Borden Ladner Gervais

FINTRAC ISSUES FINAL GUIDANCE FOR NON-FACE-TO-FACE VERIFICATION USING IDENTIFICATION DOCUMENTS

NOVEMBER 19, 2019

On July 10, 2019, the long-awaited *Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019* (the Amending Regulations) were issued. The Amending Regulations bring changes to each existing regulation (together, the PCMLTFA Regulations) under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the PCMLTFA).

The Amending Regulations seek to modernize Canada's anti-money laundering regime. Most changes will come into force in June 2020 (new virtual currency regulations) or June 2021. One promised change that took immediate effect, however, was relaxing of client verification rules designed to allow more flexibility and the use of technology-based verification processes. FINTRAC has now issued guidance stating its expectations on how to authenticate digital copies of identification, requiring use of technology solutions.

It is no longer required to view an "original" identification document in order to use the document to verify an individual client. It is now sufficient to view an "**authentic**, valid and current" copy of an identification document. While this change has been in effect since June 2019, most reporting entities have been awaiting guidance from the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) on its expectations for authentication of copies of identification documents before relying on it. The final guidance is now available and can be found here.

The key sections of the FINTRAC guidance on authentication of copies of identification documents state as follows:

If an individual is **not physically present**, the authenticity of a government-issued photo identification document must be determined by using a technology capable of assessing the document's authenticity. For example:

an individual could be asked to scan their government-issued photo identification document using the camera on their mobile phone or electronic device; and
a technology would then be used by you, as the [reporting entity], to compare the features of the government-issued photo identification document 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 an authentic document as issued by the competent authority (federal, provincial, territorial government).

When an individual **is not physically present,**you must still determine if the individual presenting the government-issued photo identification document matches the name and photo of the person in the authenticated document provided. For example:

An individual could participate in a live video chat session and you, as the [reporting entity], would then be able to compare the name and the features of the live video image to the name and photo on the authentic government-issued photo identification document; or
An individual could be asked to take a "selfie" photo using the camera on their mobile phone or electronic device, and an application used by you, as the [reporting entity], would apply facial recognition technology to compare the features of that "selfie" to the photo on the authentic government-issued photo identification document. A process would have to exist to also compare the name on the government-issued photo identification document with the name provided to you, as the [reporting entity], by the individual.

FINTRAC has indicated that it is not enough to view a person and their identification document online by video conference or otherwise. Technology must be used to analyze and authenticate the digital copy, the name and the image. All must then be confirmed to match the individual.

To use new methods, a reporting entity's compliance policies and procedures must describe the processes used to ensure the identification document is authentic, valid, current, and matched to the individual. Authentication of the document and verification that its photo and name match the client does not need to happen concurrently.

The interpretation by FINTRAC is narrow. It only contemplates use of the new regulatory framework to implement technology-based authentication processes. The language of the regulation could arguably permit other approaches and flexibility to avoid using agents and mandataries, such as receiving copies of documents authenticated by lawyers and notaries, or having staff of affiliates that do not qualify for the affiliate verification method verify the authenticity of the copy to be used for verification by the reporting entity itself.

It remains to be seen whether FINTRAC will reassess the guidance to allow manual processes of authentication that can reasonably be argued to meet the requirements of the regulation, are more flexible than an agency or mandatary process, and could be helpful stop-gap measures while technology solutions are developed and implemented.

Reporting entities can generally continue to rely upon their existing policies and procedures to meet their obligations under the PCMLTFA to verify individuals. However, if new methods are going to be adopted, policies and procedures should be reviewed and updated to reflect these new processes.

Authors

Robert Dawkins
RDawkins@blg.com
604.640.4027

Cindy Zhang
CZhang@blg.com
604.640.4201

Stephen J. Redican
SRedican@blg.com
416.367.6134

Expertise

Financial Services Sectors