Digitally Disguised:

Deepfakes and Remote Notarial Acts

NATIONAL NOTARY ASSOCIATION

CONTENTS

INTRODUCTION

Deepfakes are computer-generated synthetic media created to replace one person's physical likeness and voice with a highly realistic and convincing impersonation of another individual. Most commonly used in video formats, both recorded and live streaming, they portray something that did not actually occur in reality, often for malevolent ends.

Impersonation has always been a threat to the integrity of notarial acts. Bad actors — in the physical presence of a Notary Public — have assumed the identities of signers of documents to fraudulently convey property, rob estates, usurp authority over the elderly, and commit other crimes.

This paper will address the threat deepfakes pose to the integrity of notarial acts that are performed in the *remote* presence of a Notary Public and what may be done to counter this risk.[1]

DEEPFAKE REMOTE NOTARIZATION ATTACK VECTORS

The term "deepfake" is made up of the words *deep*, as in "deep learning,"[2] and *fake*. According to Britannica, the term originated in 2017 when a Reddit moderator created a subreddit named "deepfakes."[3] It has been around just long enough for the major dictionaries to define the term. Oxford defines a deepfake as "Any of various media, esp. a video, that has been digitally manipulated to replace one person's likeness convincingly with that of another, often used maliciously to show someone doing something that he or she did not do."[4]

At the same time deepfakes were gaining attention, state legislatures were enacting new laws authorizing a Notary Public and remotely located individual to meet on an online "platform" that provides the technology in real time for both to hear and see each other and for an electronic record to be presented for signature and notarization. To date, forty-seven states and the District of Columbia have enacted such "remote" notarial act statutes.

---

[1] The term "remote presence" is not generally used or defined in state remote notarial act laws, but a close synonym, "electronic presence" is defined as "the relationship of two or more individuals in different locations communicating in real time to the same extent as if the individuals were physically present in the same location" (Uniform Law Commission, Uniform Electronic Wills Act, 2021, Section 2(2)).

[2] "Deep Learning." *Wikipedia*. https://en.wikipedia.org/wiki/Deep_learning. Last viewed on June 20, 2024.

[3] "Deepfake." *Brittanica*. https://www.britannica.com/technology/deepfake. Last viewed on June 20, 2024.

[4] "Deepfake." *Oxford Online English Dictionary*. https://www.oed.com/search/dictionary/?scope=Entries&q=deepfake. Last viewed on June 20, 2024.

Deepfake fraud can plausibly be committed using remote notarization under the same circumstances as fraudulent paper notarial acts, including:

- Committing real property seller impersonation deed fraud.[5]
- Posing as a vindictive spouse in a refinance or second mortgage transaction.
- Modifying a family trust with terms that are more favorable to a disgruntled heir.
- Executing a power of attorney to gain control of an elderly person's financial affairs.

Like any notarial act, to perpetrate these and other impersonations the remotely located individual must prove their identity to a Notary Public. Under the laws of virtually every state, a Notary may identify a remotely located individual by personal knowledge if the Notary and individual have had sufficient interactions for the Notary to be reasonably certain the individual is who they claim to be.[6]

When a Notary's personal knowledge of a remotely located individual is not the basis for establishing the individual's identity, multiple identity proofing methods — the most common of which are "credential analysis" and "dynamic knowledge-based authentication" (DKBA) — must be used.

In credential analysis, the remotely located individual takes photographs of the front and back of the individual's driver's license or passport at the time of the remote notarial act and uploads them onto the platform.[7] The platform then sends the scans to a third-party identity service provider for an analysis of the credential's authenticity.[8]

Dynamic knowledge-based authentication involves an identity service provider posing highly granular questions[9] related to the remotely located individual's life and credit history culled from public or private data sources.[10]

These identity proofing methods are formidable obstacles to pulling off a deepfake impersonation because the bad actor must have a valid credential that can pass credential analysis and intimate knowledge of the victim's entire life history to correctly answer the dynamic knowledge-based authentication questions.[11]

---

[5] See "Seller Impersonation Fraud in Real Estate." *American Land Title Association*. https://www.alta.org/file/ALTA-Seller-Impersonation-Handout. Last viewed on June 20, 2024.

