

**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

COMPETITION TRIBUNAL TRIBUNAL DE LA CONCURRENCE  FILED / PRODUIT Sept. 6, 2005 CT2005-006  Chantal Fortin for / pour REGISTRAR / REGISTRAIRE	
OTTAWA, ONT.	#0015

**SECOND AFFIDAVIT OF RAYMOND F. GRACE**  
**Affirmed September 1, 2005**

**I, RAYMOND F. GRACE**, of the City of Sherwood Park in the Province of Alberta **AFFIRM AND SAY AS FOLLOWS:**

1. I ("**Grace**") am 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 have knowledge of the matters hereinafter deposed to, except where such matters

are stated to be based on information and belief, and where so stated, I verily believe those matters to be true.

2. I make this Affidavit (the "**Grace Affidavit**") 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. I make this affidavit 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**"). While I try to detail the specific paragraph numbers in which the allegation and issue is raised, because Rosatelli continuously repeats himself throughout his, my reply making the reference to specified paragraph numbers may not be all inclusive.

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 I sent 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 I 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 terms Surely 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 were 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 21 of 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 banking 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 Manager 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) transactions 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. Rosatelli read the letter, Exhibit "B", and is aware of the Scotiabank online banking system shortcomings. Nonetheless Rosatelli 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, 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 SOFTWARE 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 banking 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 to 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 Tribunal 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 from 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 Rosatelli 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 through 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 own 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:

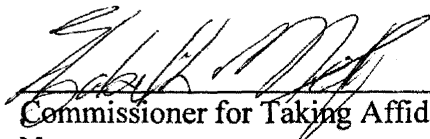
- a. **to address the miniscule but ongoing problem of fraudulent transactions:** the Applicants will permit the Scotiabank to withdraw the amount of the alleged fraud from their account (if the Applicants have not already caught the fraud and already refunded the money) and work with the Applicants, 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.

**AFFIRMED BEFORE ME**

at the City of Sherwood Park  
in the Province of Alberta  
on this 1<sup>st</sup> day of September 2005

  
Commissioner for Taking Affidavits  
Name:

Elizabeth Meddings  
Barrister & Solicitor

  
RAYMOND F. GRACE

----- Original Message -----

**From:** GPAY

**To:** [letty.snethen@scotiabank.com](mailto:letty.snethen@scotiabank.com)

**Cc:** Joseph Iuso ; Adam Atlas

**Sent:** Monday, April 18, 2005 1:37 PM

**Subject:** To Letty Snethen from GPAY Ray Grace

This is the Exhibit "A"  
referred to in the affidavit of  
"Raymond Grace"

Sworn before me this 1st  
day of August, 2005

*Elizabeth Meddings*  
"Elizabeth Meddings"

Elizabeth Meddings  
Barrister & Solicitor

Good afternoon Ms Snethen,

We would like to ask for some assistance in a housekeeping matter in our accounts, as you have instructed us to correspond only with you. We believe that a paper statement is now available on the money manager accounts for \$2.00 per month.

We would like these statements.

Would you be so kind as to instruct the branch to begin issuing these statements.

Finally, we have made a request for a copy of our file maintained at the Bank. Would you be so kind as to confirm when we should expect to receive the copy?

Many thanks for your assistance.

Yours truly,

Raymond Grace

[ray@gpay.com](mailto:ray@gpay.com)

866-344-4729

9 Highvale Cres

Sherwood Park, Alberta T8A 5J7

----- Original Message -----

From: <[letty.snethen@scotiabank.com](mailto:letty.snethen@scotiabank.com)>

To: "Ray Grace" <[gpay@gpay.com](mailto:gpay@gpay.com)>; "Adam Atlas" <[atlas@adamatlas.com](mailto:atlas@adamatlas.com)>

Cc: <[margaretj.parsons@scotiabank.com](mailto:margaretj.parsons@scotiabank.com)>

Sent: Tuesday, April 05, 2005 3:27 PM

Subject: Customer Concern - Follow-up

> Dear Mr. Grace,

>

> Further to our telephone conversation of yesterday and to your follow-up  
> e-mail message, I am still in the process of obtaining background details  
> and information in order to respond to your concerns. I hope you can  
> appreciate that our investigation involves contacting several different  
> areas in the Bank to gather information.

>

> In the meantime, while our investigation is underway, I would ask that you  
> not contact the branch or any other Scotiabank department. If you have  
> questions or concerns, please feel free to contact me directly.

>

> Sincerely,

>

> Letty Snethen

> Senior Manager - Office of the President

> Scotiabank - Executive Offices

> Tel: 877-700-0043

> Fax: 877-700-0045

> ----- Forwarded by Letty

> Snethen/SharedServices/ScotiabankGroup on 04/05/2005 05:33 PM

> -----  
>  
>

> GPAY <[gpay@gpay.com](mailto:gpay@gpay.com)> on 04/05/2005 12:22:33 PM

>

> To: [mail.president@scotiabank.com](mailto:mail.president@scotiabank.com)

> cc: Adam Atlas <[atlas@adamatlas.com](mailto:atlas@adamatlas.com)>

> Subject: GPAY RAY GRACE - ATTENTION LETTY  
> SNETHEN

>

> Attention Letty Snethen,<?xml:namespace prefix = o ns =

> "urn:schemas-microsoft-com:office:office" />

>

> Good morning,

> Thank you for taking the time to speak with us yesterday.

> Here is the email that I sent yesterday.

> About an hour after our conversation I recieved a call from the Fir St

> Branch Manger Margaret Parsons.

> She advised me that a small business client was limited to 1 bankcard per

> principal and 3 accounts per bank card.

> The accounts are limited to 100 transactions per month.

> She advised I need to advise her which three accounts for each business

> that I want to keep.

> She advised that this is ScotiaBank policy.

> I asked what about the other accounts; she said that I could keep them and

> access them at the branch.

> I pointed out that I am processing 750,000.00 per month though the  
> accounts  
> and about 6000 transactions.  
> I asked to be referred to a commercial manager. She advised that it takes  
> a month to get an appointment with a commercial manager.  
> She advised before being referred to a commercial manager I have to  
> comply  
> with the Small Business Policy and choose the 3 accounts first.  
> I asked for an email to explain all this but I have not recieved anything  
> yet.  
> Thank you in advance for any assistance in clearing up this matter.  
>  
> Yours truly  
>  
> Raymond Grace  
> President GPAY  
> Office 780-449-3650  
> Toll Free 1-866-344-4729  
> Cell 780-668-6729  
> Fax 780-416-7641  
>  
>

> ----- Original Message -----  
> From: GPAY  
> To: Steve Burnham  
> Cc: Adam Atlas ; Ryan J Woodrow  
> Sent: <?xml:namespace prefix = st1 ns =  
> "urn:schemas-microsoft-com:office:smarttags" />Thursday, April 04, 2005  
> 10:42 AM  
> Subject: GPAY CONCERNS APRIL 4, 2005  
>  
>  
> Subject: GPAY CONCERNS APRIL 4, 2005  
> Importance: High  
>  
>  
> To [STEVE.Burnham@scotiabank.com](mailto:STEVE.Burnham@scotiabank.com)  
> CC

>

mARGARTEJ.PARSONS@SCOTIABANK.COM;RYAN.WOODrow@sco  
tiabank.com;atlas@adamatlas  
.com

> Good morning Mr Burnham,

>

> Would you be so kind as to lift the block on card 4536056774494709?

> It has been blocked for 10 days now.

> If you are never going to lift the block please extend me courtesy of  
> written notice.

>

> Please send me a written explanation as to why the card was blocked and  
> what provision of the bank act or card user agreement was  
> used to block the card and seize the funds in the account.

>

> Please provide copies of all correspondence that you received from a 3rd  
> party and internal memos that caused you to take this  
> action.

> We are concerned that we have been slandered, and we wish to take action  
> accordingly.

> Our reputation has been damaged and this correspondence and may cost us  
> many millions of dollars of future revenue.

>

> As you are perhaps aware, we were the victim of a fraud. We did  
everything

> we could to protect the bank and the customer.

> We did protect the bank involves as they confirmed. A full refund was  
sent

> to the bank.

>

> We incorrectly thought that we were a valued Bank of Nova Scotia  
customer

> in good standing, clearly not.

>

> The Bank of Nova Scotia is the largest bank in Canada , I cannot believe  
> that you do this by treating all of your business

> customers like me.

>



- > We, and I, Raymond Grace, very much want to continue my good corporate
- > relationship with the Bank of Nova Scotia.
- >
- > Our lawyers have advised us to seek a written response from you to this
- > letter within forty-eight (48) hours.
- > Thank you in advance for your kind cooperation.
- >
- > Yours truly,
- >
- >
- > Raymond Grace
- > President GPAY
- > Office 780-449-3650
- > Toll Free 1-866-344-4729
- > Cell 780-668-6729
- > Fax 780-416-7641
- >

----- Original Message -----

From: <ryan.woodrow@scotiabank.com>

To: <ray@gpay.com>

Sent: Tuesday, March 22, 2005 1:15 PM

Subject: Small Business Account Status

This is the Exhibit "B"  
referred to in the affidavit of  
" Raymond Grace "

Sworn before me this <sup>18<sup>th</sup></sup> 21<sup>st</sup>  
day of August, 2005

*Elizabeth Meddings*  
" Elizabeth Meddings "

Elizabeth Meddings  
Barrister & Solicitor

- >
- >
- > Good Afternoon Mr. Grace,
- >
- > As per our conversations we will require the following information as
- > soon
- > as
- > possible;
- >
- > 1.) A detailed copy of your Joint Venture Agreement with UseMyBank.
- >
- > 2.) A copy of the statement (B of M) confirming that the \$154,000.00
- > Draft issued to yourself was deposited to the GPAY account at Bank of
- > Montreal.
- >
- > Also, as per Bank Policy we provide the following;
- >
- > 1.) A Small Business (sales under \$5 Million) client can only hold "1" Full
- > Service Scotiacard for each owner.
- >
- > 2.) A Small Business client can only hold 3 accounts.
- >
- > 3.) A Small Business client is limited to a total of 150 transactions
- > permitted on the Full Service ScotiaCard issued.
- >
- > Ray, due to the quick expansion/growth and needs of your Business,
- > your business will no longer fall under these requirements.
- >
- > I have made a call to our Commercial Banking Centre to come up with
- > alternate products. Once I have received them, I will forward/discuss the
- > Bank's recommendation with you.
- >

> Thank you,

>

>

> Ryan Woodrow

> Account Manager

> Small Business

>>

> This e-mail message may contain privileged or confidential information.

