Lavery TECHNOLOGY

NUMBER 3, APRIL 2010

Legal newsletter for the information technology
and communication industries players

lavery
LAW ▸ BUSINESS

BREAKDOWN IN NEGOTIATIONS: THE BINDING EFFECT OF A LETTER OF INTENT

Catherine Rioux and Patrice Vaillancourt
crioux@lavery.ca / pavaillancourt@lavery.ca

You have decided to sell your business or to initiate a business relationship with a partner. You negotiate the main terms and, before going further, you sign a letter of intent. Then, you decide to withdraw from the negotiations. Can you do it? Not necessarily. Are you surprised?

The discussions and negotiations that precede the sale of a business or the beginning of a business relationship may be long and difficult. Before undertaking formal negotiations that may require a substantial investment in professional fees (accountants, lawyers) and energy, an entrepreneur may resort to a letter of intent, which he may consider as being of no real consequence.

Indeed, some entrepreneurs believe that signing a letter of intent does not bind them and only constitutes the expression of the common interest of the parties to pursue negotiations. But what about the obligations arising from a signed letter of intent? Does signing a letter of intent create legal effects between the parties? Can one be held liable for breaking off negotiations?

A letter of intent allows one or more parties to express in writing their intent to enter into a business transaction and evidences certain points of agreement between the parties before they continue negotiations.

A letter of intent may take many forms and be referred to under different names, such as *letter of intent* (LOI), *agreement in principle, articles of agreement and memorandum of understanding* (MOU). Regardless of its name, it is the intent of the parties before and after the signature of a letter of intent that will determine its scope. Therefore, the actions taken and the behaviour of the parties and even what they say will influence its interpretation.

In order not to be bound by a letter of intent, it is important to express this clearly. Failing an express stipulation whereby the parties wish to be bound by the letter of intent, the courts may review the circumstances surrounding its signature, the nature of the contract, the interpretation that the parties have already given to it as well as usage to determine the actual and common intent of the parties rather than limiting themselves to the literal meaning of the wording.

Even if a letter of intent is drafted in such a way that it creates no commitment to complete the proposed transaction, it however requires the parties to cooperate and collaborate positively between themselves towards that purpose and a party may withdraw in good faith from the negotiations to the extent that this is not abusive.

Various factual elements may also indicate improper conduct, including trying to obtain confidential information from the other party, leading the other party to believe that the proposed transaction will be finalized (for example, the attitude of the parties with their associates or the integration of the other party in the business), the advanced state of the negotiations and the amount of the costs already incurred.

Contents

Breakdown in Negotiations: the Binding Effect of a Letter of Intent

Providing Card Transactions Security: Your Responsibility

Certificate of Intellectual Property Pertaining to Software

An aggrieved party may obtain damages including interest from the party who withdrew from negotiations if the letter of intent did not allow such withdrawal or if the aggrieved party can prove that the other party did not act in good faith and that such behaviour was abusive.

Although it may seem simple, drafting a letter of intent must not be taken lightly. Since its main purpose is to frame the negotiations, it is crucial to ensure that the wording used does not create a final agreement of the parties. The use of words such as *offers, accepts, shall, must, promise, agreement, contract, undertaking* is to be avoided since they indicate the intent to be bound.

The wording of the letter of intent should never imply that it constitutes a final contract. It must be primarily a tool of reference for the parties. One cannot insist enough on the fact that involving legal counsel at the beginning of the process can avoid regrettable consequences.

A well drafted letter of intent can be a valuable tool to frame the negotiations for the acquisition or sale of a business or initiating a business relationship. However, one must not forget that breaking off negotiations can bring about significant legal consequences according to circumstances.

PROVIDING CARD TRANSACTIONS SECURITY: YOUR RESPONSIBILITY

Sarah Talpis-Guillet
stalpisguillet@lavery.ca

As a merchant or service provider, you must already deal with many sources of liability when you transact with your clients, for example the *Consumer Protection Act*, the obligations under the *Civil Code of Québec*, the *Criminal Code*... When transactions involve a payment by credit card, you must also comply with the PCI DSS standard to ensure cardholders' data security: a good reason to get acquainted with rules which you may have been unaware of until now.

WHERE DOES THE PCI DSS STANDARD COME FROM

The Payment Card Industry Data Security Standard or PCI DSS has been created to protect cardholders' data. Let us think, among other things, about the protection of data entered on the magnetic stripe of the cards or the information on their holders' NIP. The PCI DSS standard is managed by the PCI Security Standards Council (PCI SSC), an independent organization founded in September 2006 by the main credit card networks. Monitoring of these rules is concurrently ensured by these same credit card networks. That is to say that you are watched by *American Express*, *Master Card Worldwide* and *Visa International*, just to name a few.

Under the PCI DSS standard, all merchants who accept transactions paid with a credit card and all service providers who process this type of transactions must make their physical and virtual environments secure in order to ensure data protection. In practice, each credit company has its own compliance program to manage the application of the standard. Thus, under the program implemented by *Visa*, anyone who retains, transmits or processes *Visa* accounts data must comply with the standard.

