

## Guidance for virtual verification of your client's identity using government-issued photo ID and technology

### Introduction

The Law Society Rules provide for four methods to verify an individual client's identity: (1) the government-issued photo ID method (physical meeting requirement); (2) government-issued photo ID method (virtual meeting with reliable authentication technology requirement); (3) credit file method (no physical meeting requirement); (4) dual process method (no physical meeting requirement). You can use any one of the four methods. On occasion, you may decide to use more than one method if circumstances warrant.



You can verify an individual's identity in person or virtually using the individual's photo ID issued by the

government of Canada, a province or territory or a foreign government. The ID must be valid, authentic and current. The virtual verification method, effective March 8, 2024, can be used with the individual's consent, whether they are inside or outside of Canada. To verify an individual's identity virtually, you must use reliable authentication technology to confirm that the ID is genuine, and confirm that the name and photo of your client are those of the individual in the ID. Below are steps to verify an individual's identity virtually. Your responsibilities may be fulfilled by you or by a member or employee of your firm on your behalf (Rule 3-99(3)). You may use an agent (Rule 3-104).

### Step 1: Identify and assess risks

In the course of obtaining information about the client and the proposed services, identify and assess risks to determine what steps you will take and if it is proper to act. Make reasonable inquiries and record the results. Consider *BC Code* rule 3.2-7 and commentary, Law Society Rule 3-109 and applicable [Client ID & Verification and Anti-Money Laundering](#) resources such as the [Top 10 tips](#), the Federation of Law Societies' [Red Flags Quick Reference Guide](#) and the Government of Canada's [2025 Assessment of Money Laundering and Terrorist Financing Risks in Canada](#).

## **Step 2: Arrange a virtual meeting with the individual**

See our practice resource, [Using Video-conferencing technology: guidance and professional obligations](#), for best practices and tips for meetings. A video conference alone with a scan or an image of the ID is not sufficient to satisfy your verification obligations under Law Society Rule 3-102. Assuming that you will use a third-party service provider (see step 3) to verify the client's identity using authentication technology, your virtual meeting will likely occur after the client's identity has been authenticated.

## **Step 3: Authenticate the photo ID using technology**

Use reliable authentication technology to confirm that the individual's ID is genuine. Technology can assess the government-issued photo ID against security features (e.g. size, texture, character spacing, raised lettering, format, design, holograms, barcodes, magnetic strips, watermarks, embedded electronic chips) and marks such as logos and symbols (e.g. an animal or bird).

For some general background on authentication technology and what it does, see Payments Canada's ["AI Solutions for Digital ID Verification: An overview of machine learning \(ML\) technologies used in Digital verification systems"](#). Your authentication technology service provider would ask the individual (by email or text message) to provide an image of the front and back of their government-issued photo ID. They would also ask the individual to provide a live selfie or face scan. Then they would run the ID through tests to determine its authenticity and provide you with a report. You would want to let the client know what to expect so that they are not surprised and they can consider whether they will provide their consent to this process.

Use your judgment when reviewing and evaluating the risks and benefits of various authentication technology service providers and making choices. You may use the Law Society's [Cloud Computing Checklist](#), v. 4.0 to assess some aspects of a technology vendor's services and products such as privacy, security data breaches, service failure and insurance (not all of the checklist is applicable). Consider, for example:

- Will the vendor's report provide you with the information that you need?
- Does the vendor routinely ask the clients to provide more information that you normally require? If yes, why?
- Does the vendor unnecessarily retain the client's data? If they retain data, how long do they retain it?
- Does the vendor store any client data outside of Canada? If yes, does that matter to your client?
- Does the vendor share client information with any third-party service providers?
- Are you comfortable with the vendor's privacy policy? Security?
- Do they offer services English and French, or other languages?

- How easy it is to use their services? What kind of support do they offer?
- Are there onboarding costs? Do they have a pay-as-you-go option?
- Does the vendor hold any relevant certification? Did they undergo an audit by an independent third-party for the certification? Is their certification current?

Consider obtaining advice from your firm's information technology professionals for competent understanding of the vendors' products, services and certifications. Note your professional obligations in [BC Code rule 3.1-2](#), commentary [4.1] and [4.2] regarding technological competence.

Vendors' charges to verify an individual's identity vary (e.g. from around \$5 to \$25 per individual). Some vendors retain the clients' data for days or years, and it could be retained outside of Canada. One vendor explained that they do not retain the data; they provide the report to the lawyer and it is up to the lawyer to retain the report for the required time.

The Digital ID & Authentication Council of Canada (DIACC) is a non-government body that has developed certifications for vendors of authentication technology. It is not affiliated with the Law Society. While the Law Society does not vet, endorse or certify vendors of authentication technology nor vendors' claims of compliance with Law Society requirements, [DIACC's Certified Service Providers Authoritative Trust Registry](#) may be a starting place if you are considering such a service. The Trust Registry sets out a list of service providers that have been independently audited and the certifications that they have achieved.

#### **Step 4: Confirm the photo ID is valid and current**

After the ID is authenticated, you should receive a report. You want to satisfy yourself that the individual featured in the authenticated ID that you have in the report (ideally including the both the authenticated ID and the individual's selfie) is the individual you are meeting with. Assuming you are not physically meeting with the client, during a live video meeting, you can ask the individual to show you the front and back of their ID and compare it to the authenticated ID. You can compare the features of their image on your screen to that of the authenticated ID.

Check that the name, address and currency date of the ID used in the video meeting matches the name, address and currency date of the authenticated ID. Also check that the name and address match the identification information that you obtained under Rule 3-100.

#### **Step 5: Record keeping and retention**

Retain a record of the information, with applicable dates, of any information or documents obtained or produced for the purposes of client identification and verification (Law Society Rule 3-107).

#### **For more information**

For more information, read Rules 3-98 to 3-110 and refer to the resources on the [Client ID & Verification and Anti-Money Laundering Risk Management web page](#). Lawyers are welcome to contact [practiceadvice@lsbc.org](mailto:practiceadvice@lsbc.org), call 604.443.5797 or [book an appointment](#) if they have questions.