PCTF Law Society Profile

Document Status: Draft Recommendation V1.0

In accordance with the DIACC Operating Procedures, Draft Recommendations are a deliverable which is used to share early findings and to gather broad feedback.

This document has been developed by DIACC's Trust Framework Expert Committee. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme.

Table of Contents

1. Introduction to the PCTF Law Society Profile

This document specifies the Conformance Criteria for the Pan-Canadian Trust Framework (PCTF) Law Society Profile. For a general introduction to the PCTF, including contextual information and the PCTF goals and objectives, please see the PCTF Overview.

The Federation of Law Societies of Canada (FLSC) leads efforts to prevent money laundering and terrorist financing in the practice of law. Model rules developed by the Federation and implemented by Canada's law societies, ensure members of the legal profession are bound by comprehensive "know-your-client" requirements. These rules also restrict the use of professional trust accounts and limit the amount of cash legal professionals can accept.

It can be difficult for individual lawyers to perform client identification and verification in a consistent, reliable, and repeatable manner given that these activities may be outside their fields of expertise. For this reason and others, lawyers may seek professional assistance with these processes from other agents or vendors that provide those services on a commercial basis.

This profile has been created to outline a series of Conformance Criteria that can be used to assess these organizations against a set of common practices and criteria to ensure a consistent and reliable result regardless of which compliant organization is used. This can provide lawyers with the assurance that a verified compliant provider is meeting the minimum standards necessary to ensure that client identification and verification has been completed to the standards outlined by the FLSC.

This profile includes the Conformance Criteria themselves as well as related information essential to understanding and interpreting those criteria including definitions of key terms and concepts. They also set constraints around the criteria used to standardize and assess the integrity of the Trusted Processes that are described within this profile.

2. Trusted Processes

The PCTF promotes trust through a set of auditable business and technical requirements for various processes. A process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition – an output on which others typically rely.

In the PCTF context, a process that is designated a Trusted Process is assessed according to well-defined and agreed upon Conformance Criteria. The integrity of a Trusted Process is paramount because many participants – across jurisdictional, organizational, and sectoral boundaries and over the short-term and long-term – rely on the output of that process.

Note: For more information on Trusted Processes associated with client identification and verification, please review the PCTF Verified Person component.

3. Profile Background

The PCTF Law Society Profile builds on work established in other related contexts to define pertinent Conformance Criteria, including:

- The FLSC Model Rule on Client Identification and Verification;
- The PCTF Verified Person component; and,
- Best practices and lessons learned from established industry organizations that conduct these processes in the real world on a daily basis.

Note: PCTF Conformance Criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy, and regulations in their jurisdiction.

4. Document Conventions

4.1 Conformance Criteria Keywords

The following keywords indicate the precedence and general rigidity of a given Conformance Criteria, and are to be interpreted as:

- **MUST** means that the requirement is absolute as part of the Conformance Criteria.
- **MUST NOT** means that the requirement is an absolute prohibition of the Conformance Criteria.
- **SHOULD** means that the requirement is expected to be met, except in limited cases where the applicant documents valid reasons or circumstances to ignore the requirement. The full implications of such an exception must be understood and carefully weighed before choosing to not adhere to the Conformance Criteria as described.
- **SHOULD NOT** means that a valid exception reason may exist in particular circumstances when the requirement is acceptable or even useful, however, the full implications should be understood and the case carefully weighed before choosing to not conform to the requirement as described.
- **MAY** means that the requirement is discretionary but recommended.

Keywords appear in **bold** and ALL CAPS in the Conformance Criteria.

4.2 Terms and Definitions

For a comprehensive list of terms and definitions used in the PCTF, please refer to the PCTF Glossary.

- **Authorized Agent/Agent:** A lawyer may rely on an Agent to perform one or more Trusted Processes to collect information and verify the identity of an individual client, third party or individual, provided the lawyer and the Agent have

an agreement in writing. Conformance Criteria in this profile refer to such an Agent as the Responsible Authority.

- **Reliable Source:** A Reliable Source is an originator or issuer of information that is used to verify the identity of the client. To be considered reliable under the FLSC Model Rule, the source should be well known and considered reputable. For example, reliable sources can be the federal, provincial, territorial and municipal levels of government, Crown corporations, financial entities or utility providers.
- **Responsible Authority:** A Role that a Participant performs to provide one or more of the Verified Person or Verified Organization Trusted Processes in order to establish that a Subject is real, unique, and identifiable, and protects related information against compromise. In the context of the FLSC Client Identification and Verification Conformance Criteria, a Responsible Authority is an individual or organization acting as an agent on behalf of a lawyer to fulfill their responsibilities for client identification. A Responsible Authority can never assume the accountability of a lawyer for this purpose.