WHAT TO DO IN PRACTICE

The PCI DSS standard is technical and complex, but revolves around key principles that allow cardholders to be protected against real risks (identity theft, theft of business information, use of systems for illegal purposes, etc.). According to these principles, the merchant must:

1) implement and manage a secured network, by installing and managing a firewall configuration to protect data and avoiding the use of the supplier's default parameters (for example with respect to passwords);

2) protect cardholders' data, meaning the stocked data, and encrypt the transmission of cardholders' data on public networks;

3) have a vulnerability management program, meaning to use and update an antivirus program and develop safe applications;

4) use solid control measures, by restricting access to data on a "need to know" basis, by providing a unique user code to each person having access to a computer and by restricting physical access to data;

5) monitor and regularly test the networks by following the accesses and testing the security procedures;

6) establish a policy respecting information security.

Although, on the whole, the standard applies in the same way to all merchants, the measures to demonstrate compliance may vary depending on the compliance program of each credit corporation. Thus for example, in the case of *Visa*, all merchants must register with a qualified independent assessor duly authorized by *Visa*, fill out a self assessment questionnaire and perform a quarterly scan of their networks, which must be validated by an assessor authorized by *Visa*. Depending upon their annual transactions volume, certain merchants must also perform an on site assessment of the security of the data they collect.

AT WHAT PRICE?

Compliance with the PCI DSS standard is mandatory. If you and your service providers fail to comply, credit card issuers may, under their specific programs, charge you fees and fines and even prevent you from using any credit card payment service. For example, *American Express* charges amounts of up to $15,000 per day to merchants who fail to comply with the standard, which is a harsh penalty for any business.

Each credit card issuer program has its own schedule respecting the application of this standard, but most of the deadlines for compliance have already been reached. Any business accepting credit card payments must therefore act now if it has not already done so.

CERTIFICATE OF INTELLECTUAL PROPERTY PERTAINING TO SOFTWARE

Jean Tessier
jtessier@lavery.ca

The computing world evolves rapidly, as do the software programs which support it. Moreover, their increasing complexity makes it difficult to identify with certainty their components and origin, as well as the rights inherent to them.

Knowing this information is essential to any developer who wants to market a software program. It is also a significant consideration when the software edition business becomes the subject of a merger or an acquisition.

A software program is composed of a group of instructions called "**source code**". While a portion of this source code is entirely created by the developers, other portions are obtained from third party sources such as free software directories or open source software or are acquired from other developers. These other portions constitute "**external source code**". Although a portion of this external source code may be free, it is often subject to copyrights and its user licence may provide for certain obligations or conditions which must be disclosed to the public for whom the software is created.

Depending upon its complexity, any given software will likely include a significant amount of external source code. That being the case, anyone who wishes to market such a software program or hire a programmer and acquire his ongoing projects would be well advised to identify the rights and conditions attached to the software he develops.

In order to avoid the significant costs related to the due diligence process carried out after the software program is developed, it is preferable to implement an automatic and integrated verification process of the software from the initial steps of its development.

This process should particularly include the following items:

- a policy for managing the software related intellectual property, which delimits the external content which the developer may use (the "**policy**");
- the analysis of the existing source code (inherited code or patrimonial code) of the business and the creation of a data bank ensuring its compilation.
- the analysis of the status of each software program in respect of the policy;
- the real time compilation of any new source code which the developer

creates or that he borrows from third parties;

- the preventive review of any new external source code to ascertain compliance with the established policy;

- the implementation of an automatic alert system which activates whenever external source code does not comply with the established policy and the implementation of a procedure to remedy the situation.

Using such a process will facilitate the preparation of a report on all the electronic content of the business, including information on all the source code of their software programs, their origin, the obligations resulting from all licence agreements, the history of their suppliers, the versions thereof and any other useful information for their management and use.

This report on the electronic content may eventually serve as a basis for the preparation of a certificate of integrity of the electronic content (the "**certificate**") signed by a senior executive of the business.

The best business practices would require that such a certificate be provided each time a software program changes owners in order to establish with more certainty the scope of applicable rights and obligations.

Lavery's corporate law team is able to assist you in implementing an intellectual property management policy pertaining to the software programs which your business develops or uses.

LAVERY AN OVERVIEW

- In business since 1913
- 175 lawyers
- Most important law firm in Québec
- World Services Group (WSG), a national and international network

CONTACTS

MONTREAL - 1 Place Ville Marie
514 871-1522

QUEBEC CITY - 925 Grande Allée Ouest
418 688-5000

LAVAL - 3080 boul. Le Carrefour
450 978-8100

OTTAWA - 360 Albert Street
613 594-4936

▶ lavery.ca

Pour recevoir notre bulletin en français, veuillez envoyer un courriel à info@lavery.ca.

All rights of reproduction reserved. This bulletin provides our clients with general comments on recent legal developments. The texts are not legal opinions. Readers should not act solely on the information contained herein.