OSLER

FINTRAC updates guidance regarding identity verification methods permitted under amendments to anti-money laundering and anti-terrorist financing regulations

NOVEMBER 26, 2019 8 MIN READ

Related Expertise

- Capital Markets
- Corporate Governance
- Financial Services
- Financial Services Regulatory
- Privacy and Data Management

Authors: Joanna Fine, Elizabeth Sale

In this Update

- Updated *Methods to verify the identity of an individual and confirm the existence of a corporation or an entity other than a corporation* published by FINTRAC on November 14, 2019 confirm that reporting entities are expected to use software or other technological tools to verify the authenticity of electronic copies of government-issued photo identification (photo ID).
- The updated FINTRAC guidance explains that in order to verify the identity of an individual by reviewing an "authentic, valid and current" electronic copy of their photo ID, a reporting entity is expected to use software or other technological tools.
- Reporting entities will want to ensure that use of technology to authenticate photo ID complies with their obligations under Canadian privacy legislation, and that privacy and security issues are considered and addressed.
- The updated FINTRAC guidance also provides clarity and useful tips regarding the credit file method and dual-process method of identity verification, as well as the policies and procedures which must be maintained in respect of all identity verification methods.

Background

In July 2019, the Canadian government finalized amendments to regulations made under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Amendments). One key change to Canada's anti-money laundering and anti-terrorist financing regime included in the Amendments is that reporting entities are now permitted to rely on digital copies of photo identification documents provided that they are "authentic, valid and current." Prior to the Amendments, identity verification documents had to be "original, valid and current" and therefore reliance on photocopies and scanned documents was not permitted.

The change from "original" to "authentic" was expected to modernize Canada's AML regime and reduce compliance burden for reporting entities. However, the updated *Methods to verify the identity of an individual and confirm the existence of a corporation or an entity other than a corporation* published by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) on November 14, 2019, (the Updated Guidance) confirm that reporting entities are expected to use software or other technological tools to verify the authenticity of electronic

copies of government-issued photo identification (photo ID).

For reporting entities, this means that although the manual compliance burden may be reduced, the cost of compliance may not be. Further, the Updated Guidance raises issues regarding data collection and privacy that will need to be carefully considered.

Updated FINTRAC guidance on identity verification

The Updated Guidance makes changes to all three methods that reporting entities can use to verify the identity of individuals: (i) government-issued photo ID method; (ii) credit file method; and (iii) dual process method.

The Updated Guidance provides clarity regarding the process for confirming the existence of corporations and other entities, but does not materially change the previously issued FINTRAC guidance.

Government-issued photo ID

Prior to the Amendments, original photo ID had to be examined in the presence of the individual whose identity was being verified. The Updated Guidance explains how a reporting entity can verify the identity of an individual, whether physically present or not, by reviewing an "authentic, valid and current" electronic copy of their photo ID.

The Updated Guidance defines "authentic" to mean, in respect of a photo ID that is used to verify identity, is genuine and has the character of an original, credible and reliable document issued by the competent authority (federal, provincial, territorial government).

The Updated Guidance indicates that when conducting in-person identity verification, a reporting entity can determine the authenticity, validity and currency of photo ID by looking at the characteristics of the original physical document, its security features (or markers, as applicable) and expiry date in the presence of the individual. This process is consistent with current practice for in-person ID verification.

The Updated Guidance prescribes a new process for verifying the identity of an individual who is not physically present with reference to an electronic copy of the government-issued photo ID by requiring that the authenticity of such government-issued photo ID be determined "by using a technology capable of assessing the document's authenticity."

For example, the Updated Guidance indicates that an individual may be asked to scan his or her photo ID using a mobile phone camera. The reporting entity would then apply technology to compare the features of the photo ID against known characteristics (for example, size, texture, character spacing, raised lettering, format, design), security features (for example, holograms, barcodes, magnetic strips, watermarks, embedded electronic chips) or markers (for example, logos, symbols) to be satisfied that it is authentic.

In addition to verifying the authenticity of the photo ID, the reporting entity must confirm that the individual presenting the photo ID is the same person whose name and photo are on the ID. This can be achieved through a live video chat session, or the individual may take a "selfie" photo using his or her mobile phone camera, to which the reporting entity would apply facial recognition software to compare the features of the selfie to the photo on the authentic photo ID. The Updated Guidance indicates that the verification of the authenticity of the ID and the verification of the individual (ensuring that the name and picture matches the name and face of the person), do not need to happen concurrently.

