Revenue to be in the tens of millions of dollars per year. Believing this to be true, the Applicants were naturally surprised to read in the Rosatelli Affidavit that "Scotiabank refuses to have its brand associated directly or indirectly with companies which engage in illegal activities, such as off-shore Internet gambling."

162. Evidently, Scotiabank profits come from places where its brand would rather not be seen.

163. The Respondent may argue that it is wholly unaware of any Scotiabank Online Casino Revenue. As a matter of fact, the Respondent is very much aware of the precise sources of its Scotiabank Online Casino Revenue because, Grace believes, each Scotia Cardholder online casino transaction is branded with a unique code, thereby disclosing to the Respondent not only the kind of transaction, i.e. offshore internet gambling, but also the precise identity of the merchant.

164. Attached and marked **Exhibit E** to the Grace Affidavit is a copy of a Scotiabank Visa statement showing that one of the Respondent's customers made a payment to Pokerstars Internet Casino, an off-shore internet casino, for USD$400.00 (CDN$491.60) on August 25, 2005.

165. At paragraph 132 of the Rosatelli Affidavit, Rosatelli states "Scotiabank will have no involvement in transferring money to internet gambling sites." Despite this assertion, Scotiabank transferred CDN$491.60 to the Pokerstars Internet Casino internet gambling site on August 25, 2005, as evidenced by Exhibit E to the Grace Affidavit. Rosatelli is either grossly ignorant of his bank's true policies and practices or his affidavit is false.

166. Indeed the ever-present Visa logo on almost any offshore internet casino, such as those diligently recorded by the Respondent in their Response, (see, for example, Exhibit D of the *Google* searches in the Rosatelli Affidavit), acts as an invitation for Scotia Cardholders to use their Visa cards issued by the Respondent and earn Scotia Online Casino Revenue for the Respondent.

167. By these facts, the Respondent's decision to cease providing banking services because the Applicants allegedly deal with off-shore online casinos is illegal under the Act. The Respondent earns substantial revenue form off-shore online casinos thereby nullifying such revenue as valid basis on which to deny service to the Applicants.

168. The Respondent can't have it all.

VII. ROSATELLI AFFIDAVIT IS INFLAMMATORY AND MISLEADING

169. The Rosatelli Affidavit expresses concerns over alleged facilitation of money laundering by paying off-shore Internet gambling sites by the Applicants, no less than 17 times (see paragraphs 13, 13(a), 19(g), 46, 48, 50, 51, 52, 55, 56, 58(a), 67(b), 151, 152,153I(e), 155 and 160(b) thereof). **There is, however, not a single example, in the 1,000 page Response, proving the Applicants have facilitated money laundering.**

170. In the Respondent's own affidavit at paragraph 58(a), he confirms that Money Services Businesses in Canada are required to comply with Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations. Money Services Businesses are in fact regulated businesses, but not by the banks.

171. The Rosatelli affidavit expresses concerns over alleged facilitation of terrorism by the Applicants, no less than 6 times (see paragraphs 19(g), 51, 56, 58(b), 58(d) and 160(b) thereof). **There is, however, not a single example, in the 1,000 page Response, proving the Applicants have facilitated terrorism.**

172. For the record, none of the Applicants or their affiliates are money launderers, terrorists, or knowingly facilitators thereof; none of them have ever been money launderers, terrorists or facilitators thereof; and, none of them intend to ever be money launderers, terrorists or facilitators thereof. All allegations of such activity or any other illegal activity made in the Rosatellli Affidavit are false.

173. The Scotiabank is a Schedule 1 bank, one of the big 5 banks in Canada, and currently, the most international bank in Canada. When Scotiabank makes false allegations about the character of a good corporate customer of theirs, this causes ripples in the business and security communities.

174. Even after the Scotiabank later announces that the unfounded allegations in the Rosatelli Affidavit are false, the damage to the Applicants is already done.

175. Applicants submit that the Respondent is supplanting Canadian law enforcement agencies and violating the Applicants' rights to defend themselves by due process wherein the standard of proof to be met by the accuser is beyond a reasonable doubt in an open court of law.

176. **The Respondent's unilateral judgment of the Applicants' business is equivalent to the Respondent acting as investigator, prosecutor, judge and executioner – all without a hearing – and contrary to the rules of natural justice.** The judgment is also *ultra vires* the charter of the Respondent.

177. Taking the lead of the Respondent, the Applicants will briefly address opportunities for money laundering and the financing of terrorism raised by the Respondent in this case.

178. All credits and debits to and from accounts of the Applicants in the course of supplying the GPAY Services are electronic.

179. Electronic transactions leave records of every detail concerning the transaction including, without limitation, payor, payee, amount, date, time, currency, quantum and method of transfer. In so far as the enforcement of money laundering and anti-terrorism legislation is concerned, the business and affairs of the Applicants are completely transparent and known to law enforcement agencies and regulators having an interest in such matters. Indeed, if all businesses were based on only electronic payments, like those of the Applicants, we would live in a much safer world.

180. The intent of money laundering legislation and anti-terrorism legislation is to ferret out secret transfers of funds, usually done in cash. The Applicants never deal in cash, and can identify each and every Customer and Merchant using their services. Not only can the Applicant identify each of its Customers and Merchants, but so can the Respondent. Nothing in the business of the Applicants is a secret to the Respondent or any law enforcement agency.

181. In contrast, the Respondent deals in vast quantities of cash. The Respondent actually knows much less about the source of its cash deposits than does the Applicants about the source of its Customers' funds.

182. The Respondent argues that the Applicants are somehow making it easier for money laundering and terrorism to take place (see paragraphs cited above). The electronic nature of the business of the Applicants averts any uncertainty as to the payors or payees of funds, and is in fact a model business for assistance in law enforcement in this regard.

183. The Respondents also argue that offshore internet gambling is especially prone to abuses by money launderers or terrorists. As a matter of fact, if we are to compare the Applicants to the Scotiabank Casinos, the latter of which accept cash, we come quickly to the realization that the Respondent is directly invested in the one kind of casino most used and most attractive to money launders and terrorists; a cash-based casino, like the Scotiabank Casinos.

184. The Applicants submit that the specific nature of its Merchants, SOME of which are offshore internet casinos, cannot be used by the Respondent as a valid basis on which to terminate the Applicants' banking services, because the Respondent is, indirectly through the Scotia Casinos, one such merchant itself. What is more, Scotiabank earns material revenue from that kind of merchant thought its Visa cards.

185. As the owner and material investor in numerous casinos, the Respondent is much more likely, knowingly or unknowingly, assisting money launders and terrorist because it deals in vast and untraceable quantities of cash at its owns brick and mortar cash-based casinos.

186. The Applicants are compliant with all applicable laws and, respectfully submit, the Tribunal has no mandate to decide on the legality of offshore internet gambling in Canada or elsewhere in this case. It is, however, for the Tribunal to prevent a monopolistic participant in the online payments market in Canada to terminate the

banking services of the Applicants on grounds, or high principles, that it clearly does not apply to other customers, itself or its affiliates.

187. The legislator enacted the Act for facts such as these.

188. The Respondent, The Bank of Nova Scotia, is rich with Scotia Visa card fee revenue from offshore internet gambling, as well as profiting from brick and mortar cash based offshore and domestic casinos. The Applicants find that justifying its termination of banking services based on the fact that some of its Merchants are casinos is a brazen textbook example of exclusive dealing.

VIII. APPLICANTS' MANNER OF DOING BUSINESS IS BOTH SAFE AND SECURE

189. **Rosatelli paragraph 80** – Rosatelli expresses concern over security in the systems of the Applicants. That concern is unwarranted.

190. Attached and marked **Exhibit F** to the Grace Affidavit is a copy of the Applicants' current and valid Security Certificate, which is not expired, as the Respondent might wish to allege.

191. The Applicants and UseMyBank have always been completely covered in their security certification. What Rosatelli attached as Exhibit L to his affidavit was a copy of a link from the UseMyBank Services, Inc. webpage which was a wrong link and has now been corrected.

192. The Applicants have invited the security people at the Scotiabank to come and personally inspect the security measures installed in the systems of the Applicants.

193. The Applicants are prepared to file an affidavit in these proceedings detailing their security upon issuance of an order by the Tribunal sealing such affidavit from being accessed by any member of the public and the Respondent providing its sworn undertaking to keep such information confidential, not disclosing same or not using such information in any manner whatsoever, competitive or otherwise.

194. The clientele of the Applicants are bona fide legitimate businesses that, to the knowledge of the Applicants, operate in conformity with the laws that apply to them.

195. Attached and marked **Exhibit G** to the Grace Affidavit is a list of other merchant clients of the Applicants - which is not a complete list.

196. While Merchant off shore casinos may form a large part of the Applicants' revenue transactions, off shore casino merchants are actually a very small number of the whole list of Applicants' merchants. The Applicants anticipate that, as more Merchants become knowledgeable and comfortable with the Internet, the number of non-casino merchants using their services will increase exponentially. Casinos were amongst the leading front of internet Merchants.

