

COMPETITION TRIBUNAL

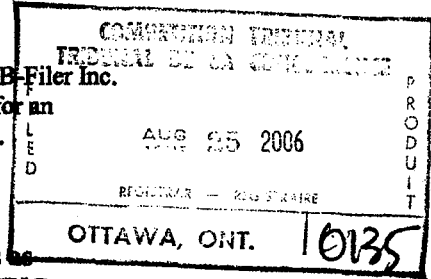
IN THE MATTER OF the *Competition Act*, R.S.C. 1985, c. C-34, as amended;

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

**REPLY AFFIDAVIT OF JAMES F. DINGLE
(Sworn August 22, 2006)**

**I, JAMES F. DINGLE, of the City of Ottawa, in the Province of Ontario, MAKE
OATH AND SAY:**

1. I worked at the Bank of Canada for 35 years, and a major portion of my career at the Bank of Canada was spent dealing with payment system matters. I retired from the Bank of Canada in 2003. Since then I have been employed by the International Monetary Fund as an expert in payment systems, and in particular as an assessor of the security, efficiency and reliability of both paper-based and electronic payment mechanisms.

2. I have sworn an Affidavit in this matter on July 27, 2006.

3. I have reviewed the Affidavit of Jack J. Bensimon dated August, 2006. I make this Affidavit in response to his Affidavit. The purpose of this Affidavit is to reply specifically to issues raised in Mr. Bensimon's Affidavit insofar as they relate to Scotiabank's business justification for terminating the Applicant's Banking Services.

The Nature of the Applicants' Business Activities

4. The Affidavit of Jack J. Bensimon permits one to produce a particularly detailed description of the Applicants' business activities, as follows. All the citations below come from Mr. Bensimon's Affidavit, as indicated by the references in parentheses. Occasional clarifications are added.

5. "Over 98 % of transactions are effectuated with online gambling casinos, some of which operate offshore with lax AML and terrorist financing controls." (Appendix C, first page.) Such transactions are clearly in the higher risk category. Gambling transactions cannot be described as lower risk and "routine". An example of a routine transaction would be the monthly payment of mortgage interest.

6. "Certain businesses, such as online casinos, may attract more suspected terrorists due to the ease of effectuating online transfers and the perception of a limited verifiable audit trail."
(Page 11, paragraph 31.)

7. “Although the average transaction is \$82, the online platform allows its customers to transact at higher levels, potentially triggering FINTRAC reporting requirements.” (Appendix D, first page.) The average is of course more representative of the great majority of internet gambling transactions, and should not be viewed as representative of the much less frequent money laundering or terrorist financing transactions.

8. “There is a possibility that through repeat use and manipulation of the Applicants UseMyBank system, a suspected terrorist can conceivably launder funds to finance terrorist activity.” (Page 11, paragraph 31.) A confirmation of actual cases follows.

9. “A few bundled transactions that attempted to circumvent the \$10 K rule.” (Appendix B, first page.) Some money launderers or terrorists are evidently aware of the FINTRAC reporting requirements which cover transactions of \$10,000 or more, and are managing their choice of amount so as to minimise their profile while using the Applicants’ system for their illegal purposes.

10. “The Applicants have several important gaps with respect to the development, implementation and monitoring of a [FINTRAC] compliance regime.” (Page 13, paragraph 36.) An important gap with respect to the maintenance of the security of all the transactions of the Applicants follows.

11. “Absence of appropriate employee screening procedures as part of an AML program (e.g., Know-Your-Employee (KYE) to mitigate internal data theft, can increase the inherent risk

of the Applicants to the Bank of Nova Scotia.” (Appendix C, third page.) The data theft of greatest importance would involve the theft by an employee of the user identification, password, and personal identification number of any of the thousands of individuals using the Applicants’ services for any purpose.

The Degree of Risk to the Respondent in Providing Services to the Applicants

12. The reputational, legal and regulatory risks to the Respondent are significant as a result of providing banking services to the Applicants. The risk is further increased when the gambling is offshore and in locations with lax anti-money laundering controls. It rises still further when there are clear signs (such as bundling) that some of the transactions are associated with money laundering or terrorist financing.

13. The risk of violating the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* rises as the percentage of the Applicants’ transactions potentially associated with such activities rises. The information contained in Jack J. Bensimon’s Affidavit makes it clear that all of the Applicants’ transactions must be viewed as potentially associated with these activities. Each and every one can correctly be viewed as suspicious, and thus requires separate analysis and reporting to FINTRAC.

14. The risk of significantly increasing the number of fraudulent transactions in the bank accounts of all the individuals who place a bet via the Applicants remains high as long as the Applicants and UseMyBank have no employee screening procedure of the sort required in an anti-money-laundering program. It also remains high as long as such individuals are required by

the Applicants to reveal their user identification number, password and personal identification number. The provisions of Rule E2 of the Canadian Payments Association with respect to preserving the confidentiality of such information are intended to limit such risk on a national basis.

15. In my opinion, if it became widely known that the Respondent was knowingly facilitating:

- (a) online offshore gambling transactions;
- (b) transactions that may be closely associated with money laundering and terrorist financing;
- (c) transactions in which the privacy and funds of approximately 20,000 banking customers at every major Canadian bank (i.e. those banking customers that have used the Applicants' services) could potentially be compromised,

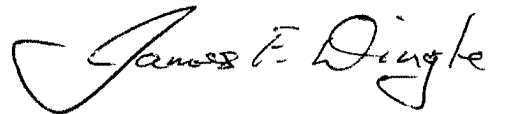
substantial damage to the reputation of Scotiabank would result. Legal proceedings against the Respondent based on the Criminal Code, or the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, or the Canadian Payments Act, would no doubt be the subject of extensive coverage in the public press. In the current world context, a financial institution that gained a reputation linking it to terrorism or other criminal activity could quickly lose the confidence of many depositors, and hence experience a costly reduction in growth potential.

16. Mr. Bensimon's report serves to highlight the serious risks to Scotiabank if it were required to offer banking services to the Applicants.

SWORN BEFORE ME at the City of
Ottawa, on August 22nd, 2006.



Commissioner for Taking Affidavits



JAMES F. DINGLE

BETWEEN:

B-FILER INC.
Applicants

- and -

THE BANK OF NOVA SCOTIA
Respondent

Court File No. CT 2005-006

COMPETITION TRIBUNAL

AFFIDAVIT OF JAMES F. DINGLE

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

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

Solicitors for the Respondent

4110483v.2