5. Conformance Criteria

Conformance Criteria are organized according to the three identification and verification methods described in the FLSC Model Rule:

Credit File Method:

- A method to verify an individual's identity by relying on information in a Canadian credit file if it has been in existence for at least three years. The name, address, and date of birth in the credit file must match that provided by the individual.

Dual Process Method:

- A method for verifying an individual's identity by relying on any two of the following:
  - information from a Reliable Source that contains the individual's name and address;

- information from a Reliable Source that contains the individual's name and date of birth; and
- information containing the individual's name that confirms they have a deposit account or credit card or other loan account with a financial institution.

Photo ID Method:

- A method for verifying an individual's identity using a valid, authentic, and current (not expired) government-issued identification document containing the individual's name and photograph (e.g. driver's licence, passport, Secure Certificate of Indian Status, Permanent Resident Card, or certain provincial or territorial health insurance cards). Identification documents issued by a foreign government that are equivalent to a Canadian-issued identification document may also be used.

Reference	Conformance Criteria
101	**Federation of Canadian Law Societies**
101.1	**Client Identification and Verification**
101.1.1	**Credit File Method**
101.1.1.10.1	The name, address and date of birth provided by the individual whose identity is being verified **MUST** be matched with the name, address and date of birth contained in the records of a Credit Bureau regulated in Canada (as examples, Equifax and Transunion).
101.1.1.20	Any credit file information used to conduct an identity verification process **MUST** have been in existence for at least three years from the date of verification.
101.1.1.30	Any credit file information used to conduct an identity verification process **MUST** contain information derived from more than one source (i.e., more than one tradeline).
101.1.1.40	Any credit file information used to conduct an identity verification process **MUST** be obtained directly from a Canadian Credit Bureau or through a third-party vendor authorized by a Credit Bureau regulated in Canada.

164i	**101.1.1.50**	The Responsible Authority **MUST** have a written agreement in place with a Credit Bureau regulated in Canada that authorizes access to Canadian credit file Information.
164j	**101.1.1.60**	Any credit file information used to conduct an identity verification process **MUST**: • Be obtained at the time the verification process is conducted; and, • Be valid and current at the time the verification process is conducted. (i.e., an individual cannot provide you with a copy of their credit file, nor can a previously obtained credit file be used).
164k	**101.1.1.80**	An identity verification policy **MUST** be developed and documented, describing the risk assessment framework used to assess differences between current credit file information and the claimed identity.
164l	**101.1.1.90**	An Identity Verification Policy **MUST** describe the approach used to evaluate differences in name, address, and date of birth between the credit file and the claimed identity, either individually or as part of a larger data set.
164m	**101.1.1.100**	When a credit bureau returns anti-fraud flags of any kind in response to an identity verification event, the Responsible Authority **SHOULD** have business processes in place to evaluate these flags for acceptable risk according to documented policy.
164n	**101.1.1.110**	The Responsible Authority **SHOULD** verify that any credit file data used for an identity verification process contains at least two distinct tradelines within the past three (3) years. (i.e., tradelines reported from two different legal entities)
164o	**101.1.1.120**	The Responsible Authority using the Credit File Method **MUST** collect the legal name, date of birth, and home address information for the individual being verified and provide this data to the Canadian Credit Bureau for processing, including: • At least two (2) home addresses if the party has moved within the past three (3) years; and, • Up to six (6) home addresses maximum.
164p	**101.1.2**	**Dual Process Method**
164q	**101.1.2.10.1**	When verifying the name, address, and date of birth provided by the individual claiming an identity, the Responsible Authority **MUST** ensure the

		information it receives is valid and current, comes from two (2) different Reliable Sources, and contains at least two (2) of the following: • Information from a reliable source that contains the individual's name and address; • Information from a reliable source that contains the individual's name and date of birth; and, • Information that contains the individual's name and confirms that they have a deposit account or a credit card or other loan amount with a financial institution.
164r	**101.1.2.20.1**	Information sourced by the Responsible Authority or agent of the Responsible Authority from within their own line of business, **MUST NOT** be used to verify identity.
164s	**101.1.2.30**	Information from the individual claiming the identity **MUST NOT** be used to also verify the identity. (Information collected from an individual is used to resolve the claimed identity to a single legal person which is then subsequently verified against reliable sources to ensure that the resolved identity exists and is valid.)
164t	**101.1.2.40**	If credit file data is used as one of the sources used to satisfy the requirements of the Dual Process Method, the Responsible Authority **MUST** confirm the credit file from which the data is extracted has been in existence for at least six months.
164u	**101.1.2.50**	If credit file data is used as one of the sources used to satisfy the requirements of the Dual Process Method, the Responsible Authority **MUST** verify that the credit file has been established and is active at time of verification and that it contains at least two distinct tradelines. (i.e., tradelines reported from two different legal entities)
164v	**101.1.2.61**	The Responsible Authority **MUST** ensure documents used to satisfy the requirements of the Dual Process Method, (e.g., a bill from a utility company): • Are valid, unaltered, current and authentic; and, • Originate from, or are issued by, the Reliable Source or, alternatively, are obtained directly from the Reliable Source.
164w	**101.1.2.70**	Physical documents without built-in authentication mechanisms **SHOULD NOT** be used as a source unless they are presented for examination in-person.