IX. RESPONDENT EXTINGUISHING COMPETITION

197. **Rosatelli: paragraphs 122-135** – The Response rejects the assertions in the Application that the termination of supply of the services of Scotiabank to the Applicants would have the effect of lessening competition in contravention of the Act.

(a) Interac Online

198. Interac Online and the GPAY Services are fungible.

199. The only material distinction between the two made in the Response is the allegation by the Respondent that the Customer inputs information directly into their bank system with Interac Online while the GPAY Services operate through the *de facto* intermediary of the Applicants.

200. As discussed above, *de jure*, the Applicants are the duly appointed agents of their customers. The Applicants are simply communicating Customer instructions to the bank of the Customer.

201. The Response suggests that because five (5) major Canadian banks happened to have created a system of EMT, bill payment and now Interac Online, that they should be

the only entities permitted to participate in this hugely profitable and narrow market sector.

202. The Applicants submit that even if Interac Online were not launched, the termination by the Respondent of services to the Applicants alone would constitute a breach of the Act. That termination alone, in light of the reasons therefore provided in the Response, reveal that it was wholly unjustified, as discussed above.

203. Rosatelli suggests that all of the Applicant's problems would be solved if they just applied to join Interac.

204. The Applicants joining Interac is not an option.

205. At the present time, Interac only offers connection services by way of POS and ATM's. Efforts have been underway to work through a third party, CU Connection, to have an indirect connection through an existing member of Interac to use Interac Online.

206. At this time the Applicants have been told that this option is not available. Until Interac provides a service that the Applicants can actually use, joining Interac does not make business sense for the Applicants. Contrary to Rosatelli's allegations, joining Interac is not an option.

207. The termination of the Applicants by the Respondent, on the one hand, and the nearly simultaneous launch of Interac Online removes any doubt as to the true intent of Scotiabank. The true intent of Scotiabank is to extinguish the Applicants as competitors in the online debit payment services market and introduce their own Interac Online service as a substitute.

(b) Bill Payee

208. The Applicants were, indeed, listed as a "bill payee" with each of the TD, CIBC, Alberta Treasury Branch, Bank of Montreal and Royal Bank customers. In or about late 2003, TD, CIBC and ATB unilaterally cancelled the Applicants as a "bill payee" for their respective customers. The Applicants' business was just starting to expand and they had very little money to fund a lawsuit to challenge the de-listing by these 3 banks.

209. If Scotiabank is permitted to terminate the Applicants as a Bill Payee for Scotiabank customers, there will only be the Royal Bank and Bank of Montreal left which permit their customers to list the Applicants as a Bill Payee. This will have a devastating effect on the Applicants' business, again causing irreparable harm.

210. The Applicants are victims of a domino effect among the few Canadian banks. A few years ago, TD, CIBC and ATB removed the Applicants, now Scotiabank wants to do the same thing. Scotiabank is arguing that the Applicants can still keep operating with Royal Bank and Bank of Montreal.

211. The Applicants do not have to be down to the last bank before there is a finding of illegality and irreparable harm.

212. One of the Applicants maintains a business bank account with each of the five (5) banks listed above (not ATB). Only the Respondent bank has permitted each of the Applicants to open bank accounts. This has permitted the Applicants to treble their volume of business. All of the other four (4) banks treat the 3 Applicants as a single business.

(b) EMTs

213. On the subject of EMTs, the Royal Bank of Canada is the only bank, other than the Respondent bank, which permits EMT's to be deposited into a business savings account without a charge for each deposit.

214. However, because the Royal Bank will only allow the Applicants to collectively open only one business account, the other two (2) Applicants are not able to process such EMT's through any other business account except at the Scotiabank. Thus, the Applicants can only process $300,000.00 per month and $3.6 million per year at the Royal Bank but can process $15 million per year at the Scotiabank as a small business customer.

215. If Scotiabank is permitted to unilaterally terminate the Applicants' banking services FOR NO VALID REASON, only one of the Applicants will be able to process EMT's through the only remaining Canadian bank that permits such EMT's into a business account and for the Applicants to possibly obtain the Certapay option (at much greater expense) and the business of the Applicants will ultimately fail.

216. The Applicants want to apply to the Scotiabank to become commercial business customers to expand the imposed limits but the Scotiabank, to date, has not allowed them to make such application.

217. The Respondent, on the one hand says that the Applicants are no longer a small business, but on the other hand refuses to deal with the Applicants as a larger business. Finally, following the termination notices, the Respondent excludes the Applicants from dealing with it altogether.

(d) CertaPay

218. It is possible for the Applicants to apply to CertaPay to process EMT's by the "Back door". However, there are serious limitations to this. The limitations are the following:

a. The application by the Applicants must be accepted by CertaPay, which is by no means certain;

b. The CertaPay limits are $10,000.00 per day, $300,000.00 per month (whereas at Scotiabank our limits are $30,000.00 per day and $900,000.00 per month;

c. CertaPay will charge $2.50 for each deposit into the Applicants' account and $1.50 to the Customer for each EMT sent;

d. The Applicants would be restricted to a single profile at CertaPay; and

e. The Certapay alternative is priced so much higher than Interac Online that is anti-competitive and not a viable business alternative for the Applicants.

X. TERMINATION WITHOUT CAUSE – STILL UNJUSTIFIED

219. The Applicants wish to emphasize the very relevant fact that the Respondent chose to terminate the Applicants "without cause".

220. Apparently, according to paragraph 114 of the Rosatelli Affidavit, the only reason for Scotiabank omitting cause was to maintain confidentiality over its fraud detection systems and its investigation into the Applicants. Why then, did the Respondent produce 1,000 pages of cause into the public record of the Tribunal web site?

221. Despite the lacunas detailed herein, the Applicants believe the Respondent to be a competent professional bank. It is that competence and professionalism that selected to deliberately (and illegally) terminate the Applicants on May 11, 2005, without cause. The Applicants maintain that that wording was chosen because, at the time, it was true. True, meaning the Respondent had no cause for which to terminate the Applicants.

222. The belated explanation of concern over secrecy, fraud and investigation is belied by the completely public nature of the Response. The Respondent could have elected to file a confidential Response. The fact that it did not proves that the Respondent is fabricating justification after the fact for its illegal termination without cause.

X. IRREPARABLE HARM TO APPLICANTS' BUSINESS REPUTATION

223. If Scotiabank is permitted to unilaterally terminate the Applicants' banking services, this will also negatively impact the Applicants' ability to expand into the American market.

224. The implication of a major Canadian bank (one of very few banks in Canada) refusing to offer banking services to a business is that the business is not a reputable business and, therefore, one that other banks should not deal with.

225. The Applicants submit that the seriousness of irreparable business harm that is a natural and foreseeable consequence of having its banking services unilaterally terminated in today's global market is such that banking services should only be terminated for cause.

XI. UNITED STATES PRECEDENT

226. The issue of the bank's customer's confidential information being accessed by authorized third parties has arisen in the United States.

227. Authorized third parties are called "data aggregators". In or about December 30, 1999, First Union Bank sued Secure Commerce Services alleging unauthorized access to a computer, trademark and copyright infringement, misrepresenting its relationship with First Union and misleading customers. Attached and marked **Exhibit H** to the Grace Affidavit is an article from Thomas Vartanian and Robert Ledig, entitled "Scrap it, Scrub it and Show it: The Battle over Data Aggregation" which summarizes the issues and actions that have happened since 1999 arising from concerns over data aggregators.

228. The attached article illustrates that the issues before the Tribunal in this case are real material issues of pertinence under the Act and need not be clouded by the Respondent's flurry of rhetoric on terrorism etc...

229. Paragraphs 4.1 and 4.2 of the attached article describe how the First Union lawsuit was settled by the data aggregator complying with First Union Guidelines. First Union indicates these guidelines help the bank to manage some of its perceived risks to the banks' systems and maintain the security and privacy of customer data. Since those 9 guidelines were published, 3 more guidelines have been added, a copy of which is attached and marked **Exhibit I** to the Grace Affidavit. Although the heading on Exhibit I does not specifically refer to First Union, this is their list of guidelines.

230. The Applicants and UseMyBank Services, Inc. are already fully compliant with these guidelines.

XI. APPLICANTS' EFFORTS TO WORK OUT POSITIVE RELATIONSHIP WITH THE SCOTIABANK

231. The Applicants have made several good faith attempts to resolve the Scotiabank's apparent complaints to enable the Applicants to continue to receive banking services from Scotiabank without taking the matter to court, including:

a. **to address the miniscule but ongoing problem of fraudulent transactions**: the Applicants will permit the Scotiabank to withdraw the amount of the alleged fraud from their account (if the Applicants have not already caught the fraud and already refunded the money) and work with the Applicants, the customer and the sending and receiving banks to investigate the fraud. Often the Applicants are the party that have the information to be able to track the fraudster.

b. **to address concern about security** – the Applicants are willing to abide by the Guidelines established by First Union (as described above) – and state they are already in compliance with same. They are willing to have the Bank of Nova Scotia's security people review their security procedures to prove to them that they are NOT a risk to the Canadian banking system. Attached hereto and marked **Exhibit J** is a copy of Scan Alert's Compliance Report for UseMyBank Services, Inc. dated August 3, 2005. Scan Alert is a qualified independent Scan Vendor accredited by Visa, Mastercard, American Express, Discover Card and JCB to perform network security audits confirming the Payment Card Industry Data Security Standards (PCI). Its certification of regulatory compliance certifies that Hacker Safe sites meet all U.S. Government requirements for remote vulnerability testing as set forth by the National Infrastructure Protection Center (NIPC), inter alia.

