

**COMPETITION TRIBUNAL**

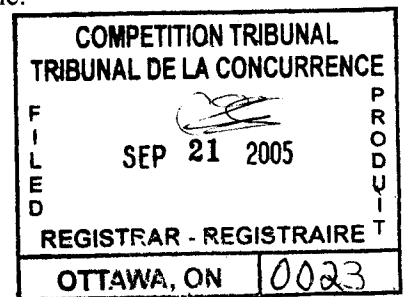
**IN THE MATTER OF** the *Competition Act*, R.S.C. 1985, c. C-34, as amended;

**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

- and -

**THE BANK OF NOVA SCOTIA**

Respondent

**RESPONDING AFFIDAVIT OF ROBERT ROSATELLI  
(SWORN SEPTEMBER 21, 2005)**

I, **ROBERT ROSATELLI**, of the City of Toronto, **MAKE OATH AND SAY:**

1. I am the Vice-President of Self Service banking at The Bank of Nova Scotia ("Scotiabank"). I have been employed by Scotiabank since 1995. I assumed my most recent position as Vice-President of Self Service banking in December 2000. My responsibilities

include Channel Management accountability for Scotiabank ABM, Telephone banking, Wireless banking, Interac Direct Payment, ScotiaCard, and Consumer Payment Programs. As the individual responsible for Scotiabank's ScotiaCard program, I am responsible for ensuring the integrity of transactions processed using the debit card, the security of customer information when using the debit card, and our compliance with various regulations.

2. I have sworn an Affidavit in this matter on July 12, 2005.

3. I have reviewed the Affidavits of Raymond Grace dated June 15, 2005 and August 29, 2005 and the Affidavit of Joseph Iuso, dated August 29, 2005. I make this Affidavit in response to those Affidavits.

**The Plaintiffs Do Save Password Information in Unencrypted Form**

4. The critical issue from Scotiabank's perspective is the fact that customers are disclosing their confidential Internet banking passwords to a third party. This raises the potential for the third party to misuse that password information or for an unauthorized third party to obtain the information, and literally drain all of the money out of the banking customers' accounts who have disclosed their passwords. Scotiabank does not and cannot tolerate disclosure of Internet password information on the part of any of its customers, and Scotiabank has gone to great lengths to emphasize to its customers repeatedly that they are not to disclose their Internet banking password or their PIN to anyone, whether it be a family member, a data aggregator, or individuals such as the Applicants who are effecting transactions on behalf of the banking customer using the banking customers' confidential password.

5. As a result of the foregoing, the level of computer security in place on the part of the Applicants is almost of secondary importance. When one weighs the risks of continuing to offer

banking services to the Applicants against the potential for fraudulent transactions in customers' accounts, Scotiabank simply cannot continue to offer banking services to the Applicants.

6. Both Mr. Grace and Mr. Iuso assert that customer password information is always transferred in encrypted form. However, it is apparent that customer password information is saved on the UseMyBank system, even if (perhaps) briefly, in unencrypted form.

7. I am advised by Scotiabank's Internet Banking Group that when a Scotiabank customer provides UseMyBank with its Bank card and password information, this information is transmitted over the network to UseMyBank's server at a server farm using 128 bit encryption. However, once it gets to UseMyBank's server it is decrypted. UseMyBank has to enter the customer's password in plain text into a scripting program. Another secure transaction is initiated by transmitting the encrypted information between UseMyBank's server and the financial institution where the on-line banking has occurred. Thus, after the encrypted information is received by UseMyBank from the customer entering the data, it is in plain text, and this plain text is stored in UseMyBank's RAM (server memory) while the script is running.

8. Mr. Grace states that he or someone else is looking at the transaction in "real time" to make sure that the debit has occurred from the customer's Bank account. Mr. Grace also states that he is validating customer information as a means of detecting fraudulent transactions. If Mr. Grace can access the server, then anyone else with the wherewithal to do so could access the server.

9. Unlike the UseMyBank server which does save unencrypted password information during the process of the transaction, a Scotiabank customer who is personally using on-line banking is never put at risk for a breach of their password. When a Scotiabank customer using internet banking types in his or her password to effect a transaction, the message is sent to

Scotiabank in encrypted form, and is never decrypted. Thus, the Scotiabank customer, acting on his or her own behalf, can complete a transaction without ever having their password information in plain text. Scotiabank does not store passwords in plain text.

10. In Joseph Iuso's Affidavit, he attached the PowerPoint presentation that he says he made to the Canadian Payments Association. On page 5 of that presentation, UseMyBank represented to the Canadian Payments Association that "critical information is not stored", but states that it is managed through an encrypted session/cookies.

