# E-commerce: Some Laws and Rules You Should Be Aware of

May 7, 2020

## Author

André Vautour

Partner, Lawyer

**Various ways of doing e-commerce**

E-commerce can take different forms. For the purposes of this article, we will refer to e-commerce where the contract of sale or of supply of services is concluded by electronic means,

E-commerce will be said to be “direct” when the product or service is delivered electronically, such as in the online conclusion of a contract for a subscription to an online-only publication, and “indirect” when the item sold is tangible or the service is rendered otherwise than online. E-commerce can be conducted entirely online or in a hybrid manner, where the vendor operates both online and through brick-and-mortar stores. It is considered “closed” when it is between a relatively small number of participants who already have a contractual or professional relationship with each other. It can be conducted between a business and a consumer, in which case it is called “B2C,” or between a business and another business and is then known as “B2B.”

E-commerce poses particular challenges for businesses and if these challenges are not properly addressed, they are likely to expose the business to additional liability. This means that e-commerce can be particularly risky for novice businesses that start to do carry out business electronically, without adequate preparation.

For example, a merchant who transacts electronically will necessarily have to take direct possession of some of its customers’ personal data, such as their names, addresses and credit card numbers, or have an e-commerce service provider take indirect possession of it. The use of such personal data is subject to the provisions of privacy laws, and, given that the data is of great value to potential thieves or fraudsters, it must be protected. A merchant may also be the victim of fraudulent

orders or payments made with stolen credit cards numbers.

To better control its risks, a novice in e-commerce may be better off doing business with established e-commerce service providers such as Shopify, BigCommerce, Squarespace or GoDaddy, which have set up robust infrastructures for their customers. A corporation should nonetheless do its homework before choosing an e-commerce service provider. It should, for example, inquire about the terms and conditions of the service agreement to be entered into with the chosen provider, and, in particular, about the services offered (including how returns and chargebacks are handled), how the service provider protects its customers in the event of data theft or fraud, what fees are charged, and so forth.

In all cases, whether or not a corporation does business with an e-commerce service provider, it should ensure that the information kept on its own servers and computers is limited to what is absolutely necessary. Likewise, once a transaction is completed, it should avoid, as far as possible, keeping personal data belonging to its customers, such as their names, addresses and credit card numbers.

Moreover, a corporation that decides to engage in e-commerce must be aware of certain specific legal aspects relating first, to the particularities of e-commerce itself and second, to the fact that its customers may be located anywhere in the world. For the purposes of this article, we will focus on the rules generally applicable to all types of e-commerce. A future article will deal with the specific rules provided in the *Consumer Protection Act (Quebec)*.

**Consumption tax**

The majority of governments impose a consumption tax on goods (and sometimes services) sold within their jurisdiction. Applicable consumption tax laws generally provide that businesses with a presence in a jurisdiction must collect applicable taxes and remit them to the competent tax authorities. For a corporation that is otherwise not present in a jurisdiction, the mere fact of selling goods in that jurisdiction is generally not sufficient to require registering with its tax authorities and collecting and remitting applicable taxes. However, the definition of what constitutes a sufficient presence to require business registration and the collection and remittance of consumption taxes varies from one jurisdiction to another. A corporation wanting to sell its goods and services electronically must therefore ensure that it is aware of the applicable consumption tax rules in the main jurisdictions where it will sell these goods or provide these services.

**Licences and permits**

Although it is generally not necessary for a manufacturer or seller to obtain a license, permit or other governmental authorization for the vast majority of goods typically sold online, they may be required before certain products, in particular medical or pharmaceutical products, can be sold online or otherwise, domestically or internationally.

It is also important to note that a licence, permit or other authorization may not be required to sell goods in a jurisdiction while the sale of the same goods in another may require such license, permit or other authorization. Thus, if a merchant wants to sell its product in a jurisdiction where a permit, licence or other authorization is required, it will be required to obtain it before proceeding with any sales.