[6] See, e.g., Ariz. Rev. Stat. Ann. § 41-263.B.1(a); 5 ILCS 312/6A-103(b)(1); Ky. Rev. Stat. Ann. § 423.325(3)(a); Mass. Gen. Laws Ann. ch. 222, § 28(a)(i)(A); Ohio Rev. Code § 147.64(E)(1); R.I. Gen. Laws Ann. § 42-30.1-12.1(b)(1)(i). However, the state of California's remote notarial act statute (Cal. Gov't Code § 8231.8(a)(1) (oper. January 1, 2030)) does not permit a Notary Public to identify a remotely located individual based on personal knowledge.

[7] See, e.g., Ohio Rev. Code § 147.60(B); Tenn. Code Ann. § 8-16-302(2).

[8] See, e.g., Kan. Admin. R. § 7-43-18(a)(1).

[9] Examples of questions could be, "Which of the following was your mortgage balance at the end of last month?" and "Which of the following addresses is not associated with you?" (Both present five potential answers).

[10] See, e.g., Ind. Code Ann. § 33-42-0.5-9; La. Admin. Code 46:XLVI.144.C.1.

[11] Most state laws require four out of five DKBA questions to be answered correctly within a time limit of two minutes.

There is another way a remotely located individual can be identified to the Notary Public under the laws of most states. A credible witness who is personally known to the remotely located individual may swear an oath or affirmation to the Notary that the witness knows the individual. This witness may be identified to the Notary through the Notary's personal knowledge of the witness, or if the witness is unknown to the Notary, through multiple means of identity proofing.[12]

Given these methods of proving identity to a Notary Public for a remote notarial act, the most vulnerable to attack by deepfake impersonators are:

- Creating a deepfake of a remotely located individual who is personally known to the Notary Public.
- Creating a deepfake of a credible witness who is personally known to the Notary Public.
- Creating a deepfake of a remotely located individual, stealing the victim's written identification or presenting a compelling fake identification card to pass credential analysis,[13] and attempting to correctly answer the DKBA questions.[14]

Success under any of these scenarios will require the illicit actor to create a convincing deepfake that looks and sounds like the targeted victim.

CAN A DEEPFAKE MOUNT A SUCCESSFUL IMPERSONATION?

To successfully deploy a deepfake to impersonate an individual in a remote notarial act, the perpetrator must clear several hurdles. Each will be discussed below.

Create a Deepfake Avatar. The first hurdle for the impostor is to create a highly realistic avatar of the victim. Early deepfake videos crudely resembled the subjects they were trying to recreate and exhibited emotionless expressions, unrealistic body movements, and poor lip syncing that betrayed them as "cheapfakes." However, a deepfake video of Morgan Freeman posted by Dutch YouTube channel Diep Nep in July 2021 demonstrated how quickly technology had improved on these deficiencies.[15]

---

[12] See, e.g., Kan. Admin. R. § 7-43-18(b); Md. Code Ann. (St. Gov't) § 18-214(a)(1)(ii); Mont. Code Ann. § 1-5-603(12)(b)(ii); Utah Code Ann. § 46-1-2(20)(a)(i)(C); Wis. Stat. Ann. § 140.145(3)(a)2. But see Cal. Gov't Code § 8231.8(a)(1), (2) (oper. January 1, 2030) and Mo. Rev. Stat. Ann. § 486.1145. Both do not allow credible witnesses to identify remotely located individuals.