232. **To date, the Scotiabank has refused to enter into any kind of dialogue and seems determined to put the Applicants out of business for no good reason, but taking the Canadian online debit payments market for itself.**

233. There is no impediment to the discretion of the Tribunal to grant an injunction to the Applicants in the present matter and accept the Application on the merits.

B. ADDITIONAL BASIS FOR APPLICATION PURSUANT TO SECTION 103.1

I. The Test for Leave to Make Application Under Sections 75 or 77

234. Paragraph 103.1(7) of the Act sets out the test for leave to make application under Section 75 or 77 of the Act as follows:

> The Tribunal may grant leave to make an application under sections 75 and 77 if it has reason to believe that the applicant is directly and substantially affected in the applicants' business by any practice referred to in one of those sections that could be subject to an order under that section.

235. Owing to its novelty, the test under paragraph 103.1(7) of the Act remains the subject of varied interpretations.[1]

236. The Applicants agree with the following interpretation of the test by Justice Rothstein, of the Federal Court of Appeal in the matter of *Symbol Technologies Canada ULC* v. *Barcode Systems Inc.*, 2004 F.C.A. 339 (***"Barcode"***):

> "The threshold for an applicant obtaining leave is not a difficult one to meet. It need only provide sufficient credible evidence of what is alleged to give rise to a *bona fide* belief by the Tribunal. This is a lower standard of proof than proof on a balance of probabilities which will be the standard applicable to the decision on the merits."[2]

237. The Applicants agree that the Federal Court of Appeal, in *Barcode*, increased, though only marginally, the burden on the party seeking leave to appeal under paragraph 103.1(7) of the Act.

238. Before *Barcode* a party may expect to be granted leave on the basis of only the direct and substantial effect of the activity in question, without the Tribunal considering all of the elements of refusal to deal set out in subsection 75(1). Following *Barcode*, applicants can now expect the Tribunal to consider not only the direct and substantial effect on their business of the activity in question, but also the elements of refusal to deal set out in subsection 75(1).

---

[1] Hofley, Randal J. and Kevin Rushton, "Recent Competition Tribunal Decisions Muddy the Leave Test for Private Access Applications, *The Competitor*, Stikeman Elliott, September 2004, a copy of which is attached hereto as **Exhibit "A"** to this Reply.

[2] *Barcode*, para 17. Paragraph 88 of the Response omits this important rule of interpretation concerning Section 103.1 and thereby misstates the law on the point.

239. However, 'considering' the elements of refusal to deal is something much less substantial than 'interpreting' or deciding on them. Indeed, concerning that consideration of elements *Barcode* states:

> The Tribunal may address each element summarily in keeping with the expeditious nature of the leave proceeding under section 103.1.[3]

240. The Response is misleading in its representation of the test. The test is not difficult to meet and requires a lower standard of proof than proof on a balance of probabilities.

241. Federal Court of Appeal makes it clear, in *Barcode*, that a leave application is not the appropriate occasion to decide if a party's refusal to deal actually meets all of the elements set out in subsection 75(1).[4] *Barcode* provides:

> "...if there are any facts in its affidavit that might meet the requirements of paragraph 75(1)(e), the benefit of any doubt should work in favour of granting leave in order not to finally preclude Barcode from its day before the Tribunal."[5]

242. The Applicants very much want their day before the Tribunal, moreover, they are entitled to it under the Act.

243. The Respondent also read *Barcode* wrongly. The Response states:

> "The Applicants fail to point out that the Tribunal's decision in *Barcode* was reversed on appeal."[6]

244. The Tribunal's decision in *Barcode* was actually affirmed on appeal, not reversed.[7]

245. The Applicants submit that all argument in this Reply must be taken together with the substance of the two Affidavits by Grace and the Affidavit by Iuso, all of which have been filed with the Tribunal.

---

[3] *Barcode*, para. 19.
[4] *Barcode*, paras. 26-27.
[5] *Barcode*, para. 27.
[6] Response, para. 89.
[7] *Barcode*, paras. 29-30.

II. The Test for Leave is More than Satisfied

(a) Product Markets at Issue

246. The Response fails to recognize the product markets at issue in this. There are two (2) relevant product markets at issue in this case.

247. The first product market is the market for the supply of EMT and bill payment services, as provided to the Applicants by the Respondent (the "**Bank Inputs Market**").

248. The Applicants are buyers in the Bank Inputs Market and Scotiabank is a seller. As will be discussed in greater detail below, there is severely limited supply in Canada in the Bank Inputs Market. The Applicants reject the self-serving position of the Applicants that because they are refusing to deal, there is, in fact, no supply in that market.[8]

249. The second product market at issue in this case, is the market for the supply of online debit payment services (the "**Online Debit Payment Market**").

250. The Applicants are sellers in the Online Debit Payment Market and so is Scotiabank, through its Interac Online service.

251. In order for the Applicants to continue their hugely successful business as sellers in the Online Debit Payment Market, they must purchase services in the Bank Inputs Market. Scotiabank is refusing to deal with the Applicants in the Bank Inputs Market, as a seller, precisely because such refusal to deal will extinguish the Applicants as competitors of Scotiabank in the Online Debit Payment Market.

252. The practice of Scotiabank of refusing to deal with the Applicants puts in jeopardy the limited competition in both the Bank Inputs Market and the Online Debit Payments Market in Canada.

---

[8] Response, sub-para. 91(b).

Section 75

(b) Direct and Substantial Effect

253. The Applicants have now proven, with two affidavits[9], that the practice of the Respondent to cease serving the Applicants will directly and substantially affect the business of the Applicants.

254. The effect of the refusal to deal of the Respondent is such that it will reduce the revenue of the Applicants by no less than fifty percent (50%).[10]

255. The Applicants submit that direct and substantial effect on their business from the practice of the Respondent has been proven beyond a reasonable doubt. However, the burden of proof on this point is less than the lower threshold of balance of probabilities.

256. The Grace and Iuso Affidavits filed concurrently herewith detail attempts by the Applicants to procure products in the Bank Inputs Market from entities other than the Respondent, without success.

257. In one of many instances of the Respondent being blind to the limits on its own standing and rights, the Respondent holds itself out as being able to speak for all Canadian Schedule I Chartered Banks. The Response states:

> "No Canadian Schedule I Chartered Bank will provide accounts and services to the Applicants on the terms that they seek.[11]
>
> "No Canadian Schedule I Chartered Bank will provide accounts and services to the Applicants based on the Applicants' manner of doing business..."[12]

258. These repeated statements beg the question of how Scotiabank can speak for the intentions of its competitors. Perhaps it does.

---

[9] See the First Affidavit of Grace at, *inter alia*, paras. 42-54 and the Second Affidavit of Grace at, *inter alia*, paras. 74, 123, 197-218 and 223-225.
[10] First Grace Affidavit, para. 43.
[11] Response, sub-para. 91(b).
[12] Response, para. 109.

259. These blanket assertions on behalf of all the Canadian banks that are suppliers in the Bank Inputs Market go to prove the intent of Scotiabank to collude with its partners in Interac to extinguish the business of the Applicants and supplant it with their novel Interac Online service.

260. The Respondent has been a seller to the Applicants in the Bank Inputs Market for years. Within a thirty (30) day period, the Respondent has refused to deal with the Applicants and launched its own Interac Online service that will supplant the services sold by the Applicants.

261. Together, these two acts constitute awesome examples of violations of the Act by Scotiabank.

(c) Inability to obtain adequate supplied of product on usual trade terms - Section 75(1)(a)

262. The Respondent contends that no bank will serve the Applicants because of issues relating to security and gambling.

263. The Respondent submits that the Applicants could not be purchasers from other sellers in the Bank Inputs Market because they convey Customer information and instructions from Customers to their banks.

264. The Applicants have proven[13] that, at law, they are agents of Customers, and are therefore bank customers vis-à-vis the bank without any concern over violation of cardholder agreements or security.

265. Indeed, the Applicants maintain high standards of security in their business and actually provide greater security in the form of fraud prevention, that the Respondent does not. Moreover, no individual person delivering the services of the Applicants comes into contact with personal cardholder information of Customers. That secret information is encrypted and transmitted only through highly secure computer systems.

---

[13] See Second Grace Affidavit paras. 82-108.

266. Security cannot possibly be a valid reason for refusing to deal with the Applicants, as the Applicants maintain better security than those that allege security as a reason not to deal with them, namely, Scotiabank.

267. Providing services to off-shore internet casinos cannot possibly be a reason for Scotiabank to refuse to deal with the Applicants, because Scotiabank itself owns or earns revenue from off-shore casinos, both internet and brick and mortar.