> If you are not the intended recipient, you may not disclose, use, distribute, or copy this message or attachment in any way. If you received this e-mail message in error, please delete the e-mail and any attachments.

>

**GPAY**  
9 Highvale Cres  
Sherwood Park, Alberta T8A 5J7  
780-464-7244 fax 780-416-7641 toll free 1800-egg-gpay  
Email [gpay@gpay.com](mailto:gpay@gpay.com) Website <http://www.GPAY.com>

March 24, 2005

To The Bank of Nova Scotia  
Sherwood Park Branch

Dear Ryan Woodrow

GPAY currently processes approximately \$500,000.00 per month through the Bank of Nova Scotia. GPAY has enjoyed a very useful and close relationship with the Bank of Nova Scotia. We aspire to continuing our mutually beneficial business relationship.

The purpose of this letter is to address some of the matters that we discussed on March 23, 2005. We wish to provide you with all the information you may wish to have in order to eliminate any concerns you may have.

**ISSUE 1 : \$154,000.00 payment**

The \$154,000.00 money order issued to Ray Grace on Jan 7, 2005.

1. Why did I withdraw \$154,000.00 from my account on January 7, 2005?
  - a. I needed to deposit the money into my Bank of Montreal account and it was faster to get a draft and walk it across the street to the Bank of Montreal and deposit the funds. We can assure you that we will avoid this kind of informal funds transfers in the future.
2. What did I do with the money?
  - a. I walked across Wye road and deposited the funds into the GPAY account 1157-298 transit 00149. (A letter form the Bank of Montreal Wye Road confirming this is attached.)
3. Why was it paid to Ray Grace?

- a. That was a mistake on the BNS teller's part, I actually commented on it but rather than have her redo the draft payable to GPAY I just endorsed it at the Bank of Montreal.

## **ISSUE 2 : Fraud**

Why did the TD Bank send a communication to the BNS advising that fraudulent Email Money Transfers were received by BNS bank card 453 6056 774 494 709 and deposited to account 007412?

- a. We received the four email money transfers into the account using the above noted bankcard. We are, however, the victim of the fraud and not the perpetrator. Someone with a compromised TD bank card made the payments in an attempt to obtaining services from our client. Fortunately our fraud detection software determined that these payments were suspicious at the time of payments. (Actually about 15 seconds after each payment was processed.) We froze the funds pending confirmation of a fraud. Subsequently, we were able to confirm that the payments were fraudulent. The total amount of the four EMT's were \$938.28.

## **GPAY RESPONSE**

- a. We sent a fax to TD security on March 22, 2005 advising that we viewed these EMT's as fraud and advised them to take the money \$938.28 from our corporate account.

## **THE TD's RESPONSE**

- a. The TD Bank instructed the Bank of Nova Scotia to place a hold on the funds of 938.28 and suspend the bank card 453 6056 774 494 709.

## **PROOF OF PAYMENT**

- a. A copy of the fax sent to the TD is attached on March 22, 2005. A copy of our TD corporate account statement shows that the TD debited out corporate account on March 23, 2005.
- b. We have sent an email to TD Security to confirm receipt of the funds to the BNS.

## **COMMENTS**

- a. We are confused as to why we are being penalized for having discovered fraud and advised the TD bank about the fraud. We urge the Bank of Nova Scotia to take into consideration the fact

that the communication it received from TD concerning the fraud had its origins in our own fraud detection system.

- b. We have asked TD to refrain from sending Scotia Security anymore communications accusing us of fraud and instructing the Bank of Nova Scotia to freeze our accounts and block our bankcards.
- c. We protected the TD from a loss and brought a compromised bankcard to their attention.

### **ISSUE 3: Money Laundering**

As a consequence of the claims by the TD Bank, we understand that the BNS is investigating our business for money laundering. We are deeply concerned that our own prudence and diligence is giving us precisely the opposite effect of its intended result.

In an effort to assure all interested parties of the soundness of our business practices, we have had several conversations with FinTrac, the money laundering watchdog for the Canadian federal government. Following from those conversations, we wish to confirm to the BNS the following:

- a. Our business does not process cash or credit card payment.
- b. We only process debit card payments.
- c. The payee is authenticated by their bank.
- d. We only disburse funds electronically to a bank account at a bank.
- e. The bank disbursing the funds to its customer is responsible for identifying the recipient thereof.

We do not money launder.

### **ISSUE 4: Web Site**

Our website points to a Toronto address. The address is a post office box number for mail correspondence. Mail received at that address is simply forwarded to GPAY. The toll free number and email address are forwarded to GPAY.

As it is Bank of Nova Scotia policy that Alberta based business have Alberta contact information on their website we are in the process of updating the websites and should have them completed within a fortnight.

Would you be so kind as to provide us with the following?

- 1) The name of the non small business manager that I have to deal with now;
- 2) A copy of the TD's communication and the Bank of Nova Scotia advising that we perpetrated a fraud;
- 3) Can you remove the hold on the funds?
- 4) Can you unblock our bank card?

We look forward to resolving these matters as soon as possible. Please contact me should you have any questions.

Yours truly,

Raymond F Grace

President GPAY NPAY

References: [tony.matthews@rbc.com](mailto:tony.matthews@rbc.com) , [Sheila.Mashinter@bmo.com](mailto:Sheila.Mashinter@bmo.com)  
[Jack.Busst@td.com](mailto:Jack.Busst@td.com) [stephen.burnham@scotiabank.com](mailto:stephen.burnham@scotiabank.com)  
[Robert\\_Morelli@TD.COM](mailto:Robert_Morelli@TD.COM) [paul.tomniuk@cibc.com](mailto:paul.tomniuk@cibc.com)

# GPAY

GPAY - A Division of B-Filer Inc.  
# 9 Highvale Crescent  
Sherwood Park, Alberta, Canada T8A 5J7  
Tel: 780-464-7244 Fax: 905-669-8452  
Email: gpay@gpay.com

**FACSIMILE COVER PAGE**

To: TD FRAUD Robert Morelli

From: Raymond F Grace

Fax #: 14163086269

Company: TD Canada Trust

MESSAGE:

March 22, 2005

To TD Canada Trust

Att Robert Morelli

Hi Robert,

Here are 4 fraudulent CertaPay payments that we found on the weekend.

DATE	TIME	Client	Name	Email	Phone	Amt	Bank	P address	certapay receipt
20/03/2005	3:59:42 PM	MDCAAA	AMANDA MCCARTHY	lunter@hot-shot.com	9024224990	\$62.55	TD	156.34.222.205	
									C0jgK3mW
20/03/2005	3:13:36 PM	MDCAAA	AMANDA MCCARTHY	lunter@hot-shot.com	9024224990	\$250.18	TD	156.34.222.205	
20/03/2005	2:55:15 PM	MDCAAA	AMANDA MCCARTHY	lunter@hot-shot.com	9024224990	\$250.18	TD	156.34.222.205	
									C00VvX3A
20/03/2005	2:35:26 PM	MDCAAA	AMANDA MCCARTHY	lunter@hot-shot.com	9024224990	\$375.27	TD	156.34.222.205	
									C0xKJhgh

The total is 62.55 + 250.18+250.18 + 375.27 CDN =938.28.

Please take the funds from our TD account 322489 transit 82389.

*Ray Grace*  
Yours truly,

Raymond Grace



- Personal
- Small Business**
- Customize Site
- Rename Accounts
- Open New Account
- Session History
- Change Password

### View Accounts

### [Help](#)

### Account Activity

[Print this page](#)  
[Make a Stop](#)

GPAY - 322489 \$3,164.15

Last 10 Days

Balance Date: Mar 24, 2005

[Bottom](#)

Date	Description	Debit	Credit	Balance
Mar 23, 2005	GC 5370-DEBIT ADJUST	938.28		\$3
<a href="#">About This Statement</a>				
			Mar 24,	

[Top](#)

to:

All transactions to the close of the previous BUSINESS day downloaded.

[Information about supported versions of software for downloads.](#)

[Print this page](#)

- EasyWeb
- Quick Links
- Pay Bills
- Make a Transfer
- Order Mutual Funds
- WebBroker
- Download Accounts
- US Banking

This is the Exhibit "C" referred to in the affidavit of "Raymond Grace"

Sworn before me this 1st day of August, 2005

September  
"Elizabeth Meddings"

Legal

## Terms and Conditions of Use

Elizabeth Meddings  
Barrister & Solicitor

### 1. Acceptance of terms

Your use of UseMyBank is subject to the following Terms and Conditions of Use. UseMyBank reserves the right to update and change, from time to time, these Terms and all documents referenced. The most recent version of these Terms can be found at <http://www.UseMyBank.com/legal.asp>.

### 2. Transaction providers

You understand that the Transaction Provider may not have consented to and/or endorsed, and/or may not have knowledge of its inclusion as a designated Transaction Provider, and/or access by you to its Online Service, and that in the context of UseMyBank as an acting agent on your behalf, and not on the behalf of any Transaction Provider. You understand that UseMyBank provides a link to the Transaction Provider for your convenience, but that (i) you activate such a link you will be using UseMyBank to access the Transaction Providers web site, and (ii) you are responsible for bill payments or email money transfer made by you using this service.

