721—43.9(9B) Standards for communication technology and identity proofing for notarial acts performed for remotely located individuals.

43.9(1) A notary public may not perform a notarial act for a remotely located individual unless the technology identified by the notary public pursuant to Iowa Code section 9B.14A(7) satisfies all of the following:

a. Has been approved by the secretary of state in accordance with this chapter.

b. Provides continuous, synchronous audiovisual feeds.

c. Provides sufficient video resolution and audio clarity to enable the notary public and remotely located individual to see and speak with each other simultaneously through live, real-time transmission.

d. Provides sufficient captured image resolution for identity proofing performed in accordance with Iowa Code section 9B.14A(3).

e. Provides a means of authentication that reasonably ensures only authorized parties have access to the audiovisual record of the performed notarial act.

f. Provides for the recording of the electronic notarial act in compliance with this chapter and Iowa Code section 9B.14A in sufficient quality to ensure the verification of the electronic notarial act.

g. Ensures that any change to or tampering with an electronic record before or after the electronic notarial seal has been affixed and the electronic notarial act has been completed is evident.

h. Provides confirmation that the electronic record presented is the same electronic record notarized.

i. Provides a means of electronically affixing the notary's official stamp to the notarized document.

j. Provides an electronic notary journal that complies with the provisions of this chapter to document the electronic notarial acts.

k. Provides security measures the secretary of state deems reasonable to prevent unauthorized access to all of the following:

(1) The live transmission of the audiovisual communication.

(2) A recording of the audiovisual communication.

(3) The verification methods and credentials used in the identity proofing procedure.

(4) The electronic records presented for online notarization.

(5) Any personally identifiable information used in the identity proofing or credential analysis.

43.9(2) Identity proofing and credential analysis must be performed by a third-party credential service provider whose methods and standards are substantially similar to those defined in the most recent edition of the National Institute of Standards and Technology's Digital Identity Guidelines, and that has provided evidence to the notary public of the ability to satisfy the following requirements:

a. Identity proofing is performed through dynamic knowledge-based authentication which meets the following requirements:

(1) Principal must answer a quiz consisting of a minimum of five questions related to the principal's personal history or identity, formulated from public and proprietary data sources;

(2) Each question must have a minimum of five possible answer choices;

(3) At least 80 percent of the questions must be answered correctly;

(4) All questions must be answered within two minutes;

(5) If the principal fails the first attempt, the principal may retake the quiz one time within 24 hours;

(6) During the retake, a minimum of 60 percent of the prior questions must be replaced;

(7) A principal who fails the second attempt is not permitted to retry with the same notary public for 24 hours; and

(8) A principal who fails the third attempt is not permitted to make any further attempts.

b. Credential analysis is performed utilizing public and proprietary data sources to verify the credential presented by the principal.

c. Credential analysis shall, at a minimum, do all of the following:

(1) Use automated software processes to aid the notary public in verifying the identity of a principal or any credible witness.

(2) Ensure that the credential passes an authenticity test, substantially similar to those defined in the most recent edition of the National Institute of Standards and Technology's Digital Identity Guidelines, that:

1. Uses appropriate technology to confirm the integrity of visual, physical, or cryptographic security features;

2. Uses appropriate technology to confirm that the credential is not fraudulent or inappropriately modified;

3. Uses information held or published by the issuing source or authoritative source(s), as available, to confirm the validity of personal details and credential details; and

4. Provides output of the authenticity test to the notary public.

(3) Enable the notary public to visually compare the following for consistency: the information and photo, if the credential presented contains a photo, presented on the credential itself and the principal as viewed by the notary public in real time through audiovisual transmission.

d. If the principal must exit the workflow, the principal must meet the criteria outlined in this rule and must restart the identity proofing and credential analysis from the beginning.

43.9(3) Upon change of any of the technology identified by the notary public pursuant to Iowa Code section 9B.14A(7) which affects compliance with the requirements of Iowa Code chapter 9B or this chapter, the provider of the technology shall immediately notify the secretary of state and all Iowa notaries public using its technology of the change. Information that qualifies as trade secret under Iowa law shall be kept confidential in accordance with Iowa Code section 22.7(3). It is the responsibility of the provider to specify to the secretary of state the information it believes falls within the definition of "trade secret" under Iowa Code section 550.2(4) and other applicable law.

[**ARC 5041C**, IAB 5/20/20, effective 7/1/20; **ARC 7059C**, IAB 8/23/23, effective 9/27/23]