268. It is not the role of the Tribunal or Scotiabank, in this case, to adjudicate on the legality of off-shore online gambling in Canada. Selecting this aspect of the business of the Applicants as a basis on which to refuse to deal is a capital example of exclusive dealing and refusal to deal, as contemplated in the Act, because Scotiabank is itself heavily invested in off-shore gambling, both online and elsewhere.

269. The Act will not permit Scotiabank to earn substantial revenue from gambling, and then use the online casino clients of the Applicants as a basis on which to refuse service. More than illegal, this position is astonishingly hypocritical.

270. If there is any example of material non-disclosure in this case, it is the failure of Scotiabank to disclose its amble investments in off-shore gambling, both online and elsewhere.

271. The Applicants have made attempts to procure products in the Bank Inputs Market from sources other than Scotiabank with limited results.

272. Competitors of the Applicants, including Yodlee and CashEdge[14], the latter of which may be partly owned by The Royal Bank of Canada, have been able to procure services in the Bank Inputs Market. These facts belie the position of the Respondent that such products do not exist.

---

[14] Response, sub-para. 114(g).

(d) Insufficient competition among suppliers – Section 75(1)(b)

273. The fact that the principal competitors of the Applicants belong to and operate through a monopolistic consortium, Interac, is one example of proof of the lack of competition in the Bank Inputs Market.

274. If there were true competition between Scotiabank and other banks in Canada, some of those banks, or all of them, would be clamoring for the business of the Applicants.

275. The Applicants pray that the Tribunal will take into consideration that they very successful businesses who bring material revenue to Scotiabank. With a legal obligation to earn profits for its shareholders, why would Scotiabank refuse business from good customers like the Applicants? The answer is that Scotiabank wants the business of the Applicants for itself.

276. All arguments of the Respondent as to terrorism, money laundering, gambling and security are proven to be irrelevant and act to cloud the true issues of competition law that are relevant before the Tribunal.

277. As a material investor in no less than ten (10) brick and mortar cash-based casinos, the Respondent has much greater need for concern over terrorism, money laundering and security than the Applicants who deal in only fully traceable electronic payments and own no casinos.

278. The Respondent has mistakenly fixated on a constellation of alleged wrongs[15], of which it is much more responsible than the Applicants, as bases on which to refuse service.

---

[15] The Applicants maintain that it is not for the Tribunal to adjudicate on matters of terrorism, money laundering, gambling or security in this case. The Applicants have never been charged or convicted of such wrongs. Entering such allegations into argument without any shred of proof thereof reveals the true intent of the Respondent to divert attention of the Tribunal away from its scheme to put the Applicants out of business and start its own business in the same market. For the moment, Canadian banks remain persons

279. As for the Online Debit Payment Market, where Scotiabank seeks to supplant the Applicants, there is no doubt that Scotiabank's Interac Online is interchangeable with the services of the Applicants.

280. From the perspective of either the Customer or the Merchant, use of either service is identical. As agent for the Customer, the Applicants convey Customer instructions to their bank. *A pari*, Interac Online serves to convey Customer instructions to their bank.

281. Once the Applicants are put out of business by Scotiabank, Scotibank will be able to occupy the Online Debit Payment Market without competition.

282. The Respondent argues that Interac Online will never replace the Applicants services, because Scotiabank would never assist in a payment to an internet casino. The Applicants have proven that Scotiabank is in the business of precisely making payments to online casinos.[16] Here, Scotiabank credibility is suspect.

(e) Applicants meet Respondent's Usual Trade Terms – Section 75(1)(c)

283. Despite processing millions of dollars for the Applicant, the Respondent claims it was completely ignorant of the business of the Applicants. On the basis of this new-found ignorance, the Respondent contends that the Applicants do not meet the usual trade terms of the Respondent.

---

under the law. They are not above the law. They do not adjudicate, legislate or anything of the sort. The Response also carries an irrelevant moralistic tone, which, when turned on Scotiabank itself reveals brazen hypocrisy. Finally, whether gambling, online or elsewhere, is a wrong or not, is a matter of personal judgment. If Scotiabank believes that offshore online gambling is wrong and illegal, why is Scotiabank accepting handsome profits from it through its Scotia Visa cardholders? The Act puts this hypocrisy in check. To the knowledge of the Applicants all of its Merchant clients, including all who are casinos, operate wholly within all applicable laws. Scotiabank as produced no evidence to the contrary. In the unlikely scenario that the Tribunal sees fit to deliberate on the subject of the legality of online gambling in Canada, the Applicants submit that the law on that topic is far from settled. Reference is made to Kayer, C. Ian and Danielle Hough, "Is Internet Gambling Legal in Canada: a Look at Starnet", CJLT Vol. 1, No. 1, a copy of which is attached hereto as **Exhibit "B"** to this Reply. There is also an important distinction between online gambling operations in Canada and those that are off-shore in jurisdictions with different laws. Scotiabank appears to address principally the latter. Again, to the knowledge of the Applicants, all of their merchant clients, including casinos, operate in full compliance with all applicable laws.

[16] Second Grace Affidavit, para. 164.

284. The Applicants enjoyed years of active and enlightened service from the Respondent, notably through the account manager of the Applicants, Woodrow and the local branch manager Mrs. Parsons.

285. What is more, the Iuso Affidavit proves that representatives of the Respondent partook in a detailed presentation explaining all of the workings of the business of the Applicants on or about October 22, 2003.[17]

286. The Respondent is nothing but wrong in stating that it knew nothing of the business of the Applicants until the very near past. In fact, the Respondent was so familiar with the business of the Applicants that it copied it to produce Interac Online.

287. The Respondent states that it has a policy of not providing services to Money Services Businesses. In other words, the Respondent is pleading to the Tribunal that it does not serve competitors. These submissions are without substance.

288. Again, concerns over terrorism, money laundering, gambling and security, all being much more true of Scotiabank than the Applicants, cannot be cited as excluding the Applicants from the usual trade terms of the Respondent.

(f) Product is in Ample Supply – Section 75(1)(d)

289. Years of sales by Scotiabank to the Applicant in the Bank Inputs Market evidence ample supply of product in that market.

290. The Respondent has not provided any evidence that servicing the Applicants was unduly taxing on its business. On the contrary, the Applicants have proven the healthy and mutually beneficial profits earned by the Respondent in servicing the Applicants.

291. The Respondent cannot argue that there is no supply of product because they have decided not to supply product. That argument, made by the Respondent[18], is circular, self-serving and illogical.

---

[17] Iuso Affidavit, para. 6-7.
[18] Response, para. 116.

(g) Refusal to Deal is Having an Adverse Effect on Competition in the Bank Inputs Market and the Online Debit Payment Market

292. The Applicants have proven the limited degree to which Canadian banks are willing to provide product in the Bank Inputs Market. Refusal of the Respondent to deal with the Applicants will only aggravate the lack of competition in that market.

293. As for the Online Debit Payment Market, before the entry of Scotiabank into that market, the Applicants were the only participants. If the Respondent has its way, it will be the only participant, rather than simply a competitor of the Applicants.

294. The Applicants would welcome competition in the Online Debit Payments Market. The Respondent does not.

(h) General Section 75 Argument

295. The Applicants emphasize that at the application for leave stage, where the parties are as of these presents, the Tribunal need only consider the five (5) elements of Section 75(1) discussed above. The Tribunal is not called upon to interpret or decide on them at this stage.

296. The test for leave to make an application is met and exceeded by the facts in this case. Considering the direct and substantial harm that the practice of the Respondent will cause to the Applicants, and the satisfaction of each element of Section 75(1), as proven, the Applicants have met the criteria to make a private Application to the Tribunal in this case.

(i) Scotiabank is Dealing Exclusively – Section 77

297. By cooperating with the other monopolistic banks in Canada to supply Interac Online, Scotiabank is providing Bank Input Market services to those other banks, because they are banks that will supply Online Debit Payment Market services through Interac.

298. Scotiabank, even in its own Response[19], proposes Interac membership as a condition to its supply of Bank Input Services. The monopolistic perspective of Scotiabank on this matter is such that it appears incapable of imagining a competitor that is not bound up in its monopolistic Intrac association.

299. The Applicants submit that it is not for Scotiabank to decide what services the Applicants can or cannot provide. The legislator is well vested for such pursuits.

300. It is common knowledge, and a matter of public record, that a variety of former monopolistic participants in the Canadian market are awakening to new forms of unregulated competition. The telephone and cable television industries are but two examples. The Applicants would prefer that Scotiabank embrace the Applicants as business partners rather than as competitors to be quashed by the overwhelming power of Scotiabank in the relevant markets.

(j) The Respondent Has No Business Reason to Terminate the Applicants

301. The best proof of the absence of a business or other reason for the Respondent to terminate the Applicants are the Respondent's own termination letters which state that the Applicants were being terminated without cause.

302. The termination without cause is, in fact, key to understanding the motivation of the Respondent in terminating the Applicants. The true cause was an intent to extinguish the business of the Applicants and supplant it with that of Scotiabank's Interac Online.