### 3. Description of use

UseMyBank is a service that facilitates account information and bill payment or email money transfer from your preferred online Transaction Provider. The providers and sources of your online accounts are referred to in these Terms as "Transaction Providers". The account information that is collected from these Transaction Providers is used on your behalf (ie. account information, Bill payee, etc). In order to access the account information from these Transaction Providers, UseMyBank will request your online Login Information. "Login Information" is your user ID, password, Personal Information Number (PIN), and other information that provides online access to the appropriate account information and billing facilities. The terms "Login Information" and "Account Information" are collectively referred to in these Terms as "Buyer Information." Please note account access from these Transaction providers will be used to process bill payment or email money

transfer transactions from the selected account and at no time will the account information of login information be logged, and hence cannot be used in the facilitation of any transactions. UseMyBank is simply a facilitator, all rules and regulation governing the transferring of funds is provided by NPAY(NPAY Inc. which is the corporation that has Biller account with the Transaction Providers). Transaction Providers may prohibit the disclosure of Login Information or deny liability to the user if Login Information is disclosed. It is the users responsibility to review their agreements with the Transaction Providers to determine whether disclosure is permitted, what the consequences of such disclosure are and what liability will be in connection with such disclosure.

- i. For funds transfer, the Seller and Affiliate Terms and Conditions can be found by clicking [here](#)
- ii. For funds transfer, the Buyer Terms and Conditions can be found by clicking [here](#).

**4. 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.

**5. Privacy**

Certain information, required by law, will be requested through your Transaction Provider. This information is solely used in the Facilitation Service of UseMyBank. All other information is subject to UseMyBank privacy policy statement

(<http://www.UseMyBank.com/PrivacyBotSecurity.asp>).

UseMyBank may contact you via your email address regarding your account status, provide information to you about enhancements of our services, and respond to your questions or comments about your transactions or other items.

**6. Method of communication**

To the fullest extent permitted by applicable law and usage, this Agreement and any other agreements, notices or other communications regarding your membership and/or your use of the UseMyBank Service, may be provided to you electronically and you agree to receive Communications in an electronic form. Electronic Communications may be posted on the pages within the UseMyBank website and/or delivered to your email address. You will print a copy of any Communications and retain it for your records. All Communications in either electronic or paper format will be considered to be in "writing," and to have been received no later than five (5) business days after posting or dissemination, whether or not you have received or retrieved the Communication. UseMyBank reserves the right but assumes no obligation to provide Communications in paper format. In Ontario, please refer to the Electronics Commerce Act. Your consent to receive Communications electronically is valid until you revoke your consent by notifying UseMyBank of your decision to do so, by sending an email message to [support@UseMyBank.com](mailto:support@UseMyBank.com). If you revoke your consent to receive Communications electronically,

UseMyBank may terminate your right to use the UseMyBank Service.

**7. Anti-spam**

You agree not to use unsolicited email, usenet, message board postings, or similar methods of mass messaging (spam) to gather referral bonuses. The use of spam to promote the UseMyBank Service has strict negative consequences. UseMyBank will immediately and permanently terminate the account of any member who has used unsolicited email to gain referrals. In addition, you may be subject to Canadian provincial and federal penalties and US state and federal penalties and other legal consequences under applicable law if you send unsolicited email. Our Anti-Spam Policy is intended to protect our members, the Internet, and UseMyBank.

**8. Specific limitation of liability**

UseMyBank's facilitation service do not assume responsibility for malfunctions in communications facilities that may affect the accuracy or timeliness of transactions or information you send or that is provided to you via online access to the site. UseMyBank's service is also not responsible for any losses or delays in transmission of instructions arising out of the use of any Internet service provider providing connection to the Internet or caused by any third party software or systems. In the event that a court should hold that the limitations of liabilities or remedies available as set forth in these Terms, or any portions thereof, are unenforceable for any reason, or that any of your remedies in connection with the online access fail their essential purpose, you expressly agree that under no circumstances will UseMyBank and its facilitation service have any liability to you or any party claiming by, through or under you for any cause whatsoever, and regardless of the form of action, whether in contract or in tort, including negligence or strict liability, in the aggregate, exceed \$5,000 (Canadian.). Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, in such cases liability is limited to the extent permitted by law.

**9. Exchange Rates**

Best efforts are made to obtain the most accurate and timely exchange rates from Bank of Canada. UseMyBank does not guarantee the accuracy, timeliness, reliability or completeness of this service from Bank of Canada. As a user, you acknowledge and

agree that any reliance on or use by you of the exchange rates shall be entirely at your own risk. In no event shall UseMyBank nor any of its bill payment or email money transfer providers be liable for any direct, indirect, consequential or exemplary damages arising from the use or the performance of the exchange rates provided by Bank of Canada.

**10. Specific disclaimer of warranties**

YOU EXPRESSLY AGREE THAT USE OF ONLINE ACCESS IS AT YOUR SOLE RISK. NONE OF USEMYBANK'S, THIRD PARTIES, TRANSACTION PROVIDERS, OR THEIR RESPECTIVE LICENSORS, AFFILIATES, EMPLOYEES, DISTRIBUTORS OR AGENTS WILL HAVE ANY LIABILITY FOR ANY DIRECT, INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR OTHER DAMAGES SUFFERED BY YOU OR ANY OTHER PARTY (REGARDLESS OF WHETHER OR NOT SUCH PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM: (I) THE USE OR THE INABILITY TO USE THE SERVICE; (II) THE COST OF OBTAINING SUBSTITUTE GOODS OR SERVICES RELATING IN ANY MANNER TO YOUR USE OR NON-USE OF THE SERVICE; (III) UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA; (IV) STATEMENTS OR CONDUCT OF ANYONE ON THE SERVICE; OR (V) ANY OTHER MATTER RELATING IN ANY MANNER TO THE SERVICE.

**11. Termination**

Either you or UseMyBank may terminate your use of this service at any time without prior notice. You can cancel your transaction at any time during the use of this service at any time and have your information deleted from our records. The UseMyBank Terms of Service which apply to your use of your online account and transaction providers, provides that UseMyBank expressly reserves the right to immediately modify, suspend or terminate your transaction and refuse current or future use of any UseMyBank service, including online transaction processing. If UseMyBank in its sole discretion believes you or someone using your online access has: (i) violated or tried to violate the rights of others; or (ii) acted inconsistently with the spirit or letter of the UseMyBank's Terms.

**12. Invalidity of specific terms**

If any provision of these Terms or any document incorporated by reference is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in the provision, and the other provisions of the such documents remain in full force and effect.

**13. Age of use**

You agree and accept that payments that require age verification have been completed and accepted. UseMyBank services restrictions are not limited. All use is governed by the Transaction Providers and Third Party suppliers.

**14. Legal matters**

The UseMyBank Terms which apply to all use of the online access through the transaction providers, provides that both you and UseMyBank agree that any dispute or controversy arising out of or relating to any interpretation, construction, performance or breach of these Terms, shall be settled by arbitration to be held in Toronto, Ontario, before a single arbitrator and in accordance with the Commercial Arbitration Rules then in effect and/or pursuant to the statues of Ontario, and in particular, the Arbitrations Act. Each party irrevocably and unconditionally consents to the jurisdiction of any such proceeding and waives any objection that it may have to personal jurisdiction or the laying of venue of any such proceeding. The parties will cooperate with each other in causing the arbitration to be held in as efficient and expeditious a manner as practicable. If the parties are unable to appoint a mutually acceptable arbitrator within thirty (30) days after a party gives written notice to the other requesting resolution of a dispute, the a Ontario court shall appoint the arbitrator in accordance with such Commercial Arbitration rules and/or the Arbitrations. The arbitrator may grant any and all relief permitted by the Arbitration Act. The decision of the arbitrator shall be final, conclusive and binding on the parties to the arbitration. Judgment may be entered on the arbitrator's decision in any court having jurisdiction. Nothing herein shall prevent the parties from settling any dispute by mutual agreement at any time.

**15. Indemnities**

EXCEPT WITH RESPECT TO CLAIMS, COSTS, AND LIABILITIES ARISING PRINCIPALLY BY REASON OF USEMYBANKS' NEGLIGENCE, YOU WILL INDEMNIFY

USEMYBANK AGAINST ANY CLAIM, COST AND LIABILITY INCURRED BY YOU IN CONNECTION WITH USEMYBANK PROVIDING ITS FACILITATION SERVICE. IN ADDITION, YOU AGREE TO RELEASE USEMYBANK FROM ANY CLAIM, COST, AND/OR LIABILITY INCURRED BY YOU IN CONNECTION WITH THE USEMYBANK SERVICE, EXCEPT FOR THOSE ARISING PRINCIPALLY BY REASON OF USEMYBANKS' NEGLIGENCE.

**16. Language**

It is agreed that this Agreement and all related documents, including notices, be drawn up in the English language only.

**17. Code of Practice**

UseMyBank endorses the Canadian Code of Practice for Consumer Debit Card Services and is committed to maintaining and/or exceeding the level of customer protection for all its clients. Note: this is a voluntary code.

**18. Notices**

- i. The following legal agreement details the users responsibilities and obligations along with UseMyBank/NPAY with its facilitation of online bill payments or email money transfer from accounts of these Transaction Providers and by using this service you agree to be bound by same.
- ii. A copy of this agreement will not be mailed to the user. Please print or save this agreement by using the "Print" or "File/Save" options the appropriate Internet browser.