While the ability to use technology to authenticate the identity of an individual will be helpful to reporting entities, reporting entities will want to ensure that privacy and security issues are considered and addressed. This will include conducting due diligence on any third-party service provider providing the technology, as well as requiring such third parties to contractually agree to comply with privacy and security obligations.

Reporting entities will also want to ensure that the use of the technology otherwise complies with its obligations under Canadian privacy legislation, including limiting the collection of personal information to that which is necessary for the verification purposes, and only recording the information that is required under the Updated Guidance.

Reporting entities will also need to ensure they comply with consent obligations under applicable Canadian privacy or other legislation. For example, in Québec, *An Act to establish a legal framework for information technology* specifically requires entities to obtain express consent prior to verifying a person's identity through a process that allows biometric data to be recorded, and there are also registration requirements that may apply.

While the use of technology to verify identity can assist reporting entities to comply with safeguarding obligations under Canadian privacy legislation, care should be taken to ensure that privacy and security issues are addressed. Canadian privacy regulatory authorities have issued guidance on the collection and use of government-issued ID as well as facial recognition technology that entities will want to review prior to implementing a new technology.

Credit file method

The Updated Guidance does not materially change the process for relying on the credit file method. However, it provides helpful clarity to reporting entities that they are permitted to exercise some discretion when there is a small discrepancy between the name or address provided by an individual and the credit file information. Reporting entities are permitted to determine that when there is a slight typo in the address or name, the information still matches what the individual provided; however, if there is a discrepancy in the date of birth, the reporting entity would be more likely to conclude that the information does not match. Similarly, the Updated Guidance notes that an address provided by an individual may not be the primary address included in their credit file, but if the address is included as a secondary address, this may meet the ER's requirements for ensuring that the information matches.

In addition, the Updated Guidance explicitly contemplates that a verifier may rely on a third-party vendor to provide valid and current information contained in the individual's credit file. A third-party vendor is an entity that is authorized by a Canadian credit bureau to provide access to Canadian credit information.

Dual-process method

The dual-process method allows reporting entities to verify identity by referring to information from two reliable sources to verify either name and address, name and date of birth or name and existence of a financial account. Documents or information reviewed under this method no longer need to be "original." Under the dual-process method, reporting entities may rely on government-issued photo ID and statements, letters, certificates, forms and other documents provided by reliable sources, such as government (e.g., property tax assessments, government benefit statements, utility bills) and financial entities (e.g., bank account statements, credit card or loan statements, processed cheques, micro-deposits). Interestingly, the Updated Guidance does not indicate that reporting entities

need to use authentication software or other technology to verify the authenticity of photo ID or other acceptable documents used in the dual-process method.

The Updated Guidance stipulates that account information collected in the dual-process method must be for a deposit account, credit account or loan account and that the account number or other number associated with the information may not be truncated or redacted. The Updated Guidance also clarifies, as under the credit file method, that a reporting entity can conclude that information in a document provided under the dual process method matches information provided by the individual notwithstanding slight typos in name and address, but that errors in the date of birth would indicate a mismatch.

Confirming the existence of entities and corporations

The Updated Guidance does not materially change the previously issued FINTRAC guidance with respect to the process for confirming the existence of a corporation or other entity. However, it provides certain clarity to reporting entities, for example, to confirm the existence of a corporation, a verifier can refer to the corporation's certificate of incorporation.

Policies and procedures

The Updated Guidance states that a reporting entity's compliance policies and procedures must describe the processes that it will use for each identity verification method, including how the reporting entity will ensure that the information is valid and current. When using photo ID, the policies and procedures must describe the steps used to verify that the name and photo are those of the individual (e.g., in-person, video chat, selfie photo). When using the credit file method, the policies and procedures must prescribe steps to be taken if the information is not valid and current (e.g., use a different method, stop the transaction, etc.).

How can we help?

We would be pleased to advise your firm regarding implementation of the Updated Guidance. Please contact Lori Stein, Elizabeth Sale, Jennifer Jeffrey, Joanna Fine or your primary legal contact at Osler for assistance.