303. The Respondent argues that it suppressed the true cause of termination for reasons of confidentiality. That submission is belied by the now public alleged reasons in the Response that the Respondent could have filed on a confidential basis with the Tribunal.

304. The Applicants believe that there was no reason to terminate them other than to take their business. The after-the-fact reasons for termination and new-found ignorance about the business of the Applicants all go to prove violations of the Act by Scotiabank.

---

[19] Response, para. 85.

III. Conclusion

305. The Applicants are a small business of successful Canadian entrepreneurs who dared to start a new venture. They succeeded.

306. Now, if the Respondent has its way, the Applicants will see half of their revenue disappear. They will also see the Respondent build a business identical to that of the Applicants for the sole purpose of taking up market share now held by the Applicants.

307. The decision of the Respondent to fill the Response principally with inflammatory and unproven accusations of concern over terrorism, money laundering, gambling and security violations, shows how the Respondent has missed the opportunity to have a healthy debate over the application of the Act to the facts in this case. The Applicants pray that the Tribunal will examine the United States precedent on this topic[20] as an example of a more mature approach to the problem than the one selected by Scotiabank.

308. This matter is time-sensitive. The Applicants pray that the Tribunal will have opportunity to review this Reply in the shortest possible delay in order to avoid loosing their business.

309. The facts and law of this case merit granting leave for the Applicants to make an application under Section 103.1(7) of the Act.

310. The Applicants need and want their day before the Tribunal.

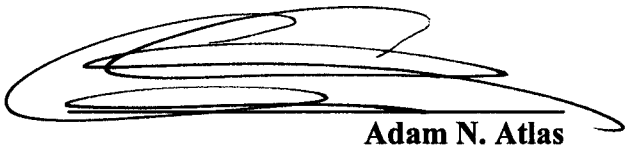
311. In support of the foregoing, Applicants rely on the Second Affidavit of Raymond F. Grace, sworn September 1, 2005, and the Affidavit of Joseph Iuso, sworn August 29, 2005.

312. In their Application, the Applicants respectfully request an order from the Tribunal granting them leave to make the Application under Section 103.1(7) of the Act.

---

[20] Second Grace Affidavit, para. 226-230.

DATED at Montreal, Quebec, this 2nd day of September 2005.



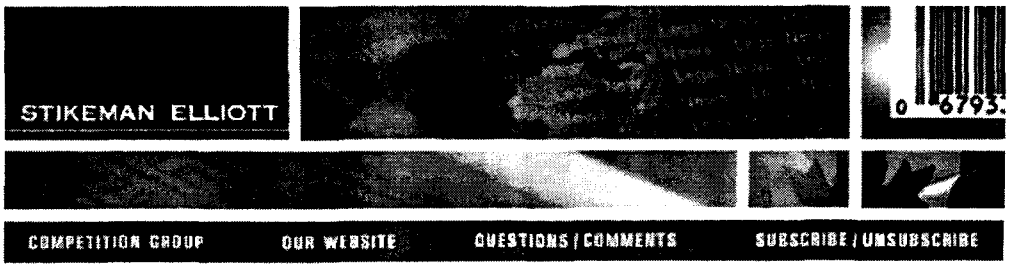
Adam N. Atlas
Adam Atlas Attorney at Law
2000 Mansfield Street, Suite 1400
Montreal, Quebec H3A 3A2
Tel: 514-842-0886
Fax: 514-842-9371
E-mail: atlas@adamatlas.com
Barreau du Québec No.: 201211-1

Counsel for the Applicants

Exhibit "A"

to

REPLY BY APPLICANTS TO REPRESENTATIONS BY THE RESPONDENT FOLLOWING APPLICATION BY THE APPLICANTS FOR LEAVE PURSUANT TO SECTION 103.1 OF THE *COMPETITION ACT*



The Competitor

September 2004

The Competitor is a regular update prepared by the members of the Competition/Antitrust Group at Stikeman Elliott LLP and reports on issues affecting Canadian and International business.

INSIDE THIS ISSUE PRINTABLE PDF VERSION >

Leave Test for Private Access Applications Remain Uncertain
Tribunal Denies CWS Application
Recent Group Developments
- **Luncheon with Canada's Commissioner of Competition**
- **Toronto Partner Recognized Among 100 Women in Antitrust**
- **Group Ranked Once Again in The World's Leading Lawyers 2004**

Recent Competition Tribunal Decisions Muddy the Leave Test for Private Access Applications

by Randall J. Hofley and Kevin Rushton

On July 13 and August 4, 2004, the Competition Tribunal granted leave to Robinson Motorcycle Limited (Robinson) and Quinlan's of Huntsville Inc. (Quinlans) to bring applications against Fred Deeley Imports Ltd. (FDI) under the refusal-to-deal provisions of the *Competition Act*[1]. The two decisions bring to four the number of leave applications granted to private parties since amendments to the Act in June of 2002. Unfortunately, these recent decisions appear to cloud the legal and evidentiary thresholds that will be applied by the Tribunal before granting leave.

As noted in the March 2004 edition of *The Competitor*, section 103.1 of the Act allows private parties to apply directly to the Tribunal to address alleged breaches of sections 75 (refusal to deal) and 77 (exclusive dealing, tied selling and market restriction). Obtaining leave of the Tribunal is a prerequisite to bringing such applications. To date, a total of nine applications for leave have been filed. Of these, the first was denied, four have been granted and the remaining four await decisions by the Tribunal.

Both recent cases involve the alleged refusal by FDI, the exclusive Canadian distributor of Harley-Davidson (H-D) motorcycles, parts and accessories, to supply Quinlans and Robinson, two Ontario-based motorcycle dealers, with H-D products. The dealers had obtained H-D products for several years pursuant to successive dealer agreements entered into with FDI. However, in December of 2003 and January of 2004, FDI informed Quinlans and Robinson that it would not offer an extension to their agreements. The dealers alleged that FDI's refusal to deal would force them out of business, adversely affecting competition in their markets.

The Legal Test

The Tribunal found that the Dealers had satisfied the requirements for leave, as set out in subsection 103.1(7) of the Act. *National Capital News v. Milliken*[2] was the first case to consider the leave threshold. Dawson J. held that subsection 103.1(7) creates a two-part test, both parts of which must be satisfied for leave to be granted. Based on the wording of the statute, the Tribunal must have "reason to believe" that (1) the applicant is "directly and substantially affected" in its business by the alleged practice and (2) the practice "could be subject to an order" under section 75. Under part two, Dawson J. held that all five paragraphs of subsection 75(1) must be satisfied, the most notable of which is that the alleged refusal to deal "is having or is likely to have an adverse effect on competition in a market".

Two decisions by Lemieux J. subsequent to *National Capital News* adopted a lower threshold for granting leave. In *Barcode Systems v. Symbol Technologies*[3], the Tribunal held that the five paragraphs of subsection 75(1) need not be satisfied in order for leave to be granted under section 103.1:

> As I read the Act, adverse effect on competition in a market is a necessary element to the Tribunal finding a breach of section 75 and a necessary condition in order that the Tribunal make a remedial order under that section. It is not, however, part of the test for the Tribunal's granting leave or not.
>
> What the Tribunal must have reason to believe is that Barcode is directly and substantially affected in its business by Symbol's refusal to sell. The Tribunal is not required to have reason to believe that Symbol's refusal to deal has or is likely to have an adverse effect on competition in a market at this stage[4].

Lemieux J. cited this conclusion with approval in *Allan Morgan and Sons v. La-Z-Boy*[5].

Unfortunately, the Tribunal's single-page decisions in *Quinlans* and *Robinson* do not discuss the legal test to be applied on leave applications. However, the decisions are structured to address each of the five paragraphs in subsection 75(1) of the Act, and state that the Tribunal could conclude that the elimination of the Dealers "is likely to have an adverse effect on competition. " The decisions thus appear to diverge from the less onerous leave test adopted in *Barcode* and *La-Z-Boy*, instead favouring the two-part test of *National Capital News*.

The Evidentiary Threshold

In *National Capital News*, the Tribunal held that for it to have "reason to believe" under section 103.1, the applicant must provide "sufficient credible evidence to give rise to a *bona fide* belief" that it is directly and substantially affected in its business by a practice that could be subject to an order under section 75 or 77. The Tribunal in *Barcode* explained that evidence advanced will be sufficient if there is a "reasonable possibility" of a direct and substantial effect. A "reasonable possibility" is a lower threshold than a balance of probabilities, but Lemieux J. held that the evidence must show more than a "mere possibility" of the required effect.

The Tribunal in *Barcode* further explained that on a leave application, its function is limited to screening the evidence to decide on its sufficiency. More particularly, Lemieux J. held that it is not the Tribunal's function "to make credibility findings based on affidavits which have not been cross-examined." However, the Tribunal did note that situations may arise "where it can be demonstrated that an applicant's evidence is simply not credible without engaging the Tribunal in weighing contested statements."

In granting the leave applications in *Quinlans* and *Robinson*, the Tribunal was clearly of the view that sufficient credible evidence had been advanced. It would have been

useful, however, for the Tribunal to address arguments by FDI that Quinlans' evidence of substantial effect was not credible on its face, because it failed to include financial statements to substantiate its allegation that H-D sales constituted exactly 64.9999% of its total sales for each of five successive years.

