Treefort Technologies Incorporated

Response to the Financial Services Regulatory Authority of Ontario's Proposed Guidance: Detecting and Preventing Mortgage Fraud

April 26th, 2023

About Treefort Technologies Incorporated

Treefort Technologies Incorporated ("Treefort") is a Canadian digital ID verification, virtual meeting, and electronic signature company. Our company was incorporated in January 2020, and we launched the first version of our digital ID verification tool in September 2020. In July 2021 Stewart Title Guaranty Company purchased a controlling interest in Treefort and in November 2022 we ran a beta-test of our digital ID verification platform with law firms in Ontario. The beta-testing concluded in January 2023, and we formally launched our digital ID verification platform in Ontario that same month. We currently count amongst our clients Canadian title insurance companies, the Society of Notary Publics of British Columbia and over 280 Ontario law firms. Although the Treefort platform is used by regulated entities across Canada to satisfy their KYC and AML requirements, our current focus is providing our digital ID verification platform to entities in the Ontario real estate sector.

Introduction

Treefort welcomes the opportunity to provide feedback to the Financial Services Regulatory Authority of Ontario ("FSRAO") on its Proposed Guidance: Detecting and Preventing Mortgage Fraud ("Guidance"). To summarize, we believe the Guidance can be improved by including:

1) a requirement that Multi-Factor Authentication be used in all scenarios;
2) specific commentary and advice on the ID verification technologies that FSRAO licensees ("Licensees") can use to satisfy the enhanced ID verification requirements contained in the Guidance;
3) a reminder that in addition to satisfying the enhanced client ID requirements, Licensees must also search sanction and politically exposed persons' lists; and,
4) a requirement that Licensees undergo mandatory training on the enhanced client ID Rules.

Treefort's response to the Proposed Guidance: Detecting and Preventing Mortgage Fraud

Recommendations:

As a result of our experience, including our experience in the legal sector, we have four recommendations for amendments to the Guidance.

Recommendation #1: Require MFAs in all scenarios

We are very pleased to see the reference to "multi-factor authentication" in the Guidance. However, we recommend the first bullet under the heading "Verify identification" in Appendix 1 to the Guidance be amended to read as follows:

- Verify identity using multi-factor authentication
    - The minimum requirement is satisfying the Government Issued ID Method, the Credit File Method **and** the Dual Source Method

The reason for this recommendation is that each of these Methods has limitations and using only one of them will not do anything meaningful to identify and prevent fraudulent transactions. With respect to the Government Issued ID Method, in transactions that have gone through our digital ID platform we have seen fake IDs that are so good that no technology on the market, or any human being without special training and extensive experience, can identify as being fake. Because of this, if a Licensee were only to satisfy the Government Issued ID method, which the current wording of the Guidance allows, these fake IDs would not be caught and the Guidance would have absolutely no effect on preventing fraud.

The Credit File Method also has severe limitations. More specifically, information from a credit file held by a Canadian credit bureau is very good at confirming an individual with a specific name, address and date of birth exists, but it does **nothing** to confirm the individual the Licensee is dealing with is that individual. In other words, if the fraudster has obtained another individual's name, address and date of birth, which is very easy to do, they can pass the Credit File Method.

The Dual Source Method is also problematic because of the weakness of the data the reliable sources have. For instance, the data we have collected from the use of our digital ID platform shows about 50% of cell phone plans are either corporate plans or family plans in the name of a family member other than the individual whose identity is being verified. Confirming the individual has an account at a Canadian financial institution provides another example as our data shows about 22% of addresses associated with bank accounts do not match the address on the ID presented by the respective individuals. This is happens because people do not update the address in their banking profile when they move.

The good news is our data confirms that if all three of the ID verification methods are used frauds can be effectively detected and prevented. As a result, if FSRAO wants Licensees to take steps that will actually prevent identity-theft based fraud in real estate transactions, it must require Licensees to use multi-factor authentication to verify the identity of each of their clients and that result can be achieved if the amendment to the Guidance proposed above is implemented. Finally, the technology required to satisfy the requirements of the three client ID

methods simultaneously exists, it is not cost prohibitive (approximately $25.00 plus GST/ID verification) and it can easily be accessed by every Licensee.

Recommendation #2: Provide Specific Guidance on Technologies

To begin, we believe our experience working with law firms in Ontario, members of whom are regulated by the Law Society of Ontario ("LSO"), is informative to this recommendation.

The LSO has requirements for its licensees to verify the identity of their clients if a financial transaction is associated with the retainer. One method is the use of authentic, valid and current government-issued photo ID. In our interaction with LSO licensees, we learned there was a range of understanding about the rules and how to comply. We were asked questions about compliance, and this included questions about technologies to authenticate ID. While the LSO does not endorse or approve commercial products, including our product, the LSO provided some guidance by referring licensees to the Digital Identity Council of Canada's Directory (a link to this Directory is included below).