[13] One way to create a compelling false ID is through "face morphing" where the photographs of two individuals are combined to create a third photo containing the physical characteristics of each. Since, for example, U.S. passports are created with photos individuals submit with a passport application, a valid U.S. passport could be created with the morphed photo, allowing both individuals to use the passport. Face-morphed photos have been shown to pass through face detection scanners and human detection checkpoints. See "Video injection attacks on remote digital identity verification solution using face recognition" (Kévin Carta et al. Submitted to the 13th International Multi-Conference on Complexity, Informatics and Cybernetics, 2022) at 94 and "Real vs Fake Faces: DeepFakes and Face Morphing" (Jacob L. Dameron, Graduate Theses, Dissertations, and Problem Reports, West Virginia University, 2021) at 24.

[14] Since many frauds involving notarized records involve close family members, a vindictive spouse or sibling who is off camera could attempt to answer the KBA questions with the personal information known about the victim.

[15] De Jong, Bob. "This is not Morgan Freeman - A Deepfake Singularity." *YouTube*. https://www.youtube.com/watch?v=oxXpB9pSETo. Last viewed on June 20, 2024.

Creating a realistic and lifelike avatar for a remote notarial act session is much more difficult than producing a believable pre-recorded video like the Freeman deepfake. The goal is to "skin" the threat actor with the victim's features so that the actor-as-avatar can naturally interact with the Notary in real time just as if the victim was appearing before the Notary.[16]

Technology is quickly evolving to the point of being able to do this.[17] Recently a financier in Hong Kong who attended an online meeting with individuals he knew as his company's chief financial officer and other members of his staff was duped into paying out $25 million to deepfake impersonators.[18]

The ability to make a lifelike avatar of almost anyone is eminently doable if targeted victims have posted photos and videos of themselves on Instagram, Facebook, TikTok, YouTube, or other social media platforms.

Voice Clone the Victim. The next hurdle, which may well be the easiest to surmount, is to clone the victim's voice so that the impersonator sounds like the victim.

The technology to clone a human voice is so effective that it has been successfully used in phone money scams and to pass bank voice identification checks.[19] So realistic are audio deepfakes that the U.S. Federal Trade Commission recently awarded cash prizes to four organizations that developed technologies to distinguish between authentic human speech and audio deepfakes produced by artificial intelligence.[20]

Launch a Video Injection Attack. This next hurdle is more difficult. The impostor could masquerade as the victim to the Notary on camera, but more likely the impostor will attempt to fraudulently insert the live video and audio of a victim's avatar into a remote notarial act session using what is known as a video injection attack. In a video injection attack, the impostor presents the synthetically made avatar to the Notary as if it were a real person.

---

[16] Brown, Tim. "Video Injection Attacks: What Are They and Are We Ignoring the Simple Solution?" *Prove.com*. https://www.prove.com/blog/video-injection-attacks-what-are-they-and-are-we-ignoring-the-simple-solution. Last viewed on June 20, 2024.

[17] On April 16, 2024, Microsoft Research Asia announced its Visual Affective Skills Animator" (VASA-1) that now can create a realistic avatar of an individual with a single photo and audio clip, paving the way for "real-time engagements with lifelike avatars that emulate human conversational behaviors" (https://www.microsoft.com/en-us/research/project/vasa-1), last viewed on April 25, 2024. Microsoft clarifies that its research focuses on positive applications of its technology, not malicious ones, and that it has no plans to release VASA-1 publicly until it is certain the technology will be used responsibly and in accordance with the law.

[18] Chen, Heather and Magramo, Kathleen. "Finance worker pays out $25 million after video call with deepfake 'chief financial officer.'" *CNN*, February 4, 2024. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html. Last viewed on June 20, 2024..

