**Section 176.835 Standards for Identity Verification**

a) If an electronic notary public does not have satisfactory evidence of the identity of a remotely located principal pursuant to 5 ILCS 312/6A-103(b)(1), the electronic notary public must reasonably verify the principal’s identity through a multi-factor authentication procedure as provided in this Section. The procedure must analyze the principal’s identification credential presented remotely against trusted third-person data sources, bind the principal’s identity following a successful dynamic knowledge-based authentication assessment, and permit the electronic notary public to visually compare the identification credential and the principal. Credential analysis and identity proofing must be performed by a reputable third party who has provided evidence to the electronic notary public of the ability to comply with this Section.

b) Credential analysis must use public or private data sources to confirm the validity of the identification credential presented electronically by a principal and will, at a minimum:

1) Use automated software processes to aid the electronic notary public in verifying the identity of each principal;

2) Require the identification credential to pass an authenticity test, consistent with sound commercial practices, that uses appropriate technologies to confirm the integrity of visual, physical, or cryptographic security features and to confirm that the identification credential is not fraudulent or inappropriately modified;

3) Use information held or published by the issuing source or an authoritative source, as available and consistent with sound commercial practices, to confirm the validity of personal details and identification credentials; and

4) Enable the electronic notary public to visually compare for consistency the information and photograph on the identification credential and the principal as viewed by the electronic notary public in real time through communication technology.

c) Identity proofing must be performed using a dynamic knowledge-based authentication assessment. The assessment is successful if it meets the following requirements:

1) The principal must answer a quiz consisting of a minimum of five questions related to the principal’s personal history or identity formulated from public or private data sources;

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

3) At least 80% 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 a retake of the quiz, a minimum of 40% of the prior questions must be replaced;

7) If the principal fails the second attempt, the principal is not allowed to retry with the same electronic notary public within 24 hours of the second failed attempt; and

8) The electronic notary public must not be able to see or record the questions or answers.

d) An electronic notary public has satisfactory evidence of the identity of the principal if:

1) The electronic notary public has personal knowledge of the identity of the principal; or

2) The requirements of 5 ILCS 312/6A-103(b)(2) are satisfied.

(Source: Added at 47 Ill. Reg. 8640, effective June 5, 2023)