Conclusion

After five Tribunal decisions on section 103.1 leave applications, the legal and evidentiary thresholds that will be applied by the Tribunal before granting leave remain uncertain. This uncertainty should be resolved by the Federal Court of Appeal, as the Tribunal's decisions granting leave in *Quinlans*, *Robinson*, *La-Z-Boy* and *Barcode* have all been appealed.

FOOTNOTES

[1] Robinson Motorcycle Limited v Fred Deeley Imports Ltd., 2004 Comp. Trib. 13, and Quinlan's of Huntsville Inc. v Fred Deeley Imports Ltd., 2004 Comp. Trib. 15

[2] The National Capital News Canada v The Honourable Peter Milliken, M.P., 2002 Comp. Trib. 41.

[3] Barcode Systems Inc. v Symbol Technologies Canada ULC, 2004 Comp. Trib. 1.

[4] Barcode, Reasons and Order Regarding Application for Leave to Make an Application Under Section 75 of the Competition Act, dated January 15, 2004, at paras. 10 and 8.

[5] Allan Morgan and Sons Ltd. v La-Z-Boy Canada Ltd., 2004 Comp. Trib. 4, Reasons and Order Regarding Application for Leave to Make an Application Under Section 75 of the Competition Act, dated February 5, 2004, at para. 14.

Return to Top

Tribunal Denies CWS Application

On June 28, 2004, the Competition Tribunal denied an application by Canadian Waste Services Inc. (CWS)[1] to rescind an October 2001 order under section 92 (mergers) requiring the divestiture of the Ridge landfill in Chatham, Ontario. In May 2003, CWS applied to the Tribunal to set aside the divestiture order under s. 106 of the *Competition Act* on the basis that the circumstances that led to the making of the order had changed, and that in the present circumstances, the Tribunal would not have made the order. The Tribunal's decision is currently under appeal. Although the Tribunal's recent decision terminated the July 10, 2003 stay of its order to divest the Ridge landfill, on August 6, 2004, the Federal Court of Appeal granted a stay of the divestiture order pending appeal of the Tribunal's recent s. 106 decision. The appeal is scheduled to be heard on November 4, 2004.

FOOTNOTE

[1] Now Waste Management of Canada Corporation.

Return to Top

Recent Group Developments

Luncheon with Canada's Commissioner of Competition

The Competition/Antitrust Group of Stikeman Elliott is delighted to welcome Sheridan Scott, Commissioner of Competition, Canadian Competition Bureau at a luncheon for clients and guests on Tuesday, September 21, 2004 in Toronto, Ontario. Ms. Scott will discuss her priorities as Commissioner followed by a general

discussion with luncheon guests.

Toronto Partner Recognized Among 100 Women in Antitrust

Katherine Kay, a partner in our Competition/Antitrust Group, has been recognized as one of the 100 Women in Antitrust in the world in a recent survey conducted by the Global Competition Review.

Group Ranked Once Again in *The World's Leading Lawyers 2004*

Chambers Global has once again ranked Stikeman Elliott's Competition practice among the best in Canada in *The World's Leading Lawyers 2004.* According to the Chambers guide, the firm's Competition/Antitrust Group is acknowledged for its "superb track record in the field." Chambers praises lead partners Paul Collins' "commendable market share" and Susan Hutton who is "renowned for her expertise on merger-related issues."

These consistently high rankings are a product of the Competition/Antitrust Group's reputation in major cross-border and domestic transactions as well as its experience in criminal investigations, civil actions, and day-to-day compliance advice. Group members work closely with M&A attorneys in the Canadian, European, U.S. and Pacific Rim offices of Stikeman Elliott, and collaborate regularly and effectively with colleagues in leading U.S. and European firms.

Return to Top

For further information regarding the articles in this newsletter, please contact the co-authors Randall Hofley or Kevin Rushton. You may also contact the editor, Susan Hutton.

Members of the Competition Group at Stikeman Elliott LLP

For contact information regarding our Competition Group in Canada please CLICK HERE
Or click on any of the following for contact information regarding:
NEW YORK, LONDON or SYDNEY.

Exhibit "B"

to

REPLY BY APPLICANTS TO REPRESENTATIONS BY THE RESPONDENT FOLLOWING APPLICATION BY THE APPLICANTS FOR LEAVE PURSUANT TO SECTION 103.1 OF THE *COMPETITION ACT*

Is Internet Gaming Legal in Canada: A Look at Starnet

C. Ian Kyer* and Danielle Hough**

Published in Canadian Journal of Law and Technology, Vol 1, No. 1.

Introduction

The development of the Internet has kindled many new business opportunities in the online environment. Despite the recent slump in online business growth and popularity, one line of online business is generating profit and growing at a rapid rate: the business of online gaming.

The legality of such businesses is questionable in Canada and there are few gaming cases to assist Canadian lawyers. The following analysis must be considered in light of the dearth of jurisprudence in this area and should not be considered legal advice. This area of the law is in flux and developments may be unpredictable.

When you are feeling in the dark, even a flickering candle is welcome. Therefore, a recent British Columbia online gaming prosecution, in which the accused pled guilty, is worthy of study. Though resolved by a guilty plea with little judicial reasoning, the case provides some guidance in this largely unmapped area. It confirms that in certain circumstances, there can be criminal liability in Canada for running an online gaming operation. Online gaming ventures will have to consider several factors and be mindful of how their ventures are structured in order to avoid prosecution in Canada and conform to Canadian laws.

The Software Mechanisms Behind Online Gaming

To begin with, some technical background is required: we need to know something of how Internet gaming is carried out. An online gaming operation has to connect and communicate with its users through software and the Internet. A user visits an Internet site and downloads graphics and communications software onto his or her PC. The graphics software generates the images on the user's PC. The communications software links the PC via the Internet with servers maintained by the gaming site. The servers use random number generators and other software to tell the graphics software what images to generate to create the gaming experience. The servers interact with the user's PC, receiving information and generating

responses. The servers also host a database that tracks bets made and wins and losses.

The flow of money is separate from the gaming itself. The user is referred to one or more e-cash providers where credits can be purchased via credit card or other electronic funds transfer (EFT) for use at the casinos. If the user wins, the e-cash provider credits their credit card or EFT provider up to the amount of their "purchase". Any excess is paid by cheque or electronic funds transfer.

Online Gaming in Canada

The development of any online business raises several similar legal issues. These include taxation, security and privacy, intellectual property infringement and protection, transborder data flow regulation, the enforcement of online contracts, online licensing, product liability, and the overriding jurisdictional question as to which laws apply. When dealing with the development of an online gambling operation, there is the added issue of potential criminal liability.

In Canada, the only guidance we have at this time is the law that applies to traditional gaming. Part VII of the Canadian *Criminal Code*[1], entitled *Disorderly Houses, Gaming and Betting*, governs all forms of gambling and betting in Canada, including on-line gambling.[2] To conduct legal gambling and betting in Canada, a valid license must be obtained from the provincial government and one must operate within government regulations.[3] Presently, only the provincial governments can run online gaming operations. They are not permitted under the *Code* to issue licenses to run such operations. None are doing so, although PEI has proposed an online lottery.[4] Thus, other than the licenses being granted by the Kahnawake Indian band, which are of doubtful validity[5], no online licenses are being granted in Canada.

The operation of an unlicensed or unlawful gambling is an indictable offence.[6] It is easier, however, to apply Part VII of the *Code* to traditional gaming operations that have a physical location or gaming house in Canada than it is to online gaming. Traditional "land based" operations are squarely within Canada's territorial jurisdiction. The facilities are tangible and whether a license is required can be easily determined. In the case of online gaming, the "gaming house" is a virtual one. No aspect of an online operation need be located in Canada for Canadians to access the gaming action over the Internet, other than the public communications systems and the user's PC. The question with any particular online gaming operation is whether there

is a sufficient connection between the gaming operation and the Canadian jurisdiction. Without this connection, it would be difficult to apply the *Code* and enforce a ban on an online gaming operation. Even if there is a sufficient connection to Canada, the manner in which the *Code* will apply to online gaming is far from clear. Canadian lawyers and advisers will still have difficulty providing Canadian legal advice to their clients who want to set up and operate this type of business. Nevertheless, the following case from British Columbia does provide some limited guidance.

Starnet

a) The Facts

The *R. v. Starnet Communications International Inc.* [7] decision came down in British Columbia. Even though it involved a guilty plea with little judicial reasoning, it is helpful in that it sheds some light on how Canadian criminal law may apply to an online gambling operation.

Starnet Communications International Inc. ("SCI") was incorporated in Delaware. Through a number of wholly-owned subsidiaries, it conducted its operations from a location in Vancouver, B.C. One of these subsidiaries was incorporated in British Columbia. The other subsidiaries were incorporated in Antigua, where online gaming is legal and where SCI had an online gaming license.