[19] Stupp, Catherine. "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case." *Wall Street Journal*, August 30, 2019. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402. Last Viewed on June 20, 2024; and Stern, Joanna. "I Challenged My AI Clone to Replace Me for 24 Hours." *Wall Street Journal*, April 28, 2023. https://www.wsj.com/video/series/joanna-stern-personal-technology/24-hour-challenge-can-my-ai-voice-and-video-clone-replace-me/EC817295-03D0-4031-B40B-694D7BDE2797. Last viewed on June 20, 2024. OpenAI recently announced Voice Engine, its voice cloning tool, that can make natural-sounding speech that closely resembles the original speaker using text input and as little as a 15-second audio clip. See "Navigating the Challenges and Opportunities of Synthetic Voices." *OpenAI.com*, March 29, 2024. https://openai.com/blog/navigating-the-challenges-and-opportunities-of-synthetic-voices. Last viewed on June 20, 2024. OpenAI chose to preview but not widely release Voice Engine until society can better understand and guard against the challenges of voice cloning.

[20] Jingnan, Huo. "The government announced winners of a contest to tell real voices from deepfake audio." *National Public Radio*, April 10, 2024. https://www.npr.org/2024/04/10/1243772203/deepfake-audio-testing-contest-winners. Last viewed on June 20, 2024.

There are several ways to do this.[21] Instead of a computer's hardware camera broadcasting a real person into the remote notarial act session, software can create a "virtual" camera that bypasses the hardware camera altogether and allows the illicit actor to present the victim's lifelike avatar to the Notary. A more difficult method is to hack the device used by the actual victim. Several French researchers did just that to gain control of two Samsung Galaxy smartphones and inject a video stream of a deepfake into a mobile application, showing that this type of identity fraud is more fact than fiction.[22]

The tools for the average person to mount a video injection attack are available for purchase on the dark web. Recently, one criminal posted a video of his injection attack to swindle an unsuspecting victim out of money in a romance scam.[23]

Bypass Liveness Detection. Many platforms will initiate a "liveness detection" test to mitigate deepfake threats. Liveness detection seeks to determine if the subject presenting to the camera in a remote notarial act is a live person.[24] Liveness can be tested through active and passive means. An example of an active liveness test is to ask the subject at the other end of the camera to move their head up or down or from side to side, or to blink or smile. An example of a passive test is to stimulate the subject's pupils without announcing it to the subject and then look for changes in pupil size which is the expected result if the subject is alive.[25]

Liveness tests initiated by remote notarial act platforms typically analyze a "selfie" photograph that the remotely located individual takes and uploads onto the platform at the time of the remote notarial act. An algorithm determines the minimum threshold of liveness and applies the test to the selfie. Like all active liveness tests, the weakness of this voluntary test is that it announces to the imposter that a check is imminent (direction to upload a selfie), giving the impostor time to work around the "pop" quiz. Passive checks are unannounced and do not afford this luxury.

---

[21] Simonchik, Konstantin. "Video injection attacks: What is that and the way forward?" *Biometric Update*, May 2, 2024. https://www.biometricupdate.com/202405/video-injection-attacks-what-is-that-and-the-way-forward. Last viewed on June 20, 2024.

[22] See "Video injection attacks on remote digital identity verification solution using face recognition" (Kévin Carta et al., Proceedings of the 13th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC) 2022).

[23] See LinkedIn blog post by Maimon, David. *LinkedIn*. https://www.linkedin.com/posts/david-maimon-29343632_bankaccounts-bankaccount-passport-activity-7058789150484828160-ld1J/?trk=public_profile_like_view. Last viewed on June 20, 2024.

[24] See "Information technology — Biometric presentation attack detection — Part 1; Framework," (International Standards Organization/International Electrotechnical Commission Standard 30107-1, first edition, 2016-01-15) at 2, 6.

[25] Id.

COUNTERING THE DEEPFAKE THREAT

At the time of publication, the National Notary Association was not aware of any deepfake impersonation schemes being attempted in an actual remote notarial act. But the technology is maturing quickly, the tools are available, and the threat is real. The NNA believes the Notary community and policymakers must quickly adopt solutions for warding off these attacks before they undermine the public's faith in the office of Notary Public and the integrity of remote notarial acts. We will discuss four potential solutions below.