April 25, 2005



**Scotia Casinos**

This is the Exhibit "D" referred to in the affidavit of "Raymond Grace"

Sworn before me this 31st day of August, 2005

*Elizabeth Meddings*

Elizabeth Meddings  
Barrister & Solicitor

Based on an internet search of publicly available information, the following is a list of casinos in which the Bank of Nova Scotia has invested or participated:

	<b>Name</b>	<b>Address</b>	<b>Bank of Nova Scotia Participation</b>
1.	Caesars Palace--Las Vegas	3570 Las Vegas Boulevard, Las Vegas, Nevada, USA 89109 Tel: 877-427-7243	Bank of Nova Scotia is a lead bank in a syndicate of banks for \$3 billion financing (together with Casinos 2 and 3), July 15, 1999.
2.	Caesars Palace-Lake Tahoe	Lake Tahoe, Nevada, USA	Bank of Nova Scotia is a lead bank in a syndicate of banks for \$3 billion financing (together with Casinos 1 and 3) July 15, 1999.
3.	Caesars Atlantic City (N.J.)	2100 Pacific Avenue Atlantic City, New Jersey, USA 08401 Tel: 800-443-0104	Bank of Nova Scotia is a lead bank in a syndicate of banks for \$3 billion financing (together with Casinos 1 and 2) July 15, 1999.
4.	Aladdin Resort & Casino	3667 Las Vegas Boulevard South Las Vegas, Nevada, USA 89109 Tel: 702-785-5555	Bank of Nova Scotia arranger of the \$410 million Senior Bank Facility, February 26, 1998.
5.	MGM Grand	3799 Las Vegas Boulevard South Las Vegas, Nevada 89109-4340, USA Tel: 702-891-1111	Bank of Nova Scotia lead bank in a syndicate of banks financing \$3 billion, April 13, 2000.
6.	St. Kitts Marriott	858 Frigate Bay Road; Frigate Bay,	Bank of Nova Scotia banking services provided

	Resort & The Royal Beach Casino	St. Kitts, British West Indies Saint Kitts And Nevis	to co-owner of casino, Mr. De Zen, February 2, 2005.
7.	Lima Marriott Hotel and Stellaris' Casino	Malecón De La Reserva 615, Miraflores, Lima, Peru	Bank of Nova Scotia receives \$27 million in loan guarantees for its investment in the casino, April 3, 2002
8.	Resort & Casino At Bahamia	P.O. Box F-207 Freeport, Bahamas	Bank of Nova Scotia operates an ATM located in the Casino at Bahamia; funds are given in U.S. currency. It accepts VISA, MasterCard, American Express cards, and any other bank or credit card on the Cirrus, Honor, and Novus networks.
9.	Harrah's Cherokee Casino	777 Casino Drive Cherokee, North Carolina 28719 USA	Bank of Nova Scotia agent for senior bank facility for construction of \$83 million casino owned by the Eastern Band of Cherokee Indians, 1997.
10.	Atlantis Paradise Island Bahama	Bahamas Tel: 242-363-3000	Bank of Nova Scotia hired by Sun International Hotels Ltd. to arrange financing for casino worth \$100s of million, January 20, 2000.

- Account Information
  - Account Summary
  - Account Details
  - Creditor Insurance Details
  - Today's Activity
  - Pending Transactions
- Account Services
  - Order Cheques
  - Mortgage Renewals
  - Verified by VISA Service

This is the Exhibit "E" referred to in the affidavit of "Raymond Grace"

Sworn before me this 31st day of August, 2005

*Elizabeth Meddings*

Elizabeth Meddings  
Barrister & Solicitor

 Print

**Account Details**

\*\*\*\*\*

**Account:**


**More Actions for this Account:**

Select... 

Account Type	Account Number	Balance	Available Credit
ScotiaGold	4538*****	\$*****	\$*****.00

**Payment Information**

Current	
Balance	\$*****
Overdue Payment	\$0.00
Overlimit Amount	\$0.00
Total Minimum Payment Due	\$0.00
Last Payment	
Amount	\$*****
Date	2005-**-*
Last Statement	
Balance	\$*****

 Scotia Rewards

**Your Scotia Rewards Points total is:**  
\*\*\*\*\*

Points are as of last business day

To redeem your points or browse the catalogue online, click here.

<b>Minimum Payment</b>	\$0.00
<b>Payment Due Date</b>	2005-09-**

Did you know you can apply for a limit increase on your personal Scotiabank VISA\* card? Apply now.

 ScotiaStar Network

ScotiaGold customers can earn up to 10x the points at participating merchants.

**Become a ScotiaStar Member Enroll today.**

### Get Transaction Details

Since Date (Optional)   -  -

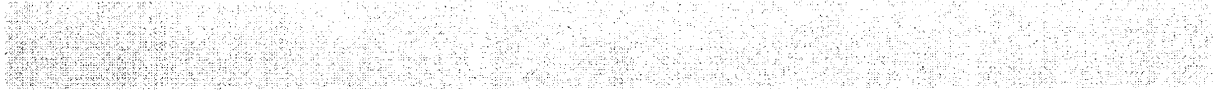
yyyy - mm - dd

### Items Posted Since Your Last Statement

Transaction Date Sort ▲	Transaction Description Sort ▲	Amount
2005-08-18	PC BANKING PAYMENT	\$***** -
2005-08-25	*****	****
2005-08-25	*****	*****
2005-08-25	*****	\$***
2005-08-25	POKERSTARS INTERNET GI AMT = 400.00 GI	\$491.60CDN

### Items on Your Last Statement

Transaction Date Sort ▲	Transaction Description Sort ▲	Amount
----------------------------	-----------------------------------	--------



**Note(s)**

- 1 Net amount posted since last statement: (debits - credits) \$296.29 .  
Does not include any items which may have been authorized but not yet posted to your Account.

 **Print**

**Download or Export Your Transactions**



**Download or  
Export to**

Quicken 

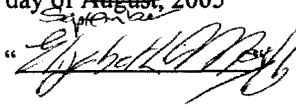
**AI2-b - Account Details**



Website Identity for:

[www.usemybank.com](http://www.usemybank.com)

Please verify that the information below is consistent with the site you are visiting.:

Name : <a href="http://www.usemybank.com">www.usemybank.com</a>	This is the Exhibit " F " referred to in the affidavit of " Raymond Grace "
Validity Period : 9/14/2004 - 9/14/2005 (month)	
Information : E= CN= <a href="http://www.usemybank.com">www.usemybank.com</a> OU= UseMyBank Support O= UseMyBank Services L= Toronto S= Ontario C= CA Domain Control Validated See <a href="http://www.ipsca.com">www.ipsca.com</a>	Sworn before me this <u>31st</u> day of <u>August</u> , 2005  Elizabeth Meddings Barrister & Solicitor

If the information is correct, you may submit sensitive data to this site with the assurance that:

- This site has an ipsCA Server Certificate.
- ipsCA has verified this site has the control of the domain associated with this server
- All information sent to this site, if in an SSL session, is encrypted, protected against disclosure to third parties.

To ensure that this is a legitimate ipsCA Certified Server , make sure that:

1. The original URL of the site you are visiting comes from [www.usemybank.com](http://www.usemybank.com) .
2. The URL of this page is <https://www.usemybank.com> .
3. The status of the Server ID is Valid.

© 1995, 2004 ipsCA, IPS Certification Authority, S.L. Todos los  
derechos reservados

For Server Certificates, Signature and Encryption Tools please visit

<http://certs.ipsca.com>

<https://certs.ipsca.com>

ClientName

FIGHT DIRECTORS  
CANADA  
RAINBOW MAGIC COMP  
MELODY WIGDAHL  
SIP Group  
WILD ROVER  
PROMOTION  
PRINCESS MARGARET  
CYBER MILIEU  
PAYMENT  
WHITLANDS PUBLISHIN  
ETHERLINX E-BUSINESS  
CROSSLAND  
CREATIONS  
IPROFIT NETWORK  
ANNE VANVLACK  
ASHLEY MADISON  
AGEN  
FUN FOR LIFE CLUB INT  
PAUL LIMA  
PRO LIGHTS Anthony  
Demarco  
DOMINIC RIBUFFO  
DUALIES INC WILLIAM  
SINGLEPOLITAN.COM  
ENDLESSADS.COM  
BEE ALIVE  
DISTRIBUTING  
Youth Athletic COP  
Media Dial Comm Inc  
www.kissandtalk.com  
CATAALLIANCE  
PATRICK DJIMI  
www.AmberOne.com  
PCS 11 Purchase on Net  
Netgiro  
Advanced Dermal Solutions  
Inc.

This is the Exhibit "G" referred  
to in the affidavit of "Raymond  
Grace"

Sworn before me this <sup>12<sup>th</sup></sup> ~~8~~ 1st day of  
~~August~~ <sup>September</sup>, 2005

*Elizabeth Meddings*  
"Elizabeth Meddings"

Elizabeth Meddings  
Barrister & Solicitor



SIA Limited  
Hadaway Hilton  
HINDUSTAN PORTALS  
INC  
ICICI Bank (India)

- About Fried Frank
- Attorneys
- Practice Areas
- What's New
- Publications
- Email Alerts
- Offices
- Pro Bono
- Recruiting
- Alumni
- Search the Site
- Other Legal Links
- Home



## Articles by 21st Century Money, Banking & Commerce Alert and BancMail Authors

This is the Exhibit "H" referred to in the affidavit of "Raymond Grace"

Sworn before me this 31st day of ~~August~~ September, 2005

"Elizabeth H. Melby"

### Scrape It, Scrub It and Show It:

#### The Battle Over Data Aggregation

by Thomas P. Vartanian and Robert H. Ledig

#### I. Introduction

The potential of the Internet to consolidate and manipulate information has a significant new application in data aggregation. This service offers users the opportunity to consolidate the usernames and passwords (collectively "PINs") that permit them to access a variety of PIN-protected websites that contain information about their personal accounts on a single website by using one master PIN. These online account providers could be financial institutions, stockbrokers, airline frequent flyer and other reward programs, e-mail accounts and any other website offering PIN-protected personal accounts to users. This paper will focus on financial institutions as sources of account information used by data aggregators since this sector now provides widespread access to customer account data through the Internet.

The attraction for users is the convenience of replacing PIN-protected sites numerous PINs with the use of one master PIN to access the aggregator site. The need to visit multiple websites and record or remember many PINs in order to obtain account information or to log on to PIN-protected sites is removed. Moreover, the user can see a comprehensive picture of their

overall financial picture in a single convenient format. In return, the aggregator and/or a hosting website gains a potentially significant marketing opportunity.

This paper sets forth the basics of how account aggregation works and explores some of the issues it raises. After an outline of the nature of the service and a brief history of events since the first aggregation service was announced, the paper outlines some of the relevant legal questions.