In addition, in some territories, the sale of certain goods must necessarily be done through a State monopoly. For instance, such restrictions are still the norm in Canada for the sale of alcoholic beverages. For example, a resident of Ontario may not order alcoholic beverages directly online from a producer in another province and have them delivered to Ontario, which prevents a small-scale producer of alcoholic beverages in Quebec from selling its products online to Ontario customers, for delivery in Ontario.

**Shipping**

Not all goods can be shipped in the same way. Some must be specially packaged, and some may even not be shipped by regular means, such as Canada Post and major courier companies.

For example, Canada Post requires that fish, game, meat, fruit, vegetables or other perishable products be properly prepared and meet certain other applicable requirements for mailing.

Other products, such as objects classified as hazardous materials, may simply not be shipped by mail. To ship these products, it will be necessary to deal with a specialized courier service.

Finally, Canadian laws prohibit the export of certain goods or require special permits for their export. In addition, merchants must ensure that the laws of the destination jurisdiction allow the goods shipped to be imported into that jurisdiction. Indeed, all countries either prohibit the import of certain goods into their jurisdiction or require the importer to obtain a permit or licence issued by their government.

**Age restrictions**

Under applicable laws and regulations, certain goods may only be sold to persons who have reached a certain age or may not be sold to children. These restrictions vary from jurisdiction to jurisdiction. For instance, in Quebec, one must be 18 years old to legally buy alcohol, while elsewhere in Canada the age is 19 and in the United States, 21. Merchants wishing to sell alcoholic beverages online must take these restrictions into account. The same applies to the sale of any other goods that are subject to age restrictions.

**PCI DSS compliance**

In 2006, the main credit card issuers, American Express, Discover Financial Services, JCB International, MasterCard and Visa formed the PCI Security Standards Council to standardize the rules and standards applicable to payments made with their credit cards.

The council adopted a set of rules called “Payment Card Industry Data Security Standard,” better known by its acronym, PCI DSS. All merchants wishing to accept credit card payments, including direct online payments, must adhere to these rules. Any merchant, regardless of its size, wishing to process credit card payments on its website must also be PCI DSS compliant, unless it is doing business through a compliant payment service provider.

The PCI DSS include the following 12 compliance requirements, which are grouped into six categories called “control objectives.” The following table, taken from the document entitled “Payment Card Industry (PCI) — Data Security Standard — Requirements and Security Assessment Procedures”[1], provides a summary of these requirements.

| Control objectives | PCI DSS conditions |
|---|---|
| Build and Maintain a Secure Network and Systems | 1. Install and maintain a firewall configuration to protect cardholder data<br><br>2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| | 3. Protect stored cardholder data |

| | |
|---|---|
| Protect Cardholder Data | 4. Encrypt transmission of cardholder data over open, public networks |
| Maintain a Vulnerability Management Program | 5. Protect all systems against malware and regularly update anti-virus software or programs<br><br>6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need to know<br><br>8. Identify and authenticate access to system components<br><br>9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data<br><br>11. Regularly test security systems and processes |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security for all personnel |

Although the PCI DSS are mandatory, only Visa and MasterCard require merchants and service providers that accept their cards to comply with these standards. However, a non-compliant corporation will nevertheless be held fully liable if fraud associated with theft of cardholder data occurs. In addition, should a security breach occur, all exposed merchants that are not PCI DSS compliant will be fined. It is up to merchants and service providers to achieve, demonstrate and maintain compliance through annual validations.

Merchants may use the services of specialized service providers to help them comply with PCI DSS standards. Useful tools to ensure compliance are also available online for these purposes[2].

Should a merchant not wish to go through the PCI DSS compliance process, it may always use the services of a PCI DSS compliant payment service provider[3].

---

1. PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures (Version 3.2.1, May 2018), online (PDF): *Official website of the PCI Security Standards Council*
2. These can be found through a search using the keywords “PCI DSS compliance” or “PCI DSS conformity.”
3. These can be found through a search using the keywords “PCI DSS Payment Gateway.”