11. It was noteworthy to me that Mr. Iuso was careful to indicate that only the transmission process is encrypted. "Cookies" are storage facilities on a PC or a server. By indicating that they use Cookies, UseMyBank is confirming that they are storing the session or parts of the session containing password information.

12. This can be demonstrated by a review of the transaction that David Metcalfe undertook when he made a donation to Princess Margaret Hospital using UseMyBank. This was described by David Metcalfe in his Affidavit sworn July 12, 2005, and filed with the Tribunal. David Metcalfe was able to determine that, after he provided his password information to UseMyBank, UseMyBank entered his Scotiabank on-line banking account twice in order to effect the \$5.00 donation to Princess Margaret Hospital. The significance of logging in twice is that the password information was stored in order for UseMyBank to log on more than once without the customer re-entering his password information.

13. While UseMyBank might assert that the password information is only stored during the course of the session, which might only last a few minutes, the fact is that the customer's password information is potentially available in unencrypted form to either a rogue employee of UseMyBank or to a computer hacker. Moreover, as mentioned above, because the information is

stored in the computer system's RAM, anyone can dump memory from the computer's RAM, including the password information stored in an unencrypted form in UseMyBank's computer RAM.

14. When the plaintiffs' very manner of doing business requires Scotiabank customers to provide their secret password information, Scotiabank has a legitimate interest in keeping customers' information secure. Scotiabank is well within its clear contractual rights to terminate banking services with any of its customers for any reason on 30 days' notice.

**Scotiabank Did Not Know the True Nature of the Plaintiffs' Business**

15. Mr. Grace asserts in his August 31, 2005 Affidavit that Scotiabank knew about the manner in which the plaintiffs were conducting business as a result of a presentation made by the President of UseMyBank, Joseph Iuso, to the Canadian Payments Association in 2003.

16. Mr. Iuso did make a presentation to the Canadian Payments Association and two of the attendees present were members of Scotiabank. One of those attendees was Beth Bailey. Ms. Bailey holds the position of Vice President, Strategic Payment and Remittance Services at Scotiabank. The second person who attended the meeting of the Canadian Payments Association was Tom Provencher. Mr. Provencher worked under Ms. Bailey and held the position of Senior Manager, Payment Products.

17. I am advised by Ms. Bailey, and verily believe, that at no time during Mr. Iuso's presentation on behalf of UseMyBank, did he identify Scotiabank as the banker for UseMyBank's joint venture partners and affiliates, GPAY, NPAY, and B-Filer. Indeed, UseMyBank itself does not bank at Scotiabank. I am further advised by Ms. Bailey, and verily believe, that she had no knowledge of the relationship between UseMyBank, GPAY, NPAY, or

B-Filer. Mr. Grace therefore has no basis to assert that Scotiabank “knew” of the manner in which the plaintiffs were conducting business as a result of the presentation by Mr. Iuso to the Canadian Payments Association.

18. Ms. Bailey advises me and I believe that following UseMyBank’s presentation to the CPA, there was a discussion amongst those in attendance about UseMyBank’s business, as described in Mr. Iuso’s presentation. The consensus of the group was that UseMyBank’s practice of obtaining confidential customer passwords put Bank card holders using this service at increased risk that fraud could occur in their account. Moreover, the group expressed the view that financial institutions whose customer accounts are being entered in this manner are themselves at considerable risk for a number of reasons; for example, if UseMyBank were to become insolvent while holding funds directed to, but not yet disbursed to, the intended recipients.

19. Mr. Iuso further asserts in his Affidavit that Scotiabank “knew” of the nature of UseMyBank’s business by virtue of the fact that apparently there were a number of “hits” to UseMyBank’s website, from computers with a web address indicating that the computer was owned by Scotiabank.

20. As I indicated in my Affidavit sworn July 12, 2005, there are over 40,000 employees of Scotiabank worldwide. To suggest that a few hits from computers with web addresses at Scotiabank affixes Scotiabank with “knowledge” that UseMyBank and the Applicants herein were taking customer’s Internet banking passwords to transact banking business on their behalf is completely false. Moreover, to link it in time to the CPA presentation by Mr. Iuso is also completely inaccurate. I am advised by Beth Bailey and by Mr. Provencher that neither of them instructed anyone at Scotiabank either before or after the CPA presentation by Mr. Iuso to make

inquiries about the business of UseMyBank or the Applicants. Nor did either of them make a report to anyone at Scotiabank about the presentation. As a result, the so called "hits" to the UseMyBank website by one of Scotiabank's 40,000 plus employees has absolutely nothing to do with the CPA presentation.