## **2. Basic Approaches to Data Aggregation**

Data aggregation or (more pejoratively) "screen scraping" is gathering, at an account holder's request, the account or other information from designated websites using that account holder's PINs and making that user's account information, taken from a range of sources, available to them at a single website operated by the aggregator.<sup>1</sup>

An aggregation service may be offered on a standalone basis or may be offered either in conjunction with other financial services, such as portfolio tracking and bill payment provided by a specialized website, or as an additional service to augment the online presence of an enterprise well-established outside the virtual world (such as a bricks and mortar financial institution). As discussed below, a range of established companies with an Internet presence appear to recognize the value of offering an aggregation service to augment other web-based services and attract visitors. In this regard, offering a data aggregation service as a vehicle to a website may be viewed as particularly attractive because of the potential that it will regularly draw users of the service to the hosting website.

In order to enroll in an aggregator service, the user provides the PINs for the accounts they wish to access through the service. The aggregator then uses these PINs to access the user's accounts. As discussed below, there are a variety of approaches aggregators have taken in dealing with account providers, in how the information is extracted and in the functionality available to the user accessing their accounts from the aggregator's site.

### **2.1. Data Aggregators Interaction and Relationship with Information Providing Websites**

The aggregator and institution may agree on a data feed arrangement activated on the customer's request, using the Open Financial Exchange

("OFX") standard to request and deliver information to the site the customer has selected as the venue from which they will view their account data. Such agreements provide an opportunity for institutions to negotiate to protect their customers' interests and offer aggregators the opportunity to provide a more robust service than is possible through other methods. However, developing these relationships is time consuming and many account providers may not yet have decided to cooperate with aggregators in this manner.

A lower level of consensual relationship may be reached in the case of aggregators who agree with information providers to extract data without using an OFX standard. Thus "scraping" or HTML technology may be used to obtain account data, but for business or other reasons, the aggregator may choose to obtain prior consent and negotiate the terms on which customer data is made available.

"Screen scraping" without content provider consent has the advantage of allowing subscribers to view almost any and all accounts they happen to have opened anywhere on the Internet through one website. As no pre-existing relationship between the aggregator and the content provider is required, the number of potential sites from which data may be harvested by the aggregator is limited only by the PINs the customer is willing to provide and by any restrictions the aggregator puts on its own activities.

## **2.2. User Interaction with Data Aggregators**

The information obtained by the aggregators from the content-providing site may be displayed on a "read-only" basis, which does not allow the customer to perform transactions, but merely to view account balances and history on the aggregator's website. This service may be teamed with a bill payment service. Users obtain an "available" balance after bills paid through the service are deducted from the account balance obtained from their financial institution.

Data aggregators may also include a link on their site that takes the user directly to their account providing institution's website. The link may take the user to the institution's log on page where the user is required to enter their PIN with the institution in order to be able to enter transactions on the site or it may take the user directly into the PIN-protected section of the institution's website without any further PIN entry.

### **2.3. How Aggregators Obtain Access to User's Account Data**

If an aggregator is able to obtain account data from an information provider using OFX (or some other standard or protocol enabling a direct data feed) once a customer has authorized the transfer by providing the aggregator with their account number and PIN, then an aggregator could provide around-the-clock "real time" account information and possibly transactional functionality no different from that the institution itself provides, assuming the institution is willing to deliver this level of access.

On the other hand, non-direct feed data aggregation, whether consensual or not, involves the aggregator periodically logging into its users' accounts with their PINs, extracting account balances (and potentially transaction history) and holding it on its own servers for presentation to the user in the event they access the aggregator's site. As this information is not "real time," it may be refreshed more or less frequently depending on the resources the aggregator chooses to devote to maintaining the currency of the data it presents to its users. The ability to perform transactions involving the account can only be provided by a link to the customer's account within the institution's website.

### **2.4. Data Aggregator Usage of Information Obtained in Data Aggregation Activities**

Data aggregation by definition involves the transfer of large amounts of account data from the account provider to the aggregator's server. Over time, this could develop into a comprehensive profile of a user, with details of their banking and credit card transactions, balances, securities transactions and portfolios, travel history and preferences and numerous other types of personal information. With the growing sensitivity to data protection considerations, there is likely to be considerable focus on the extent, if any, to which data aggregators may seek to use this data either for their own purposes or to share it on some basis with the operator of the website on which the service is offered or with other third parties.

## **3. A Brief History**

Data aggregation, although only a recent phenomenon, has developed rapidly as the events outlined below illustrate.

May 25, 1999 -- Ezlogin.com announces the launch of its "JumpPage" service which automates the usual steps required for access, registration and sharing of personal web services.<sup>2</sup> The site launches officially on July 26, 1999.<sup>3</sup> The JumpPage service is apparently available both through the Ezlogin site itself and partner sites. Ezlogin.com allows partner sites to offer their users a single point of sign-on to online accounts, as well as the ability to consolidate, access and manage personalized content from virtually any source on the Internet.<sup>4</sup>

August 2, 1999 -- VerticalOne launches what it calls the first account aggregation service. The service operates solely through partner sites and provides current account information to users and links to partner content providers sites. It operates exclusively through partner sites to provide current account information to users from the partner site and quick links into the content providers' sites. It relies primarily on non-consensual data aggregation to obtain account data.<sup>5</sup> VerticalOne is reported to be the leader "in terms of the maturity of its product, . . . [and] . . . the numbers of consumers using the firm's site to access their accounts."<sup>6</sup> As of mid-May, 2000 the company was reported to be providing a version of the service on twelve Internet portals (including iVillage.com, go.com, and wfn.com) and with 86,000 people registered to use the VerticalOne service.<sup>7</sup>

December 29, 1999 -- First Union announces requirements for aggregators to access its website. The nine requirements for any agreement with an aggregator represented the first attempt by the banking industry to exert some control over the activity. In a press release, the bank said that the requirements would enable it to "oversee aggregator activities on firstunion.com and address such issues as privacy and information sharing, customer authorization to access accounts, confidentiality of data, contractual agreements, technical and security audits, and indemnification against losses."<sup>8</sup>

December 30, 1999 -- First Union files a complaint against Secure Commerce Services ("SCS"), the providers of the Paytrust bill payment service,<sup>9</sup> in North Carolina concerning the Paytrust "Smartbalance" feature.<sup>10</sup> Among other things, the complaint alleged unauthorized access to a computer, trademark and copyright infringement, misrepresenting its relationship with First Union and misleading customers.

January 2000 -- eBay files complaints against ReverseAuction.com and Biddersedge.com, alleging unauthorized mass copying of auction listings and seller details from the eBay site for their own purposes.

February 10, 2000 -- Ezlogin.com announces that its "personalization infrastructure tools" provide automated access to 2,500 sites, including 700 financial sites, 500 shopping sites, 425 information sites, 325 communications sites, 250 Internet tools and services, 200 personal interest sites and 100 travel and award-related sites.<sup>11</sup>

February 28, 2000 -- First Union drops its legal action against SCS as Paytrust agreed to meet the conditions set in First Union's Internet Aggregation standards.<sup>12</sup>

April 20, 2000 -- Intuit announces its financial aggregation service (MyFinances) available through the Quicken.com website and agreements with 33 banks, fifteen brokerages and eight credit card companies to allow Intuit to aggregate account information from their websites at their customers request. Relationships with another 57 banks and credit card companies are anticipated.<sup>13</sup> Intuit, which provides the service through Yodlee, indicated that it aggregates only after coming to an agreement with the account provider.<sup>14</sup>

April 19, 2000 -- First Union announces plans to introduce an aggregation service by the end of the year.<sup>15</sup>

April 25, 2000 -- CNBC announces an agreement with VerticalOne to offer account aggregation on its website.

May 9, 2000 -- Microsoft announces that its MSN MoneyCentral website was the first to go live with Corillian software.<sup>16</sup> Corillian provides account aggregation software to other websites and is quoted as planning a network of affiliated financial institutions sharing account data for presentation on websites, using the OFX messaging specification. It uses proprietary methods to obtain data from institutions that are not yet OFX-enabled.<sup>17</sup>

May 15, 2000 -- eBalance, Inc., announces a new version of its platform allowing users to interact with all of their financial information on one site, providing individual account and transaction data from more than 1,300 financial institutions.<sup>18</sup>

## **4. Challenges to Data Aggregation**

The response by financial institutions to data aggregation has been wary. Institutions are concerned, among other things, about the possibility of liability arising from data aggregation activities, potential security problems, infringement on intellectual property rights, and the possibility of diminishing traffic to the institution's website.

### **4.1. First Union Requirements for Aggregation**

In December 1999 First Union issued guidelines that attempted to manage some of their perceived risks to the banks systems and maintaining the security and privacy of customer data. The guidelines provide that First Union will obtain a written agreement with aggregators holding them to the following requirements:

- First Union customers authorize the aggregator service with full and meaningful disclosures to ensure that they understand the risks associated with sharing their authentication information with a third party.
- Aggregators protect both the customer's bank authentication information and the aggregator's customer authentication information using industry standards, such as encryption and authorization.
- Aggregators use First Union reviewed and approved technologies in order to access information and perform transactions on behalf of a First Union customer.
- The aggregator provides the ability for First Union to identify and track aggregator activities on First Union's site and to be able to differentiate aggregator activities from direct customer initiated activities.
- The aggregator agrees to establish a process to ensure the validity and accuracy of all data displayed by an aggregator.
- The aggregator agrees to establish a process to protect the confidentiality and security of customer data and to limit information sharing.
- The processes established by the aggregator enable First Union to continue to adhere to all banking and financial service laws, regulations and corporate policies.



- The aggregator agrees to establish a process that provides end-to-end audit trails at the system and transactional level to enable First Union to validate the source, authorization and execution of transactions.
- The aggregator agrees to allow a First Union approved third party to perform a security and process assessment on a regular basis at First Union's expense.

