

111:6-1-05

Requirements for online notarial acts.

- (A) An online notary public must be physically located within the boundaries of Ohio at the time the notarial act takes place; however, the signer may be located anywhere within the territory of the United States or outside the United States only if the conditions set forth in division (C)(2) of section 147.64 of the Revised Code are met.
- (B) Online notarizations must occur with the use of an online notarization system, which has two-way live audio and video conference technology, and that meets the following requirements:
- (1) The online notary public must be able to verify the identity of the remotely located individual at the time the signature is taken by one of the following methods:
 - (a) The online notary public's personal knowledge of the individual;
 - (b) Each of the following:
 - (i) Remote presentation of an unexpired government-issued identification credential that contains the photograph and signature of the individual to the online notary public by means of communication technology;
 - (ii) Credential analysis of the identification credential in accordance with paragraph (B)(4) of this rule; and
 - (iii) Identity proofing of the individual in accordance with paragraph (B)(5) of this rule.
 - (c) Oath or affirmation of a single credible witness who personally knows the individual and either is personally known to the online notary public or who is identified by the online notary public under paragraph (B)(1)(b) of this rule.
 - (2) A credible witness under paragraph (B)(1)(c) of this rule may appear before the online notary public by means of communication technology that complies with Chapter 147. of the Revised Code and this chapter.
 - (3) Credential analysis and identity proofing must be performed by a reputable third person who has provided reasonable evidence to the online notary public of the person's ability to satisfy the requirements of Chapter 147. of the Revised Code and this rule.
 - (4) Credential analysis must utilize public or private data sources to confirm the validity of an identification credential and must, at a minimum:

- (a) Use automated software processes to aid the online notary public in verifying the identity of a remotely located individual;
- (b) Ensure that the identification credential passes an authenticity test, consistent with sound commercial practices that:
 - (i) Use appropriate technologies to confirm the integrity of visual, physical, or cryptographic security features;
 - (ii) Use appropriate technologies to confirm that the identification credential is not fraudulent or inappropriately modified;
 - (iii) Use information held or published by the issuing source or an authoritative source, as available, to confirm the validity of identification credential details; and
 - (iv) Provide output of the authenticity test to the online notary public;
- (c) Enable the online notary public to visually compare for consistency:
 - (i) The information and photograph on the presented credential, and
 - (ii) The remotely located individual as viewed by the online notary public in real time through communication technology;
- (d) Require a government-issued identification credential that:
 - (i) Is an unexpired government-issued identification credential that contains the photograph and signature of the individual; and
 - (ii) May be imaged, photographed, and video recorded under applicable state and federal law; and
 - (iii) Can be subjected to credential analysis.
- (e) Include an image capture procedure that confirms that:
 - (i) The remotely located individual is in possession of the credential at the time of the notarial act;
 - (ii) Credential images submitted for credential analysis have not been manipulated; and
 - (iii) Credential images match the credential in the possession of the remotely located individual; and

- (f) Require the captured image of the identification credential to:
 - (i) Be of sufficient image resolution to perform credential analysis in accordance with the requirements of this paragraph;
 - (ii) Be of sufficient image resolution to enable visual inspection of the credential by the notary public; and
 - (iii) Include all images necessary to perform visual inspection and credential analysis in accordance with the requirements of this paragraph, including the identity page of any passport and the front and back images of any identification card.
- (5) Identity proofing shall be performed by means of ~~a dynamic knowledge-based authentication or through another process approved by the secretary of state. that meets the following requirements~~The dynamic knowledge based authentication must, at a minimum, meet the following requirements:
 - (a) Each remotely located individual must answer at a ~~quiz consisting of a~~ minimum ~~of~~ five questions related to the remotely located individual's personal history or identity, formulated from public or private data sources;
 - (b) Each question must have a minimum of five possible answer choices;
 - (c) At least eighty per cent of the questions must be answered correctly;
 - (d) All questions must be answered within two minutes;
 - (e) If the remotely located individual fails the first attempt, the individual may retake the quiz two times within forty-eight hours;
 - (f) During a retake of the quiz, a minimum of forty per cent of the prior questions must be replaced;
 - (g) If the remotely located individual fails the second attempt, the individual is not permitted to retry with the same notary or the same third person providing the identity proofing service within twenty-four hours of the second failed attempt; and
 - (h) The online notary public must not be able to see or record the questions or answers.
- (6) The online notarization system used must meet the following criteria:

- (a) The persons communicating must simultaneously see and speak to one another.
 - (b) The signal transmission must be live, real time audio-visual feeds.
 - (c) The signal transmission must be secure from interception or access by anyone other than the persons communicating.
 - (d) The technology must provide sufficient audio clarity and video resolution to enable the notary to communicate with the signer and utilize the permissible signer identification methods.
 - (e) The system must provide confirmation that the electronic document presented is the same as the electronic document notarized.
 - (f) Allow for the affixation of the notarial certificate, signature and seal.
 - (g) Allow for viewing the notarial certificate, signature and seal.
 - (h) Provide a method for determining if the electronic document has been altered after the electronic notarial seal has been affixed and the electronic notarial act has been completed.
 - (i) Provide a method of generating a paper copy of the document including the notarial certificate, signature and seal and any other document associated with the execution of the notarial act.
- (C) If the signer or online notary public must exit the audio-video communication session, the audio-video communication link is broken, or the resolution or quality of the transmission becomes such that the electronic notary public believes the process has been compromised and cannot be completed, the identity authentication process and any incomplete online notarial acts must be started from the beginning.
- (D) The online notary public shall refuse to perform an online notarization if:
- (1) The online notary public is unable to verify the identity of the principal;
 - (2) The online notary public is unable to verify the security of the two way audio visual transmission;
 - (3) The signature of the principal cannot be attached to the electronic document; or
 - (4) The online notarization system or technology cannot render the notarial act tamper-evident.

Effective:

Five Year Review (FYR) Dates: 3/21/2025

Certification

Date

Promulgated Under: 119.03
Statutory Authority: 147.62.
Rule Amplifies: 147.62, 147.64, 147.65.
Prior Effective Dates: 09/22/2019