SCI had developed software in Canada to facilitate online gaming and had issued several licenses to third parties that provided online gaming to Canadians. The police, using false identities and credit cards, engaged in online gaming offered by SCI's licensees. Their winnings were received in the form of credits to their credit cards and also by cheques. SCI officers, located in Vancouver, signed some of these cheques and mailed them from their Vancouver offices.

SCI's Vancouver operation consisted of computer servers and computer applications, which enabled persons to engage in gambling or betting via the Internet. Users wanting to wager had to access these B.C. based servers first before being redirected to offshore servers. Many of the gaming websites developed by SCI's employees were hosted in British Columbia. Users downloaded software to their PCs from these BC sites. The server side software was also located in Vancouver. The registration and control of the domain name servers for many of the licensee pages were also controlled and physically located in Vancouver.

As the police investigation revealed, the role of the Canadian subsidiary and its operations in Vancouver was pivotal in this enterprise. Approximately 100 people were employed by the Canadian subsidiary and were located in offices in Vancouver. Only about four employees were working offshore. The Canadian subsidiary developed the server and client software packages, which enabled users to engage in online gambling. Further, they were responsible for the ongoing administration of the services, applications and computer systems.

Canadians were relatively unimportant for the profitability of the operation, representing only four per cent of online gamblers in 1999.[8] Nevertheless, and significantly, SCI allowed Canadians to gamble on its site.

SCI had several Canadian residents who held multiple positions in the various companies. These people were determined to be the corporation's controlling mind in the various aspects of the enterprise. This enabled the Crown to allocate corporate criminal liability under the alter ego theory.

Charges were laid in 1999. A deal was struck at some point between SCI and the Crown and SCI pled guilty to a charge under Section 202(1)(b) of the *Code*.[9]

b) Section 202(1)(b) of the Code

Section 202(1)(b) of the *Code* makes it an offence to

keep or knowingly allow to be kept in any place under his control any device for the purpose of recording or registering bets or selling a pool, or any machine or device for gambling or betting.[10]

The required elements of this offence are: "keeping", and the presence of a "device" for gambling or betting.

A "device" must be one for the purpose of gambling or betting. *Starnet* interpreted "device" to include all the computer servers, applications and systems that clients would have to access to begin any gambling.[11] SCI's "devices" were kept in Vancouver.

To "keep" does not simply mean to possess. It means possession that results in making the gambling machine available for use by the public.[12] The device must be somehow useable by the public for the

purposes of gaming and this can be direct or indirect.[13] In *Starnet,* the servers and applications in question were kept in Vancouver. These same servers and websites made the gambling activities available to Canadian users. This qualified as "keeping".

Although not explicit in the *Code*, it is implied that the gaming has to be available to the public in Canada. If the police investigation had not been able to show that Canadians could gamble with SCI, there probably would not have been a case. The *Code* provisions, taken as a whole, prohibit the provision of unlicensed gambling in Canada. It is questionable whether the keeping of gaming devices in Canada would have been an offence if these devices had not been used to make gaming available to the Canadian public.

c) Changes to the Canadian Operations

Subsequent to being charged but prior to the hearing, SCI purportedly changed the structure of its operations in order to comply with the *Code*. SCI was placed under the umbrella of a British holding company. The new company, as of May 2001, was named World Gaming, with its headquarters in London, England. Completely new management was put in place.[14] A new management committee was established in Antigua, and a new company called Starnet Systems was created to operate all the gambling activity from Antigua. Starnet Systems handled all the day-to-day gambling and financial activities. The devices that allowed customers to engage in gambling were moved out of Canada.

Only one element was said to remain in Canada. This was a company called Inphinity Interactive, which developed software for lawfully operated offshore gambling operations. Defence counsel submitted to the Court that there was nothing illegal with respect to Inphinity's operation. The Court and the Crown gave no indication they disagreed.[15]

To comply with the *Code*, all "devices" and the controlling mind of the corporation were moved offshore. Links to Canada were significantly reduced. The company also ceased offering access to Canadians. These changes seemed to satisfy the Crown and the Court and no action has been initiated against World Gaming.[16]

In essence, *Starnet* indicates that an online gaming operation that is unlicensed in Canada but has sufficient connections to Canada may be successfully prosecuted under the *Code*. Before the restructuring,

SCI's connections to Canada were indeed substantial. The devices, the controlling mind, the majority of the staff and services were located in Vancouver and gaming services were available to Canadians. To relieve itself of criminal liability, SCI had to restructure itself in a way that reduced its connections to Canada significantly.

Application of other Provisions of the *Code*

SCI pled guilty to a charge under Section 202(1)(b) of the *Code*. There are several other Sections in this Part of the *Code* that they could have been charged with but were not. This is probably the result of the deal SCI struck with the Crown. It does not mean that other provisions in the *Code* were not applicable. These other Sections of the *Code* that require analysis with respect to online gambling operations include Sections 202(1)(a), (c), (d), (e), (f), (i) and (j), and 207(1).[17]

a) Section 202(1)(a)

Section 202(1)(a) of the *Code* makes it an offence to use or knowingly allow a place under one's control to be used to record or register bets or sell a pool.[18] If an online gaming operation has an office or place in Canada where the recording and registering of the gaming bets goes on, this operation may violate this Section of the *Code*. This might include locating a database server in Canada. SCI kept its gaming servers offshore to begin with and was not in contravention of this Section.

b) Section 202(1)(c)

Section 202(1)(c) of the *Code* makes it an offence to have "control of any money or other property relating to a transaction that is an offence under this section".[19] For there to be an offence, there must be control of money or property that relates to a transaction that is an offence under this Section.

This section has been applied to bookmaking charges[20] or those of keeping gaming houses or devices.[21] The element of control, however, is not well defined in case law. In these types of cases, the control of money or property would be direct. The bookie or gaming house owner would have control over the profits made from the gamblers. It would be in their possession and theirs to deal with as they saw fit.

This section could similarly apply to an on-line gambling situation, where the Crown could prove that money is in the control of an

unlicensed on-line gambling operation in Canada. SCI was likely in control of money that was related to illicit gambling transactions with Canadians. However, no specific charge was made under this Section. Instead, the Crown used Sections 462.3 and 462.37 of the *Code*, which enabled them to get an order for SCI to forfeit its proceeds of crime. This effectively allowed the government to seize the profits that SCI made and had control of through illegal gambling transactions as prohibited by Section 202(1)(c).

Another possible application is against a third party company that provides the "chips" or online "casino cash" to gamblers. It is customary for e-cash providers, a form of financial intermediary between the online casino and a credit card company to provide an e-commerce solution to the gamblers. This third party essentially sells chips to gamblers so that they can then gamble on the gaming operator's site. The third party does not provide the gambling activity.

Two issues arise as to this section's applicability to the "chip" provider. First, it is not clear whether the "chip" provider would have the requisite "control" over money from an illegal gambling transaction. Second, the gambling transaction that the service supports must be illegal under Section 202 of the *Code*. Support services of this sort in Canada for a lawfully conducted offshore casino would not qualify

c) Section 202(1)(d)

Section 202(1)(d) of the *Code* makes it an offence to record or register bets or sell a pool.[22] If an online gaming operation has its database servers that record and register the bets located in Canada, this could contravene this Section of the *Code*. In the case of SCI, the database servers were offshore. These offshore servers recorded and registered bets. Therefore, it is not likely that this Section would have applied to SCI.

d) Section 202(1)(e)

Section 202(1)(e) of the *Code* makes it an offence to make "any agreement for the purchase or sale of betting or gambling privileges".[23] This section also usually applies to bookmaking[24] or the selling of a pool. It could also apply to selling the right to play in a lottery.[25] There must be an agreement, oral or written, in Canada to purchase or sell the right to gamble.

All the cases interpreting this section involve a direct purchase of a gambling privilege.[26] They involve phoning in a bet to a bookmaker or purchasing a lottery ticket or a share of a lottery ticket. It has not been applied to online gambling. However, it is possible. The Crown will have to prove beyond a reasonable doubt that an online gambling operation made such an agreement with Canadians. Most online gambling sites have a registration page. The gambler must enter information about him or herself and agree to certain terms and conditions in order to be granted access to gamble. This registration in itself could provide the evidence of an agreement that contravenes this Section of the *Code*.

If this type of registration equates an agreement contrary to this Section of the *Code*, this Section could have applied to SCI as all of the servers and staff that serviced the registration were in Vancouver.

If the registration site is offshore it may be more difficult to apply this section. An argument can be made that the agreement itself is made offshore. However, it can and has been argued in the United States that the agreement is made in the location of the gambler's computer. This debate has not been determined as of yet in Canada.

e) Sections 202(1)(f) and (i)

Sections 202 (1)(f) and (i) of the *Code* could have the effect of making advertising efforts for an unlicensed gaming operation an offence. Subsection (f) makes it an offence to print, provide or offer to print or provide information intended for use in connection with any game, whether or not it takes place in or outside of Canada.[27] Subsection (i) makes it an offence to willfully and knowingly send any message that conveys any information relating to betting or wagering or is intended to assist in it.[28]

These two Sections address various forms of conveying information relating to unlicensed gaming and betting within Canada. The law as it relates to these offences is not well developed and it is difficult to predict with any certainty what would be considered an offence. However, if the gambling activity were viewed as illegal, the provision of information relating to it would also likely be an offence. Thus, any communication of information in Canada relating to an unlicensed online gambling operation could be an offence under this Section. This could include information on a website or communicated online.