#### **4.2. First Union Litigation**

The day after it issued these guidelines, First Union filed a complaint against SCS in North Carolina.<sup>19</sup> Prior to filing the complaint, First Union had expressed concern regarding the "Paytrust Security Guarantee" that every transaction would be "100% safe" and made a written demand to SCS that SCS cease use of the Smartbalance feature and remove First Union customer account number data and account information from its computers. SCS declined to do so.

The complaint made nine claims:

- Unauthorized access (by continuing to copy customer account information after First Union had written demanding that the practice cease) to a computer operated by a financial institution, thereby obtaining a financial record of a financial institution in violation of the Computer Fraud and Abuse Act.
- Trespass to chattels under common law by interfering with computers and software that are the property of First Union and computer trespass under state law.
- Infringement of First Union's registered service mark under federal law and state common law arising out of its use on the Paytrust website.
- False designation of origin and unfair and deceptive trade practices arising out of the implication that the Smartbalance feature is affiliated with or endorsed by First Union.
- Copyright infringement for copying portions of the First Union website and republishing it to users of the paytrust.com website.
- Misappropriation of First Union's intangible trade values and commercial property by accessing and copying portions of the First Union Online Banking Service, extracting and reformatting time sensitive commercial data from that service and republishing it to

others on paytrust.com for financial gain in competition with the First Union Online Banking Service.

First Union said that the suit was "strictly a privacy and security issue."<sup>20</sup> The settlement of the case in February 2000 was reported to be based on an agreement by SCS that it would meet the First Union's aggregation standards.<sup>21</sup>

### 4.3. eBay Litigation

Apart from consolidating consumers' financial and other online accounts, non-consensual data aggregation has also been used by online auction sites to expand their auction inventory. In January 2000, eBay brought actions in California against two sites that scraped eBay's site, Bidder's Edge and Reverse Auction Inc.

eBay alleged that Biddersedge.com selectively copied truncated auction listings hosted on other auction sites, including eBay, onto its home site, and "using a . . . format imitative of that . . . used by eBay . . . claims that it is 'a free service which allows you to search across many auction sites at once.'<sup>22</sup> In the event a user wishes to bid, they must go to the site hosting the auction. In November 1999, eBay wrote to Bidder's Edge to advise that it was not authorized to access the eBay site for purposes of copying auction listings, and that eBay did not wish to be included on the Bidder's Edge site. Nevertheless, the practice continued. eBay's claims against Bidder's Edge included the following:

- Trespass to personal property for interference with eBay's computer systems;
- Violation of the Computer Fraud and Abuse Act for unauthorized access to, thereby obtaining information from a protected computer;<sup>23</sup>
- Unfair business practices, false advertising, injury to business reputation, federal trademark dilution and unjust enrichment for the inferences of an association between the parties made by Bidder's Edge.

ReverseAuction.com allegedly would copy eBay's users' e-mail addresses, user ids and feedback ratings, then send these users e-mails falsely warning that their eBay id will "expire" soon and offering the opportunity to let them use their id and accompanying feedback rating on ReverseAuction's website. Ebay's claims against ReverseAuction.com are substantially similar to those

against Bidder's Edge, with the addition of allegations of violation of the Electronic Communications Privacy Act and the omission of an allegation of misappropriation of eBay's property under state law.<sup>24</sup> The Federal Trade Commission ("FTC") also brought an action against ReverseAuction concerning the unfair or deceptive aspects of the ReverseAuction operation.<sup>25</sup>

The court granted eBay a preliminary injunction in the Bidder's Edge case on May 24, 2000, based on a finding that the trespass claim had sufficient likelihood of success to grant the relief requested, without addressing the remaining claims.<sup>26</sup> The claim of trespass required eBay to show that Bidder's Edge had intentionally interfered with its possessory interest in the computer system, causing loss to eBay. The court found a likelihood that the activities of Bidder's Edge were sufficiently outside the scope of the use permitted by eBay as to be unauthorized activities. To the extent Bidder's Edge activities imposed even a small burden on eBay systems, the court found that eBay could show that it was deprived of the ability to use that portion of its own property for its own purposes. If relief were denied, the court found little doubt the load on eBay's system would qualify as a substantial impairment of condition or value sufficient to grant the preliminary injunction.

#### **4.4. The Financial Services Roundtable**

The Banking Industry Technology Secretariat ("BITS"), the technology group for the Financial Services Roundtable, identified a number of concerns with the practice of data aggregation. These include:

- Potential liability of financial institutions for compromise or misuse of customers authentication information by third parties;
- Business, financial and reputational risks to financial institutions flowing from inadequate security of storage of customer data by aggregators;
- Lack of technology to track and control data aggregation or identify unauthorized transactions; and,
- Lack of any uniform security and privacy requirements for aggregators.<sup>27</sup>

In response to these concerns, BITS formed a task force of fifteen financial institutions to develop business practices, policies and a legal framework for

aggregators and to pursue development of voluntary industry guidelines. BITS is also working with the bank regulatory agencies and the FTC to understand and assess the risks and liabilities of the practice. The BITS Financial Services Security Lab is exploring the kind of security criteria for testing the security and privacy functionality of aggregator software and services.<sup>28</sup>

#### **4.5. Data Aggregation Implications for Account Providers**

A private research report identified two major concerns in regard to data aggregation as:<sup>29</sup>

- Erosion of the value and visibility of an institution's online brand name, as the consumer no longer needs to visit the institution's site to perform transactions. Thus, the ability of banks and other online service providers to maintain a primary relationship with their customers is undermined; and
- Loss of control over the user's web experience, which, for example, reduces opportunities to cross sell.

Much of the press attention to this issue has focused on the competitive question of whether banks, having invested in establishing a presence and transactional capability online, will find that customers who use their site are drawn away to an aggregator's site or will respond, for example, either by setting up their own aggregation service or by other means, such as negotiation or litigation.

The impact on a provider's system resources of harvesting growing amounts of customer data on an ever more frequent basis has yet to emerge as a publicly discussed issue, but it may have the potential to be significant. It has been estimated that as of April 2000 about 100,000 people used account aggregation services, but growth forecasts by some in the industry anticipate over 800,000 users by the end of the year, 4 million users by 2002 and 7 million by 2003.<sup>30</sup> The process of non-direct feed data aggregation involves automated periodic mass-inquiries of each account provider's server. As aggregation services gain popularity, the number of these inquiries may rise as an increasing proportion of accounts are enrolled in an aggregation service. Further, as aggregators gain subscribers and resources, they may seek to offer more frequently refreshed data, further increasing the demands on a provider's computer resources.

In response to the issues raised by the growth of aggregators, information providers have begun to take aggregation services into account in their website terms and conditions and online agreements. The focus of their efforts vary. They be directed at preventing customers from disclosing PINs to aggregators or to preventing aggregators from using the information relating to a customer for the aggregator's own commercial benefit. Some examples of this trend are as follows:

- Each [frequent flyer] member needs to establish a ... PIN to gain access to their . . . account information online or over the telephone. If your PIN is lost, misappropriated or stolen, you must notify your nearest [airline] representative immediately. Failure to notify . . . could result in a deduction of miles. You are responsible for maintaining the confidentiality of your PIN. It is a violation of . . . program rules to divulge your . . . PIN to a third-party business. [Airline] shall have no liability for losses resulting from unauthorized access to or use of your PIN.
- Users who are not either (i) registered with [airline] as Users of [airline] services ("Registered Users") or, (ii) trusted invitees of such Registered Users authorized to act on behalf of such Registered Users, are hereby prohibited from accessing or using [airline].com services, . . .
- Users may exhibit the [airline] screen displays only to Registered User authorized invitees, and use [airline's] data and information relating only to or generated by the Registered User for the purpose of performing the specific passenger seat booking, [Program] profile corrections, reservation and related activity authorized by [airline] services but for no other purpose or function. Any undesignated non-business use and all business uses are strictly prohibited.
- The content available through this Site is the property of [broker] is protected by copyright and other intellectual property laws. Content received through this Site may be displayed, reformatted, and printed for your personal, non-commercial use only. You agree not to reproduce, retransmit, distribute, disseminate, sell, publish, broadcast or circulate the content received through this Site to anyone, including but not limited to others in the same company or organization, without the express prior written consent of. . . .

## 5. Legal Issues

## **5.1. The Electronic Fund Transfer Act and Regulation E**

Because data aggregation may involve access to consumer asset accounts accessible through financial institution websites, transfers from these accounts when access was obtained through the aggregator service may raise issues under Regulation E.

### **5.1.1. Status of a Data Aggregator Under Regulation E**

It is not clear how data aggregators whose systems provide a user with the ability to effect transactions in their financial institution's website without reentering the PIN for that website will be affected by Regulation E. This analysis may vary greatly depending on the type of system used by the data aggregator and the nature of any arrangement between the data aggregator and the financial institution.

Data aggregators may make a number of arguments to support the position that they are not subject to Regulation E. These could include the argument that they do not fall within the definition of "financial institution" because they do not issue an "access device" and do not agree with a consumer to provide electronic fund transfer services. On the other hand, to the extent the effect of the service offered by an aggregator is to issue a master PIN that allows the user to access a financial institution's website and to initiate electronic fund transfers on an institution's website without entering a PIN, it may be argued that the aggregator comes within the intended scope of the rule.

### **5.1.2. Regulation E When a Data Aggregator is Involved**

In the event that a customer encounters a loss that may be associated with data aggregator activity, there may be a dispute as to whether the data aggregator, the financial institution or the consumer must bear the loss. Regulation E defines an unauthorized electronic fund transfer as a transfer initiated by a person other than the consumer without actual authority and from which the consumer receives no benefit. A transaction does not qualify as unauthorized if it is made by a person who was furnished with an access device by the consumer, unless the consumer has notified the institution that transfers by that person are no longer authorized.

