State of Wisconsin
Department of Financial Institutions

Tony Evers, **Governor** Kathy Blumenfeld, **Secretary**

November 4, 2020

Remote Online Notarization: Guidance on Identity Proofing

The Remote Notary Council and this Department are jointly tasked with developing standards for remote online notarial acts performed by notaries public of this state, including standards relating to confirming the identity of the remotely located individual.[1] Wisconsin law provides three permissible means for the notary to verify the individual's identity:

(1) Personal knowledge of the identity of the individual, if the individual is personally known to the notary through dealings sufficient to provide reasonable certainty that the individual has the identity claimed[2];
(2) Satisfactory evidence of the identity of the remotely located individual by oath or affirmation from a credible witness appearing before the notary whose identity is verified under methods (1) or (3)[3]; OR
(3) Satisfactory evidence of the identity of the remotely located individual by using at least two different types of "identity proofing"—that is, a process or service by which a third party provides the notary with a means of identity verification by a review of personal information from public or private data sources.[4]

This guidance addresses the standards for the third method of identity verification (identity proofing).

In adopting standards for identity proofing and other elements of remote online notarization, the Council and the Department must "keep the standards and practices of notaries public in this state in harmony with the standards and practices of notaries public in other jurisdictions," so long as they are consistent with the purposes, policies, and provisions of Wisconsin law.[5]

The Mortgage Industry Standards Maintenance Organization (MISMO) is a national standards-setting organization for the mortgage industry. In 2019 it released detailed standards for remote online notarization, including identity proofing, that have proven influential in the industry and have been referenced in model legislation that is substantially similar to Wisconsin law. The Council and the Department have determined MISMO's standards for identity proofing are consistent with the purposes, policies, and provisions of Wisconsin law. Therefore, subject

[1] Wis. Stat. §§ 140.145(8, 11).
[2] Wis. Stat. §§ 140.145(3)(a)1, 140.07(1).
[3] Wis. Stat. §§ 140.145(3)(a)2, 140.07(2).
[4] Wis. Stat. §§ 140.145(3)(a)2, 140.145(1)(c).
[5] Wis. Stat. §§ 140.145(11)(b), 140.145(9).

Division of Banking
Mail: PO Box 7876 Madison, WI 53707-7876
Courier: 4822 Madison Yards Way, Madison, WI 53705
Voice: (608) 261-7578 Fax: (608) 267-6889 Web: www.wdfi.org

to one exception described in the footnote below,[6] the Council and the Department intend to apply those MISMO standards when evaluating whether a proposed process of identity proofing is sufficient to produce satisfactory evidence of the identity of the remotely located individual.

That said, the Council and the Department recognize that remote online notarization (and the technologies that enable it) continue to evolve. The Council and the Department are willing to consider approving other mechanisms for identity proofing that are not specified in the MISMO standards below, so long as those alternative mechanisms are reliable and secure. Comments on these standards, including requests to consider alternative means of identity proofing, should be sent to DFINotary@wisconsin.gov.

The applicable MISMO standards for identity proofing are as follows[7]:

CREDENTIAL ANALYSIS AND AUTHENTICATION

The following authentication and analysis protocols are intended to support the notary public (Notary) in making the determination that satisfactory evidence of each Principal's identity has been established for a Remote Online Notarization.

a. **Principal identity verification for Remote Online Notarization services must include consistent Multi-Factor Authentication procedures**:
    i. Each Principal's identity credential must be verified against trusted third-party data sources;
    ii. Each Principal's identity must be bound to each individual Principal following successful Knowledge-Based Authentication, or another form of authentication or trusted third-party identity verification such as online banking authentication; and
    iii. Procedures must provide for human visual comparison between the Principal's identity credential presented to the Notary and the Principal himself or herself.
b. **Credential Analysis of Government Issued Identification**
    Remote Online Notarization service providers must use automated software processes to aid the Notary with their role in verifying each Principal's identity.
    i. The credential must pass an authenticity test, consistent with sound commercial practices that:
        1. Use appropriate technologies to confirm the integrity of visual, physical or cryptographic security features;
        2. Use appropriate technologies to confirm that the credential is not fraudulent or inappropriately modified;

[6] The MISMO standards anticipate, but do not give direct guidance on, technologies that would enable identity proofing by biometric means (such as face, voice, or fingerprint recognition). While the Council and the Department will continue to monitor technological developments in this emerging field, at this time they believe additional experience, evidence, and safeguards are needed before they can authorize the use of biometrics as a means of identity proofing. Therefore, that paragraph of the MISMO standards has been removed from the quoted section below.

[7] Non-substantive footnotes appearing in MISMO's text are omitted herein.

3. Use information held or published by the issuing source or authoritative source(s), as available, to confirm the validity of credential details; and
4. Provide the output of the authenticity test to the Notary.[8]

ii. The credential analysis procedure must enable the Notary to visually compare both of the following for consistency:
   1. The information and photo on the presented credential image; and
   2. The Principal as viewed by the Notary in real time through the audio/video system.

iii. Credential Type Requirements
   1. Must be a government-issued document meeting the requirements of the State that contains a photograph of the individual, may be imaged, photographed and video recorded under applicable state and federal law, and can be subjected to credential analysis.

iv. Credential Image Capture
   1. The credential image capture procedure must confirm that:
      a. The Principal is in possession of the credential at the time of the Notarial Act;
      b. Credential images submitted for credential analysis have not been manipulated; and
      c. Credential images match the credential in the Principal's possession.
   2. The following general principles should be considered in the context of image resolution:
      a. Captured image resolution should be sufficient for the service provider to perform credential analysis per the requirements above.
      b. Image resolution should be sufficient to enable visual inspection by the Notary, including legible text and clarity of photographs, barcodes, and other credential features.
      c. All images necessary to perform visual inspection and credential analysis must be captured—e.g., U.S. Passport requires identity page, state driver's licenses require front and back.

c. Dynamic Knowledge-Based Authentication

Dynamic Knowledge-Based Authentication (KBA) is an identity assessment that is based on a set of questions formulated from public or private data sources. A Dynamic Knowledge-Based Authentication procedure must meet the following requirements:

i. Each Principal must answer questions and achieve a passing score.
   1. MISMO recommends:
      a. Five questions drawn from public or private data sources.
      b. A minimum of five possible answer choices per question.
      c. At least four of the five questions answer correctly (a passing score of 80%).

[8] The output may simply indicate a "pass" or "fail" type score, or may provide more information to indicate the outcome of the authenticity test to the Notary.

d. All five questions answered within two minutes.

ii. Each Principal to be provided a reasonable number of attempts per Signing Session.
    1. MISMO recommends:
        a. If a Principal fails their first quiz, they may attempt up to two additional quizzes within 48 hours from the first failure.
        b. During any quiz retake, a minimum of 40% (two) of the prior questions must be replaced.

iii. The Remote Online Notarization system provider must not include the KBA procedure as part of the video recording or as part of the system-provided person-to-person video interaction between the Notary and the Signatory, and must not store the data or information presented in the KBA questions and answers. However, the output of the KBA assessment procedure must be provided to the Notary.[9]

d. Workflow Continuity Requirement

If a principal must exit the workflow, they must meet the criteria outlined in this section and restart the Credential Analysis and Authentication workflow from the beginning.

.

[9] The output may simply indicate a "pass" or "fail" type score, and/or may provide more information to indicate the outcome of the KBA assessment to the Notary.