164x	**101.1.2.80**	The acceptable level of risk resulting from differences between the information provided by the reliable source and the claimed identity information **MUST** conform with the requirements of regulated industry services, if applicable.
164y	**101.1.2.90**	An Identity Verification Policy that describes the risk assessment framework and the approach used to evaluate differences in the name, address, and date of birth, **MUST** be developed and documented.
164z	**101.1.2.100**	Any credit file information used to conduct an identity verification process **MUST** contain information derived from more than one source (i.e., more than one tradeline).
164aa	**101.1.3**	**Photo ID Method**
164ab	**101.1.3.10**	The Responsible Authority **MUST** collect and return all the following data points from Government-Issued Photo Identification to the to the Relying Party (e.g., lawyer): • The individual's name; • The date on which the individual's identity was verified; • The type of document used for verification (e.g., driver's licence, passport, etc.); • A unique identifying number of the document used; • The jurisdiction (province or state) and country of issue of the document; and, • The expiry date of the document, if available. (i.e., if this information appears on the identification document, it must be collected and returned).
164ac	**101.1.3.20**	The Responsible Authority **MUST** evaluate the security features of the government-issued photo identification document to verify that it is a valid document as issued by the Authoritative Source (e.g., federal, provincial, territorial or foreign government).
164ad	**101.1.3.30**	For documents with MRZs and/or barcodes, the Responsible Authority **SHOULD** compare the contents of the MRZ/barcode with OCR extracted data and highlight mismatches. (An MRZ code is a string of characters that appears on the bottom of the personal data page of a passport. It is a combination of letters, numbers, and symbols that are arranged in three lines.)

		(OCR data extraction is the process of turning images of text into a machine-readable format)
164ae	**101.1.3.40**	The Responsible Authority **MUST** enforce the capture of Government-Issued Photo Identification documents in real time and prevent the uploading of an image file.
164ef	**101.1.3.50**	The Responsible Authority **MUST** support, at minimum, presentation of any of the following Government-issued Photo ID document types: • Canadian Passports; • Canadian Drivers' Licenses; • Canadian Permanent Resident Card; • Canadian Provincial or Territorial Photo ID Card (including the BC Services Card); and, • Canadian Certificate of Indian Status.
164ag	**101.1.3.60**	The Responsible Authority **MUST** comply with accessibility standards such as WCAG (2.0 level AA or better). (Web Content Accessibility Guidelines (WCAG) are developed through the W3C process in cooperation with individuals and organizations around the world, with a goal of providing a single shared standard for web content accessibility that meets the needs of individuals, organizations, and governments internationally.)
164ah	**101.1.3.70**	The Responsible Authority **MUST** use face recognition technology to compare the features of the selfie to the photo on the authentic government-issued photo identification document (i.e., face matching).
164ai	**101.1.3.80**	Face-matching solutions employed by a Responsible Authority **MUST** undergo testing by a third-party lab to evaluate the performance of the face recognition algorithm in a one-to-one matching scenario. (The existence, but not the content, of these test results must be available to be verified by an external auditor.)
164aj	**101.1.3.90**	The Responsible Authority completing the Government-Issued Photo Identification Method **MUST** perform an active or passive liveness check on the selfie.
164ak	**101.1.3.100**	The Responsible Authority completing the Government-Issued Photo Identification Method **MUST** have the Liveness check certified for

		Presentation Attack Detection according to the following criteria: ISO 30107-3 (certified by a third party). (Presentation Attack Detection is automated detection of an attempt to subvert a liveness check through measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture.)
164al	**101.1.3.110**	When using a mobile application to scan NFC-readable Photo ID documents, an NFC chip reading **SHOULD** be used for a higher level of assurance to cryptographically verify authenticity and issuer certificate origin. (Near-field communication (NFC) is a set of communication protocols that enables communication between two electronic devices over very short distances)

165

166 # 6. Revision History

Version	Date of Issue	Author(s)	Change Description
0.01	2024-10-22	PCTF Law Society Design Team	Initial Discussion Draft
0.02	2024-12-02	PCTF Law Society Design Team	Minor editorial changes per initial TFEC review, addition of examples and improved clarity on conformance criteria.
1.0	2025-01-15	PCTF Law Society Design Team	Approved by TFEC as Draft Recommendation V1.0

167