

# Navigating the regulatory minefield: A guide for digital asset businesses in Canada

February 20, 2023

The regulatory environment for digital asset businesses in Canada is complex and involves a wide array of agencies and laws. These laws aim to protect investors, enforce tax laws, safeguard personal information, and combat financial crimes. Organizations must be familiar with these laws and ensure that they are complying with the requirements set out in them in order to avoid enforcement action from government entities, such as securities commissions, tax agencies, the privacy commissioner and law enforcement. Penalties for failing to comply with these laws can be severe and may include fines, asset seizure, and criminal prosecution. This article provides an overview of the types of regulatory enforcement that cryptocurrency businesses may encounter while operating in Canada.

## I. Securities

Securities commissions—such as the [Ontario Securities Commission](#) (OSC) and the [British Columbia Securities Commission](#) (BCSC)—are responsible for regulating the trading of cryptocurrencies and digital assets in order to protect investors from fraud and other unlawful practices. These commissions can take enforcement action against cryptocurrency businesses that fail to comply with provincial securities laws by: issuing cease and desist orders; adding businesses to investor warning lists; imposing fines of up to C\$1 million per violation; and ordering businesses to forfeit any profits that were obtained as a result of non-compliance.

Cryptocurrency businesses may also be subject to national instruments, such as [National Instrument 31-103 Registration Requirements and Exemptions](#), which sets out the registration requirements for businesses that engage in the trading of securities, including cryptocurrencies. This instrument specifies the categories of individuals and firms that are required to register with securities commissions and the exemptions that may apply in certain cases. Failure to comply with these registration requirements can result in enforcement action, and potentially private litigation (often in the form of expensive class actions).

## II. Tax

Tax agencies—such as the [Canada Revenue Agency](#) (CRA)—are responsible for enforcing tax laws and ensuring that cryptocurrency businesses pay the appropriate taxes on their transactions. The CRA can take enforcement action against businesses that fail to report their cryptocurrency transactions or that do not pay the required taxes.

The [Income Tax Act](#) is a federal law that sets out the rules for taxing income, including income from cryptocurrency transactions. This law requires businesses to report their cryptocurrency transactions and to pay the appropriate taxes on them. The specific tax treatment of cryptocurrency transactions depends on the circumstances of the transaction and the nature of the business. The CRA has also issued guidance on the tax treatment of cryptocurrency transactions, [including guidelines](#) on how to calculate the fair market value of cryptocurrency and how to report such transactions on tax returns.

Penalties for failing to comply with the tax laws can be severe and can include fines, interest charges, and penalties. The amount of the penalty depends on the specific circumstances of the non-compliance, such as whether the conduct was intentional or unintentional, and whether the business has a history of non-compliance. In addition, businesses may be required to pay any unpaid taxes, interest, and penalties that are assessed by the CRA.

### III. Privacy

The [Office of the Privacy Commissioner of Canada](#) is responsible for ensuring that businesses handle personal information in a way that complies with privacy laws. This includes ensuring that businesses have appropriate safeguards in place to protect the personal information of their customers, such as by encrypting data and limiting access to authorized individuals. The privacy commissioner can take enforcement action against businesses that fail to comply with privacy laws.

The [Personal Information Protection and Electronic Documents Act](#) (PIPEDA) is a federal law that sets out the rules for how businesses must handle the personal information of their customers, including requirements for protecting personal information and obtaining consent from customers. This law applies to businesses that collect, use, or disclose personal information in the course of their commercial activities, including cryptocurrency businesses that collect personal information from their customers.

Under PIPEDA, businesses are required to obtain the consent of customers before collecting, using, or disclosing their personal information. This means that businesses must inform customers of the specific purposes for which they are collecting personal information and must obtain the customer's consent before collecting, using, or disclosing that information. In addition, businesses must take reasonable steps to protect the personal information of their customers from unauthorized access, disclosure, or misuse.