21. Only one of the "hits" to the UseMyBank website has a name attached with it which has allowed me to follow-up on that specific incident. The Scotiabank employee in question is Susan Gilmore. I am advised by Susan Gilmore, and verily believe, that she was attempting to make a donation to the Princess Margaret Hospital for personal reasons and that her attempts to access the UseMyBank website were in no way related to her employment duties. The spouse of a colleague was undergoing treatment at Princess Margaret Hospital. Ms. Gilmore visited the Princess Margaret Hospital website and clicked on the link "How You Can Help". This took her directly to the UseMyBank website. I am further advised by Ms. Gilmore, and verily believe, that her attempts to make a donation to the Princess Margaret Hospital, which incidentally brought her to UseMyBank website, were in no way related to any inquiry on the part of Scotiabank about its banking relationship with any of the Applicants, or the Applicants' relationship to UseMyBank.

22. I attempted to make inquiries with respect to the other so called "hits" by Scotiabank employees identified by Mr. Iuso in his affidavit. However, when an employee of Scotiabank accesses the Internet via his or her computer at Scotiabank, the Bank's routers and firewalls consolidate the user specific IP address to the public IP address. Thus, although the individual employees have unique IP addresses, the Bank's system rolls these up into our public IP address when accessing the Internet and utilizes dynamic host configuration protocol to assign IP addresses which result in IP addresses being transferred from one employee to another. As a result, it is impossible to determine who in the Bank accessed the UseMyBank website, apart

from Ms. Gilmore, who had configured her computer to have her e-mail address form part of her IP address. However, the specific circumstances of Ms. Gilmore's incidental access to the UseMyBank website via the Princess Margaret Hospital website is instructive. It is completely inaccurate to assert that Scotiabank "knew" about the business of UseMyBank, including the fact that it was requiring customers to disclose their Internet banking password, given the number of Scotiabank employees (over 40,000), and the fact that employees may access the UseMyBank website for purely personal reasons, such as was the case with respect to Ms. Gilmore.

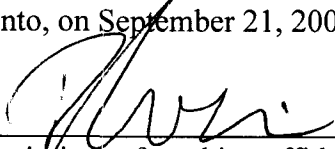
23. Scotiabank did not know that the Applicants were requiring disclosure of Scotiabank customers' Internet banking passwords via its joint venture partner UseMyBank until after it began investigating the Applicants in early 2005. It was the culmination of this investigation which resulted in the letters of termination dated May 11, 2005 for all of the reasons stated in my original Affidavit.

24. It is also noteworthy that, at the time that Mr. Iuso made his presentation, Rule E2 of the CPA Rules, which requires the Bank to directly authenticate the customer, was not yet in place. It came into force in 2005 subsequent to the UseMyBank presentation.

25. Mr. Grace asserts that the Applicants should be "grandfathered" and should not have to comply with Rule E2. There is no basis to make this assertion. Scotiabank is required to comply with Rule E2. This means that all of its transactions submitted for clearing and settling must meet the requirements of E2. If Scotiabank's customers are not meeting E2, Scotiabank cannot meet its obligations. Scotiabank cannot make exceptions for customers that may have been undertaking business in a manner that does not comply with E2, simply because they were transacting the business before the Rule came into force.

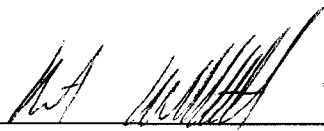


SWORN BEFORE ME at the City of  
Toronto, on September 21, 2005.



Commissioner for taking affidavits

TANYA A. PAGLIAROLI



ROBERT ROSATELLI

**B-FILER INC.**  
Applicants

and

**THE BANK OF NOVA SCOTIA**  
Respondent

Court File No: CT 2005-006

**COMPETITION TRIBUNAL**

**AFFIDAVIT OF ROBERT ROSATELLI  
(SWORN SEPTEMBER 21, 2005)**

McCarthy Tétrault LLP  
Suite 4700  
Toronto Dominion Bank Tower  
Toronto ON M5K 1E6

F. Paul Morrison LSUC #: 17000P  
Tel: (416) 601-7887  
Fax (416) 868-0673

Glen G. MacArthur LSUC #: 13669A  
Tel: (416) 601-7888  
Fax (416) 868-0673

Lisa M. Constantine LSUC#: 35064B  
Tel: (416) 601-7652  
Fax: (416) 868-0673

Solicitors for the Respondent

#4032015 v.3