For licensees who were not familiar or had limited familiarity with the requirements in the LSO Rules, this contributed to confusion and consternation about how to comply. For others, they wanted to make sure they were fully complying with the LSO Rules, but it was apparent from our experience that they did not yet have the time or expertise to determine what technologies they could or should use to ensure compliance. The risk is that the practice of examining original copies of ID in a physical proximity meeting, because that is the only client ID verification method that is understood, impacts the effectiveness of the LSO Rules as an effort to prevent fraud. This is because reviewing an original ID in a physical proximity meeting on its own is a very ineffective way of preventing ID theft-based fraud.

It is our opinion that the following are the learnings that can be gleaned from our experience with LSO licensees:

A) Those who are subject to client ID verification rules want to comply with the rules that govern them;
B) Unfamiliarity with the rules and how they are to be applied can affect and sometimes frustrate compliance;
C) Where compliance with client ID verification rules requires the use of technology, specific guidance on what technologies can be used is crucial, and will assist those who may not have the time or expertise to find, assess and implement technologies; and,
D) Without material and specific guidance on technologies, those who are subject to client ID verification rules risk continuing with practices that can result in the entrenchment of very weak anti-fraud practices and the defeat of fraud prevention initiatives.

Because of these learnings, it is respectfully submitted that the Guidance should be amended to provide specific and meaningful commentary on the types of technologies that Licensees can use to comply with the enhanced client ID requirements. One option we believe FSRAO should consider is attaching a schedule to the Guidance that contains the following sections:

A) Technologies that can be used to satisfy the requirements of the Government Issued ID Method

In this section you should consider either referring licensees to the existing Digital Identity Authentication Council of Canada ("DIACC") Directory (see: https://diacc.ca/2021/05/03/directory-of-products-that-assess-identification-documents-and-verify-identity-version-2-0/) or working with the DIACC to develop a customized list of technologies that FSRAO licensees can use to comply with the improved client ID requirements contained in the Guidance.

B) Technologies that can be used to satisfy the requirements of the Credit File Method

In Canada there are only two Credit Bureaus, and the ID verification tools they offer are:

I. Equifax – AML Assist
II. TransUnion – eBVS and eBVS ID

We recommend that you contact Equifax and TransUnion and work with them to develop the material describing their products for insertion into this schedule. We would be happy to introduce you to the people at each of Equifax and TransUnion that you would need to talk to if that is helpful.

C) Technologies that can be used to satisfy the requirements of the Dual Source Method

In our opinion, the following are the technologies currently available that Licensees can use to satisfy the requirements of the Dual Source Method:

I. The selfie/ID technologies, including those listed in the DIACC Directory;
II. AML Assist;
III. eBVS and eBVS ID;
IV. Enstream (access to telco databases);
V. Flinks and MX (screen scraping services that allow users to verify the individual has an account at a Canadian Financial Institution);
VI. Interac verification service (allows users to verify the individual has an account at a Canadian Financial Institution).

We recommend this section of the Guidance contain descriptions of each of these products, and how they can be accessed.

Finally, another advantage of adding a schedule in this form to the Guidance is that Licensees can refer to it if, and when, the FINTRAC regulations are amended to add mortgage brokers as Reporting Entities as these three methods are the methods the FINTRAC regulations require Reporting Entities to use.

If FSRAO does not have the time or expertise to review and assess the various technologies that would be listed in the schedule we recommend that FSRAO consider collaborating with the DIACC to review and assess the digital ID technologies and produce the content for the proposed schedule that would be attached to the Guidance. If it would be helpful, we can introduce you to the people at DIACC you would need to talk to about this.

Finally, this schedule would need to be updated at least annually.

Recommendation #3: Add commentary on Sanction and PEP list searches

The requirement to search Sanction and PEP lists is also an important anti-fraud/AML step and, because of that, we recommend the Guidance be amended to include commentary on the importance of conducting these searches. Further, we recommend that FSRAO include a schedule to the Guidance that lists the products Licensees can use to conduct these searches. If it would be helpful, we can assist FSRAO with the list of products.

Recommendation #4: Require licensees to undergo training on the improved Client ID Rules

To ensure compliance with the enhanced Client ID Rules contained in the Guidance, we recommend FSRAO consider requiring Licensees to attend mandatory training on those Rules. Based on our experience in the legal sector, we believe knowledge and understanding of the Client ID Rules is essential to ensure Licensees comply with those Rules. To reduce cost and friction, FSRAO could prepare video tutorials that Licensees are required to watch within a specified time frame. It has been our experience that this training format is very effective.

Sincerely,

Jay Krushell

Jay Krushell, CLO Treefort Technologies Incorporated
jkrushell@treeforttech.com
780-983-5941