Penalties for failing to comply with PIPEDA can include fines, orders to correct non-compliance, and orders to destroy personal information that has been collected, used, or disclosed in violation of the law. The privacy commissioner can also make public any findings of non-compliance with PIPEDA, which can damage a business's reputation.

## IV. Law enforcement

Law enforcement agencies—such as the Royal Canadian Mounted Police (RCMP) and the [Financial Transactions and Reports Analysis Centre of Canada \(FINTRAC\)](#)—are responsible for enforcing laws related to money laundering and other financial crimes. Cryptocurrency businesses can face enforcement action from these agencies if they are found to be involved in illegal activities, such as facilitating money laundering or other financial crimes.

The [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Act \(PCMLTFA\)](#) is a federal law that aims to prevent money laundering and terrorist financing by imposing requirements on businesses, including cryptocurrency businesses, to report suspicious transactions and to maintain records of their financial activities. This law also gives law enforcement agencies the power to seize assets, including cryptocurrencies, in connection with criminal investigations.

Under the PCMLTFA, businesses are required to report any transaction that they believe may be related to money laundering or terrorist financing to FINTRAC. This includes transactions involving large sums of money, transactions with no apparent economic or lawful purpose, and transactions that are structured to avoid reporting requirements. In addition, businesses are required to maintain records of their financial activities, including transaction records and customer identification information, in order to assist law enforcement agencies in their investigations.

FINTRAC works with businesses to ensure that they are complying with their obligations under the PCMLTFA. This may include providing guidance and support to businesses on how to meet their obligations, conducting compliance assessments, and taking enforcement action against businesses that fail to comply with the law. Law enforcement agencies, such as the RCMP, also have the power to take enforcement action against businesses that are involved in illegal activities, such as money laundering or terrorist financing, including by seizing assets and conducting criminal investigations.

## Conclusion

Given the complicated and continuously evolving regulatory landscape for digital asset business in Canada, it is an uphill battle to maintain compliance. The importance of compliance cannot be stressed enough given the severity of the penalties for violations (i.e., criminal prosecution). To avoid these potential repercussions, it is crucial for digital asset businesses to stay informed about changes in the law and seek counsel to ensure they maintain compliance.

By

[Caitlin Sainsbury](#), [Mohit Sethi](#), [Carol Derk](#), [Julie Mansi](#), [Jason Brooks](#), [Jonathan Doll](#)

Expertise

[Digital Assets](#), [Cybersecurity](#), [Privacy & Data Protection](#), [Tax](#), [Capital Markets](#), [White Collar Criminal Defence and Corporate Investigations](#)

## BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

[blg.com](http://blg.com)

## BLG Offices

### Calgary

Centennial Place, East Tower  
520 3rd Avenue S.W.  
Calgary, AB, Canada  
T2P 0R3

T 403.232.9500  
F 403.266.1395

### Ottawa

World Exchange Plaza  
100 Queen Street  
Ottawa, ON, Canada  
K1P 1J9

T 613.237.5160  
F 613.230.8842

### Vancouver

1200 Waterfront Centre  
200 Burrard Street  
Vancouver, BC, Canada  
V7X 1T2

T 604.687.5744  
F 604.687.1415

### Montréal

1000 De La Gauchetière Street West  
Suite 900  
Montréal, QC, Canada  
H3B 5H4

T 514.954.2555  
F 514.879.9015

### Toronto

Bay Adelaide Centre, East Tower  
22 Adelaide Street West  
Toronto, ON, Canada  
M5H 4E3

T 416.367.6000  
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing [unsubscribe@blg.com](mailto:unsubscribe@blg.com) or manage your subscription preferences at [blg.com/MyPreferences](http://blg.com/MyPreferences). If you feel you have received this message in error please contact [communications@blg.com](mailto:communications@blg.com). BLG's privacy policy for publications may be found at [blg.com/en/privacy](http://blg.com/en/privacy).

© 2025 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.