It is not clear how the concept of an unauthorized transaction would be applied in the context of aggregation. A consumer might argue that he or she

never authorized the data aggregator to effect any transactions with regard to the consumer's account and therefore any transaction not authorized by the user should be treated as such notwithstanding the presence of the data aggregator. The financial institution, on the other hand, may, as a practical matter, be hard-pressed to distinguish between a legitimate and an illegitimate use of the PIN. As a result, at least one financial institution appears to have attempted to address this issue by including in its terms the following statement:

If you permit another person to use the Service or give them you PIN or password, you are responsible for payments, transfers, or advances that person makes from the deposit and credit accounts linked to your Service registration even if that person exceeds your authorization.

### **5.1.3. Federal Reserve Board Request for Comment**

The Board of Governors of the Federal Reserve System ("FRB") took official note of the Regulation E issues raised by aggregators by requesting comments on aggregation issues in connection with a proposed revision to the Official Staff Commentary to Regulation E issued on June 22, 2000 ("Comment Request"). The Comment Request asks for information on how aggregators operate or plan to operate; on whether aggregators provide or plan to provide bill payment or other EFT services; and to what extent agreements exist between aggregators and account holding institutions.

The FRB asked for comments on the implications of a determination that aggregators are or are not financial institutions for purposes of Regulation E generally or under section 205.14. In that regard, the FRB first noted that typically only one access device is contemplated to initiate an EFT to or from a consumer's account. It then went on to state that if a consumer enters a security code issued by an aggregator to access information on the aggregator's website and the consumer initiates an EFT using a security code provided by the account holding institution, the security code issued by the aggregator arguably meets the definition of an "access device." The FRB then commented that two access codes (one from the aggregator and one from the account holding institution) are needed to initiate electronic transfers from the consumer's account from the aggregator's website. Thus, in the words of the FRB, the aggregator would be a financial institution for purposes of Regulation E.

Finally, the FRB states that if an aggregator is not a financial institution and an unauthorized EFT occurs through an aggregator's service, Comment 2(m)-2 could be read to suggest that a consumer who has given the aggregator access to the consumer's account assumes liability for the transfers. In this regard, the FRB noted that the guidance in the comment, which concerns liability for the actions of parties whose activities were authorized by the consumer, was not originally provided to address the aggregator situation.

While the Comment Request leaves the FRB some flexibility on how to treat aggregators, it indicates that the FRB is inclined to treat aggregators who offer automatic click through access into an EFT capable portion of an account holding institution's website without having an agreement with the institution as being subject to Regulation E. The FRB will be accepting comments through August 31, 2000.

## **5.2. Computer Fraud and Abuse Act**

As the central concern of the Computer Fraud and Abuse Act<sup>31</sup> ("CFAA") is to protect against unauthorized access to certain computers, its application to account aggregation may depend to a significant extent on whether the activity involved is viewed as falling outside of a permissible type of instruction. As a result, aggregators extracting information from an account provider's website without express consent should be aware of the potential impact of this statute on their operations.

The legislative history of the CFAA indicates that the provision does not extend to any type or form of computer access that is for a legitimate business purpose. "Thus, any access for a legitimate purpose that is pursuant to an express or implied authorization would not be affected. The provision does not extend to normal and customary business procedures and information usage and so these legitimate practices will not be . . . affected. It imposes criminal sanctions upon hackers and other criminals who access computers without authorization."<sup>32</sup>

Under the CFAA, fines and/or imprisonment<sup>33</sup> apply for (i) intentionally accessing a computer without authorization, or exceeding authorized access,<sup>34</sup> and (ii) obtaining information either: derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution; or from any protected computer (a computer



exclusively for the use of a financial institution or . . . , or any computer used in interstate or foreign commerce or communication), or intentionally accessing a protected computer without authorization, and causing damage as a result. The CFAA also provides for a civil cause of action by any person suffering loss by reason of a violation of the Act (limited to economic damages totaling at least \$5,000 over a one-year period, arising from impairment to the integrity or availability of data, a system or information), injunctive relief or other equitable remedies.

Consumers are provided with PINs to access online services with the intent that they will use those PINs to use the online services. One question that arises is whether the PIN, once issued, is a blanket authority for the consumer to access (and authorize others to access) their account information, or whether the provider may prescribe terms and conditions limiting the purposes for which it may be used and the parties by whom even a PIN may be used. In that regard, the recent case of *America OnLine Inc. v. LCGM Inc.* suggests that a breach of the terms of use of an online service is sufficient basis for a finding of unauthorized access for the purposes of the Act.<sup>35</sup> In that case, America Online took action against an enterprise sending "spam"<sup>36</sup> to its members in violation of the conditions of use of the service and the court found that this breach constituted violation of the CFAA constitutional.

## **6. Intellectual Property Issues**

### **6.1. Copyright**

Taking information from one website and reformulating it on another involves a significant amount of copying, certain aspects of which may be protected under the copyright laws. If the aggregator merely takes hard factual data and presents it on its own website in its own format there can be less objection on copyright grounds than if it adopts aspects of the source sites "look and feel."<sup>37</sup>

### **6.2. Service Mark Infringement and False Designation of Origin**

A second issue raised is the nature of the use by a screen scraper of the information providers name and service mark. The question is whether the use made creates a likelihood of confusion as to the source or sponsorship of the services. A significant concern of Applicants in both the eBay and First Union litigation was the perceived adverse effect on the information

providing sites' business reputation because of the alleged implicit relationship between the screen scraper and the institution as a result of representations by the scraper that account data from the institution was available on their site, use of the institution's corporate logo, and other misleading representations. The concern was that a user's adverse experience with an aggregator may thus "rub off" on the financial institution.

It is interesting to note how Paytrust addressed this issue following the resolution of First Union suit. The Paytrust Smartbalance enrollment page, where the user enters their bank account number and PIN, now includes a disclaimer of any affiliation or endorsement between the two parties.<sup>38</sup>

## **7. Privacy**

Title V of the Gramm-Leach-Bliley Act ("GLBA") directs the bank regulatory agencies, the FTC and the Securities and Exchange Commission to promulgate regulations to govern the data protection policies and practices of financial institutions in accordance with the provisions of the GLBA.<sup>39</sup> The rules will apply to "financial institutions"<sup>40</sup> and will require financial institutions to provide both an initial, and ongoing periodic, notices to customers about their privacy policies, and to provide a customer opt-out procedure from disclosure of some kinds of information to certain unaffiliated third parties.

The FTC issued a final rule on May 24, 2000,<sup>41</sup> implementing the GLBA privacy provisions and in the accompanying commentary consider the application of the rule to "certain Internet industries." Because the definition of financial institution includes data processing and data transmission services, facilities, data bases, . . . and access to such services if the data is financial banking or economic,<sup>42</sup> the FTC found that "this language brings into the definition of financial institution an Internet company that compiles, or aggregates, an individual's online accounts . . . at that company's website as a service to the individual. . . ."<sup>43</sup> Thus, as far as the FTC is concerned, the activities of aggregators are subject to the privacy provisions of the Act.<sup>44</sup>

## **8. Reputational Issues**

Where a third-party website acts as the host for a data aggregation service, this may raise both reputational and liability issues for the host site. One aspect of these issues may be addressed through the agreement that governs user access to the data aggregation service. Such agreements may be

between the data aggregator and the user or they may be structured between the venue hosting the service and the user. Potential website hosts, particularly those that are themselves financial institutions of one type or another should evaluate the protections that contractual agreements and on-screen disclaimers may offer in regarding their potential exposure to liability risk and reputational risk in the event of problems or issues in connection with use of the data aggregation service. Potential website hosts should also consider the privacy considerations associated with the aggregator's use of user data collected through the service and how such uses, including uses by the host website or third parties, will be disclosed.

---

## NOTES

\* We wish to acknowledge the assistance of Andrew Ham, Associate, Fried, Frank, Harris, Shriver & Jacobson LLP, in the preparation of this article.

1. The pejorative nature of this term may be indicated by the range of alternative phrases aggregators have developed to avoid it. They include "surrogate browsing," H-Connect (for connecting via HTML), "secure data mining architecture" and "Web harvesting." See David Hallerman, BANK TECH. NEWS, *All data, All the time; Aggregation of consumer financial information by third party companies threatens banks but opens doors to e-commerce*, Mar. 2000, at 1.
2. *Ezlogin.com jump starts the Internet*, Ezlogin.com Press Release (May 25, 1999), available at <http://www.ezlogin.com/press/beta.html> (visited May 30, 2000).
3. *Ezlogin.com simplifies access and registration to internet sites*, Ezlogin.com Press Release (July 26, 1999), available at <http://www.ezlogin.com/press/launch.html> (visited May 30, 2000).
4. *About Ezlogin.com*, Ezlogin.com Press Release (July 26, 1999), available at <http://www.ezlogin.com/press/21400.html> (visited May 30, 2000).
5. Hallerman, *All data, All the time*, *supra* note 1.
6. *Id.*
7. Barry Flynn, *Internet Banking Gets Personal*, ORLANDO SENTINEL, May 14, 2000, at H1.
8. *First Union Announces Internet Requirements for Aggregator Companies in an Effort to Address Customer Security and Privacy Concerns*, First Union Press Release (Dec. 28, 1999).