SCI created and maintained certain websites in Vancouver. To register to gamble, a gambler had to access one of these sites. If these sites provided information about SCI's gaming, it could have contravened this section. Any other form of SCI advertising directed at Canadians could also be problematic under this Section. However, this Section has yet to be applied to an online casino, so the extent of its application is still uncertain.

f) Section 202(1)(j)

Section 202(1)(j) of the *Code* makes it an offence to aid or assist "in any manner in anything that is an offence under this section".[29] There is no jurisprudence applying this section of the *Code*. Most activities that surround illegal gambling and betting are covered in the previous sections. This section is broad and is most likely intended to catch activities surrounding unlicensed gambling and betting that are not specifically covered in the preceding sections. Without jurisprudence to guide us, it is impossible to say what activities are caught in this section.

It is likely, however, that online activity could be caught under this Section. The Crown could have charged SCI under this Section to cover it. However, because SCI was charged under one of the other Sections, a Section 202(1)(j) charge was likely thought to be redundant. In the absence of proof of the necessary elements, it is unlikely that the Crown could establish the necessary elements of aiding and abetting under this Section.

g) A Telling Exemption: Section 207(1)(h) of the Code

Some guidance in the application of these various prohibitions can be gained by a study of Section 207(1)(h) of the *Code*.[30] This Section states:

Notwithstanding any of the provisions of this Part relating to gaming and betting, it is lawful

(h) for any person to make or print anywhere in Canada or to cause to be made or printed anywhere in Canada anything relating to gaming and betting that is to be used in a place where it is or would, if certain conditions provided by law are met, be lawful to use such a thing, or to send, transmit, mail, ship, deliver or allow to be sent, transmitted, mailed, shipped or delivered or to accept for carriage or transport or convey any such thing where the destination thereof is such a place.[31]

Section 207(1)(h) creates an exemption for the printing of information in Canada relating to gaming and betting that is to be exported and used in a place where it is legal to do so.[32]

The exemption, although narrow in scope, suggests that it is not considered to be contrary to public policy to carry on certain activities in Canada in support of lawful offshore gaming operation.

As the *World Media* decision[33] suggests, the exemption is subject to an important caveat. This potential caveat is that the place or places to which the information is being exported must also view the importing of the information as legal.[34] In this case, the accused corporation was selling shares of tickets in a Spanish lottery. They sent promotional material regarding this sale of shares from Canada to people in the United States. This promotional material was intended to promote participation in the share purchase, which was seen to be gambling. Because the information was created in Canada and exported to the United States, it was then asked whether the Section 207(1)(h) exemption would apply. The Crown brought forth evidence that American law did not consider the importing of this information into the United States legal. Therefore, the court found that Section 207(1)(h) did not apply.[35]

Conclusion: How to Avoid Criminal Liability

Due to the projected growth and profitability of online gaming, many Canadian entrepreneurs may be interested in participating in this industry. Licenses are less expensive offshore than in Canada, where it is often easier to qualify for such a license. This will make it more attractive to obtain a license offshore but try to capture the Canadian market over the Internet. Though this business is proving to be profitable, the potential sanctions under the *Code*, as demonstrated in *Starnet,* make this venture much less attractive. If an unlicensed company still wishes to pursue this venture, it must structure itself in a way that complies with the *Code* or risk such sanctions.

From the facts of the *Starnet* case, the resulting changes SCI made to its corporate structure and through our analysis of the *Code*, perhaps we now have some idea as to how such a company should structure itself to comply with the *Code*.

In short, the prudent approach is to minimize or eliminate all connections with Canada. All download, database and gaming servers should be located in a jurisdiction where online gaming is lawful.

If all connections cannot be severed with Canada, then an online gaming operation should bar all Canadians from access to the gaming activity. If no Canadians can gamble or bet, there is likely no offence under the *Code*. There would be no control of illicit funds and no unlawful agreements to purchase or sell gaming privilege in support of an illegal gambling operation in Canada. The *Code* serves to protect Canadians and without any harm to them, there would not likely be any prosecution under the *Code*. (If the activities constitute an offence in another jurisdiction, the possibility of extradition remains.)

Care should also be taken as to where management resides and decisions are made. If management resides in Canada and decisions are made here, it may be argued that the controlling mind of the operation is in Canada.

The exemption in Section 207 and the SCI restructuring suggest that certain aspects of such an operation, such as software development and perhaps advertising can remain in Canada with some degree of legitimacy. A company that merely develops the software for lawful offshore online gaming operation is not likely in violation of the *Code*.

An advertising group or the branch of the parent company that develops information intended to promote lawful offshore online gaming is also not likely in violation of the *Code*, especially if they merely create this information for the gaming operation. In this situation, an arms length agreement with the gaming operation similar to the one for the software developer is advisable. If, however, they distribute such information as well, they must ensure that they do not distribute it directly into Canada. To be completely sure that they are not in violation of the *Code*, such a group should ensure they do not distribute this information into other jurisdictions that consider the online gaming operation to be unlawful.[36]

---

* Back Ian Kyer is co-director of the Computer and IT Law Group in the Toronto office of Fasken Martineau and is a member of the Steering Committee for the National Technology and IP Group. He is a founder and former President of the Canadian IT Law Association and a former President and Life member of the Computer Law Association.

** Back Danielle Hough is an articling student at Fasken Martineau.

---

[1] Back R.S.C., 1985 c. C-46 [hereinafter *Code*].

[2] Back *Code*, *Ibid.*

[3] Back *Ibid.* ss. 201 to 204, 206, 207 and 209.

[4] Back R. Kelley et al., "Gambling@Home: Internet Gambling in Canada" (2001) CWF Doc. #200111, online: Canada West Foundation http://www.cwf.ca/pubs/200111.cfm?pub_id=200111 (date accessed: 5 November, 2001) at 3-4 [hereafter "Gambling@Home"].

[5] Back Gambling@Home *Ibid.* at 7; Kahnawake Gaming Commission, online: Kahnawake Gaming Commission Homepage http://www.kahnawake.com/gamingcommission/ (date accessed: 9 November 2001).

[6] Back *Code*, *supra* note 1, s. 201.

[7] Back (August 17, 2001), Vancouver 125795-1(B.C.S.C.) [hereinafter *Starnet*]. A copy of this transcript was received from Interactive Gaming Council Canada.

[8] Back *Starnet, Ibid.* at 13.

[9] Back The individuals were probably not prosecuted personally most likely as a result of the deal.

[10] Back *Code*, *supra* note 1.

[11] Back It was only after contacting the Vancouver based servers that clients could be forwarded to the offshore gaming servers.

[12] Back *R. v. Volante* (1993), 14 O.R. (3d) 682 (Ont.C.A.) [hereinafter *Volante*].

[13] Back *Volante, Ibid.*

[14] Back In May 2001, SCI announced the appointment of Michael Aymong as its President and CEO. See, "Starnet Communications appoints new CEO" (25 May, 2001), online: World Gaming homepage http://www.worldgaming.com/news/may25-2001.html (last accessed 16 October, 2001).

[15] Back Since this decision, World Gaming has also established a sales and marketing office in Toronto. See, "Interview with Michael Aymong" (6 July, 2001), *Wall Street Reporter,* online: Wall Street Reporter http://www.wallstreetreporter.com/v2/asp/profile/default.asp?content=99&id=1794&s=1 (last accessed 16 October, 2001).

[16] Back This is to the authors' knowledge.

[17] Back *Code*, *supra* note 1. Section 209 could also apply, but the authors are addressing this paper to online gambling operations that are not intending to defraud clients.

[18] Back *Code*, *Ibid.*

[19] Back *Ibid.*

[20] Back *R. v. Solomon* (1996), 110 C.C.C. (3d) 354 (C.A. Que.) [hereinafter *Solomon*].

[21] Back *R. v. Bear Claw Casino Ltd.*, [1994] 4 C.N.L.R. 81 (Sask. Prov. Ct.).

[22] Back *Code*, *supra* note 1.

[23] Back *Ibid.*

[24] Back Solomon, *supra* note 20.

[25] Back *Regina v. World Media Brokers Inc. et al.* (1998), 132 C.C.C. (3d) 180 (Ont. Ct. Prov. Div.) [hereinafter *World Media*].

[26] Back *Solomon*, *supra* note 20; *World Media*, *Ibid.*

[27] Back *Code*, *supra* note 1.

[28] Back *Ibid.*

[29] Back *Ibid.*

[30] Back *Ibid.*

[31] Back *Ibid.*

[32] Back *World Media, supra* note 25.

[33] Back *Ibid.*

[34] Back *Ibid.*

[35] Back *Ibid.*

[36] Back This concern will be heightened if the countries in question are ones with which Canada has close relations, such as the US.

Published in Canadian Journal of Law and Technology, Vol 1, No. 1.