



Law Society PEI

Use of Technology to Support Client Identification and Verification Guidance

September 21, 2026

Contents

Introduction.....	2
Client Identification Verification.....	2
Government-issued Documentation.....	3
Steps to verify an individual’s identity (ID).....	3
Authentication Technology	4

Introduction

Money laundering and terrorist financing are on the rise in Canada. Guidance, prepared by the Federation of Law Societies of Canada (FLSC) describes the responsibilities of Canada’s legal profession to ensure they are not facilitating money laundering and terrorist financing. In February 2024, FLSC published Guidance to the Legal Profession – [Your Professional Responsibility to Avoid Facilitating or Participating in Money Laundering and Terrorist Financing](#). This document provides detailed guidance including red flags and real-life examples and sets out the components of the legal profession’s duties as contained in the Model Rules.

FLSC has issued guidance requiring the use of technology capable of verifying the authenticity of government-issued photo identification (ID) when verification occurs remotely.

Members who choose to verify an individual’s identity using video conferencing or other forms of virtual communication must have a process or method in place to authenticate the individual’s ID.

This guidance only applies to the verification of government-issued photo identification.

Client Identification Verification

When a lawyer has been retained by a client to provide legal services engages in or gives instructions in respect of the receiving, paying or transferring of funds, the lawyer is required to verify the identification of the client [regulation 86.(6) (a)]. Methods include:

1. reviewing government-issued photo identification (ID);
2. reviewing the client’s credit file;
3. the dual-process method (reviewing two original, valid and current documents or information from independent and reliable sources).

Government-issued Documentation

You may rely on a valid, authentic and current federal, provincial or territorial government, or a foreign government, other than a municipal government, that is used in the presence of the individual to verify that the name and photograph are those of the individual [regulation 86. (6) (f)]. A document is authentic if it is genuine and has the character of an original, credible and reliable document. For example, an original physical government-issued photo identification document is authentic.

Verification of the government-issued photo identification can be completed by using one of the following:

1. When relying on the physical document, you or your agent must examine it in the presence of the individual. The document must show the individual's name, include a photo of the individual, and have a unique identifier number. You must ensure that the document is issued by a competent authority, that it is valid and current and that the individual's name and photograph match. It is not acceptable to view photo identification online through a video conference.
2. When an individual is not physically present you or your agent may rely on a government-issued identification document if you have a process in place to authenticate the document and to determine that it is valid and current. To authenticate the document, certain technologies can be used. Available through various commercial identity verification platforms, these include technologies such as optimal character recognition data capture (a program that extracts data from scanned documents, camera images, etc.) and biometric face matching, which process the information and are capable of determining the document's authenticity.

If you opt for in-person review, you are permitted to use remote authentication technology to verify the identity document.

Steps to verify an individual's identity (ID)

1. **Identify and access the risks** – obtain information about the client and the proposed legal services, identify and access the risks to determine if it is proper to act. Make reasonable inquiries and record the results. Consider the FLSC [Red Flags Quick Reference Guide](#).
2. **Set up a virtual meeting.** Book a virtual meeting with your client on a secure and private video conferencing technology. Ask the client to have their ID with them when you meet.

3. **Confirm the ID is authentic.** Obtain from the client, by a secure manner, a copy of the front and back of the government-issued identification document. A high-resolution image is preferable (clearer, easier to see detail) to a low-resolution image (less sharp). Use verification technology and the providers defined process to confirm the ID is authentic. Obtain and maintain confirmation of verification.
4. **Confirm the ID is valid and current.** During the virtual meeting ask the client to hold their ID to the camera and compare it to the ID that was authenticated. Check the name and photo match and the expiry date is current.
5. **Document and retain a record.** Document the process you followed and maintain a copy of all documents, including the scanned ID and confirmation of its authenticity from the verification technology.

Authentication Technology

The use of technology to verify government-issued identification documents is growing in Canada's legal sector. According to the Digital Identification and Authentication Council of Canada ([DIACC](#)) 2025 Annual Report, Canada's legal sector processed more than [700,000+ client IDV transactions](#). Increasing use of technology is being driven by increase in fraud activity and fraudulent documents and the law society's requirements as it relates to Anti Money Laundering and Terrorist Financing (AMLTF).

The Law Society does not vet or endorse authentication technology products. It is the lawyer's responsibility to review and evaluate the risks and benefits of authentication technology products and whether their preferred choice satisfies the burden on them to verify the authenticity of the ID.

Considerations when considering an authentication product:

- Will the vendor's report provide you with the information that you need?
- Does the vendor ask the client to provide too much information?
- Does the vendor unnecessarily retain the client's data?
- Do they store any information outside Canada?
- What does their privacy policy say?
- Consider obtaining advice from your firm's information technology professionals for competent understanding of the vendors' products and services.

For additional information please refer to Payment's Canada – [AI Solutions for Digital ID Verification: An overview of machine learning \(ML\) technologies used in Digital ID verification systems](#). Additionally, [DIACC](#) a non-profit, offers a certification program for service providers. It provides a directory of member services which can be found [here](#).