9. A service whereby subscribers provide their bank account information and the details of various regular bills they receive (such as telephone, electricity and gas) including account number and billing address. When a bill is received the user writes a "check" on line which Paytrust remits to the biller (generally by post, but possibly by electronic means if the biller has the technical capacity).
10. *First Union Corp. v. Secure Com. Serv., Inc.*, No. 3:99CV519H (W.D.N.C. filed Dec. 30, 1999).
11. *Ezlogin.com announces support for 2,500 sites reaching new high mark for automated access to personal web content*, Ezlogin Press Release, available at <http://www.ezlogin.com/press/21400.html> (visited May 30, 2000).
12. *First Union Corp. Drops Suit Against New Jersey Aggregator*, BANKING REP. (BNA), Mar. 6, 2000, at 450.
13. *Megan Ptacek, Intuit Joins Ranks of Screen Scrapers with a Service 33 Banks Participate*, AM. BANKER (Tech. Section), Apr. 20, 2000, at 1.
14. *The Screen Scraper Challenge*, BANK MARKETING INT'L, Jan. 28, 2000.
15. *Jessica Toonkel, First Union Aims for Yearend Debut of Account Aggregation on Web Site*, AM. BANKER, Apr. 19, 2000, at 1.
16. *Jessica Toonkel, New Microsoft Challenge to Banks: Account Aggregation on MSN Site*, AM. BANKER, at 1.
17. Hallerman, *All data, All the time*, *supra* note 1.
18. *eBalance, Inc. Introduces the next generation of its On-line Personal Finance management Solution; Internets most comprehensive Financial ASP Provides real-time Data Collection*, BUS. WIRE, May 15, 2000.
19. First Union Corp., *supra* note 10.
20. Kenneth Kiesnoski, *Web Aggregators Pros and Cons for Banks*, BANK SYS. & TECH., Apr. 1, 2000, at 28 (quoting Gayle Wellborn, Director of Customer Advocacy for First Union's E-channels Division).
21. Flynn, *Internet Banking*, *supra* note 7.
22. *eBay Inc. v. Bidder's Edge Inc.*, No. C-99-21200RMW (ENE) (N.D. Cal. filed Jan. 14, 2000).
23. A protected computer includes any computer used in interstate or foreign commerce or communication if the conduct involved an interstate or foreign communication.

24. *eBay, Inc. v. ReverseAuction.com, Inc.*, No. C-00-20023RMW (EAI) (N.D. Cal. filed Jan. 6, 2000).
25. *Federal Trade Commission v. ReverseAuction.com, Inc.*, No. 00-23046 (Jan. 6, 2000).
26. *eBay, Inc. v. Bidder's Edge, Inc.*, No. C-99-21200RMW (ENE) (N.D. Cal. May 24, 2000)
27. *Report on Key Initiatives, Aggregator Issues*, BITS Bull., May 2000, at 3 (reporting on the endorsement, by the Boards of both BITS and the Roundtable, of BITS efforts to develop business practices, policies, and a legal framework for aggregators).
28. *Id.*
29. *Account Aggregators, Screen Scrapers and Online Financial Services*, CELENT COMMUNICATIONS Apr. 2000 (quoted in *Banks look forward to becoming Aggregators*, RETAIL DELIVERY NEWS Apr. 26, 2000 and *Banks Face Loss of Customers to Account Aggregators*, WEB FINANCE, Apr. 10, 2000.)
30. *Id.*
31. 18 U.S.C. \* 1030.
32. Counterfeit Access Device and Computer Fraud Abuse Act of 1984, H. REP. NO. 98-894, *reprinted in* 1984 U.S.C.C.A.N. 3689, 3707.
33. The penalty is greater (up to 5 years rather than one) if the offense is committed for commercial advantage or private financial gain.
34. Defined as accessing a computer without authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter (18 U.S.C. § 1030(e)(6)).
35. 46 F. Supp.2d 244 (E.D. Va. 1998).
36. Unsolicited commercial bulk email.
37. In *Ticketmaster Corp. v Tickets.com*, No. 99-7654 HLH (BQRx) (C.D. Cal. Mar. 27, 2000), the court held that the practice of hyperlinking does not itself involve a violation of the Copyright Act, as no copying is involved. In the same way as an index card is used, a customer using the link is transferred to the genuine webpage of the original author. Presentation of factual data in its own format is distinguished from copying the method in which it is presented.
38. [www.paytrust.com](http://www.paytrust.com) (visited May 24, 2000). The page lists the banks that the feature works with, and continues "[t]he banks have no affiliation with Paytrust, nor have they endorsed, in any fashion, any of the services offered by Paytrust."
39. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, tit. V, 113 Stat. 1338 (1999).

40. Section 509(3) of the Gramm-Leach-Bliley Act defines financial institution as "any institution the business of which is engaging in financial activities as described in section 4 (k) of the Bank Holding Company Act. . . ."
41. Privacy of Consumer Financial Information, 65 Fed. Reg. 33646 (2000) (to be codified at 16 C.F.R. pt. 313).
42. *Id.* at 33654.
43. *Id.* at 33655.
44. The application of the GLBA privacy rules to aggregators raises some interesting issues. For example, how do the provisions regarding limitations on redisclosure and reuse apply to aggregators. From one perspective, a customer of a data aggregator will know what nonpublic personally identifiable financial information will be held by the aggregator and will receive a privacy policy notice and opt out notice, if applicable, from the aggregator. Arguably this should address any concerns regarding the privacy interests of the customer.

At the same time, the aggregator will be receiving nonpublic personally identifiable information from financial institutions. It is unclear whether the GLBA privacy rules will be applied to transfers of nonpublic personally identifiable financial information from a financial institution to an aggregator, including transfers where there is no agreement between the aggregator and the institution with respect to such transfers. If these provisions were to be deemed to apply, the following considerations would have to be addressed.

Under the GLBA privacy rules, a party that receives nonpublic personally financial information from a financial institution is itself subject to certain requirements under the rules. If the party receives the information under one of the specified exceptions relating to the servicing of an account or the completion of transactions and certain other exceptions ("Specified Exceptions") under which a financial institution may disclose information to a third party without making a specific statement regarding such disclosures and without being required to offer an opt out, the receiving party is strictly limited as to how it may use such information. The receiving party may disclose the information to affiliates of the financial institution from which it received the information; it may disclose the information to its affiliates but they may only use and disclose it only to the same extent as the receiving party may; and it may disclose and use the

information pursuant to one of the Specified Exceptions in the ordinary course of business to carry out the exception under which the receiving party received the information. In a situation where there was no agreement between the financial institution and the aggregator, it would seem unlikely that the Specified Exceptions would apply. If they did, however, apply, the receiving party could not disclose the nonpublic personally identifiable information to a third party for marketing purposes and could not use the information for its own marketing purposes.

If a party receives nonpublic personally identifiable financial information from a financial institution other than under the Specified Exceptions, the receiving party may disclose the information to affiliates of the financial institution from which it received the information; it may disclose the information to its affiliates but they may only use and disclose it only to the same extent as the receiving party may; and may disclose the information to any other person if the disclosure would be lawful if made directly to that person by the financial institution from which the receiving party received the information. As a practical matter, if applicable to aggregators, this would pose a significant restriction on them since they arguably would have to know whether the customer had opted out of disclosures of their nonpublic personally identifiable financial information to third parties. An aggregator that had not entered into an agreement with a financial institution might find it difficult to obtain such information from the institution.

21st Century Money, Banking  
& Commerce Alert

Antitrust and Competition  
Alert

Fried Frank Government  
Contracts Alert

---

Fair Lending Alert

FraudMail Alert

SecMail

Disclaimer. Terms of Service. LLP. Last updated: September 11, 2002 .  
Copyright © 2000-2005 Fried, Frank, Harris, Shriver & Jacobson LLP. All rights reserved. "Fried Frank" and "FFHSJ" are trademarks of Fried, Frank, Harris, Shriver & Jacobson LLP.

## Visa USA Cardholder Information Security Program (CISP)

### Overview

Every piece of cardholder account information that passes through the Visa payment system is vital to our business operation. However, without proper safeguards in place, this information can be extremely vulnerable to internal and external compromise(s), which can often lead to fraud and identity theft. Visa's Cardholder Information Security Program (CISP) ensures the highest standard of due care to help keep sensitive cardholder data safe from hackers and fraudsters. The Payment Card Industry (PCI) Data Security Standard is a result of collaboration between Visa and MasterCard industry security requirements. Other card companies have also endorsed the Standard within their respective

This is the Exhibit "I" referred to in the affidavit of "Raymond Grace"

Sworn before me this 21<sup>st</sup> day of August, 2005

[Signature]

**These 12 requirements are the foundation of Visa's CISP.**

### PCI Data Security Standard

1. Build and Maintain a Secure Network1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

### Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

### Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

### Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data



**Regularly Monitor and Test Networks**

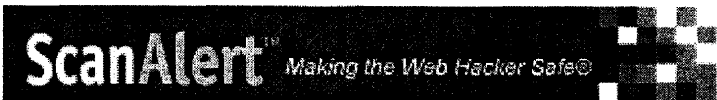
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
11. Maintain an Information Security Policy
12. Maintain a policy that addresses information security

This is the Exhibit "J" referred to in the affidavit of "Raymond Grace"

Sworn before me this 31st day of August, 2005

September  
"Elizabeth Meddings"

Elizabeth Meddings  
Barister & Solicitor



English



**HACKER SAFE sites help protect you from Identity Theft and Credit Card Fraud**

This site is tested and certified daily to pass the FBI/SANS Internet Security Test. The "live" HACKER SAFE mark appears only when a web site's security meets the highest security scanning standards of the U.S. government, Visa, MasterCard, American Express, Discover and JCB.

[www.usemybank.com](http://www.usemybank.com)



Research conducted at the federally funded research and development center operated by Carnegie Mellon University indicates that sites free of all known vulnerabilities that can be remotely scanned for, such as those earning HACKER SAFE certification, will prevent over 99.99% of hacker crime.

Click Here for a risk-free security audit

**Important Disclaimer:** This information is intended as a relative indication of the security efforts of this web site and its operators. While this, or any other, vulnerability testing cannot and does not guarantee security; it does show that [www.usemybank.com](http://www.usemybank.com) meets all payment card industry guidelines for remote web server vulnerability testing to help protect your personal information from hackers. HACKER SAFE does not mean hacker proof. HACKER SAFE certification cannot and does not protect any of your data that may be shared with other servers that are not certified HACKER SAFE, such as credit card processing networks or offline data storage, nor does it protect you from other ways your data may be illegally obtained such as non-hacker "insider" access to it. While ScanAlert makes reasonable efforts to assure its certification service is functioning properly, ScanAlert makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that ScanAlert shall be held harmless in any event.

**This ScanAlert HACKER SAFE verification page was generated on a secure server at <https://www.scanalert.com>**