Personal Knowledge. The urgency to address the deepfake threat could lead state legislatures to repeal existing laws authorizing a Notary Public to use personal knowledge as the basis for verifying the identity of remotely located individuals and credible witnesses.[26] No doubt it would be extremely difficult for a deepfake actor posing as a remotely located individual or credible witness to be identified to the Notary by identity proofing. Furthermore, personal knowledge has become an anachronism. In today's highly mobile society, Notaries Public and individuals for whom notarial services are rendered are more likely than not to be total strangers. This was not the case a hundred years ago when people lived in close-knit communities where everyone knew each other and infrequently traveled outside their hometowns.

Technology. Another way to mitigate the deepfake risk is by fighting fire with fire: Use artificial intelligence to slay the deepfake dragon created by artificial intelligence itself.

The NNA urges platform providers to implement technologies, such as tests to detect liveness, that will make remote notarial acts safer for signing and relying parties. Questions remain, however. Will the detection technology be reliable enough to spot deepfakes? Will operators of platforms choose to adopt, or as needed, adapt the technology — and how quickly? Should society confide more in remote notarial act platforms to ensure the security and integrity of notarial acts than in the Notaries who perform them?

The Notary Public. No matter how effective, any use of technology to detect deepfakes cannot replace the active official witnessing of the Notary Public.[27] Notaries bring great value to documentary transactions by exercising discretion[28] in making various judgments that are critical to the integrity of the notarial act. These include the

---

[26] As noted in footnote 12, California neither authorizes remotely located individuals to be identified based on the Notary Public's personal knowledge nor through the oath or affirmation of a credible witness.

[27] Wakefield, Jane. "Tackling deepfakes 'has turned into an arms race.'" *BBC*, March 26, 2024. https://www.bbc.com/news/business-68549609. Last viewed on June 20, 2024. Yoti, a British ID firm, provides face recognition services. "Back at Yoti, [Yoti employee] Louise Bruder says that no matter how good AI gets at fighting deepfakes, there will always be a need for human checkers like herself."

[28] "We recognize the critical need for a notary's duties to be carried out correctly and with integrity. But a notary's duties, important as they are, hardly implicate responsibilities that go to the heart of representative government. Rather, these duties are essentially clerical and ministerial" (Bernal v. Fainter, 467 U.S. 216). The U.S. Supreme Court's characterization of the duties of Notaries Public as ministerial in the case may have been accurate in 1984 when the Court decided the case, but in recent years, state laws have invested Notaries Public with significantly more responsibility to apply sound judgment, prudence, and discretion in performing notarial acts. The footnotes which follow point to several areas in the law where the Notary's role is anything but "essentially clerical and ministerial."

Notary being satisfied[29] as to the individual's identity,[30] mental capacity,[31] and voluntary signature[32] at the time of the notarial act.

Fortunately, states had foresight to adopt specific provisions in their remote notarial act laws that also require the Notary to exercise discretion. Two such laws can be directly applied to the deepfake threat. In the first, the Notary must take reasonable[33] steps to uphold the security and reliability of remote notarial acts[34] and in the second, the Notary must take reasonable steps to ensure that the audiovisual communication used in remote notarial acts is secure from unauthorized interception.[35] Since the "reasonable steps" are rarely, if ever, enumerated in the law, the Notary must exercise judgment to identify and apply them in each situation.

What are the reasonable steps Notaries can take to detect a deepfake? Notaries should conduct their own passive liveness test without warning the remotely located individual or credible witness that it is coming. This involuntary test would involve observing the person blinking their eyes, smiling, turning their head, and changing their facial expressions — all natural signs of human beings engaging in normal conversation.[36] Notaries also should look for skin features that do not appear to match the age of the person and artificial light reflecting from eyeglasses, and carefully watch lip movements to detect lip syncing irregularities.[37]

Similarly, the Notaries can initiate their own active liveness test. Since most remote notarial act platforms only show the head of the remotely located individual onscreen, the Notary will not be able to observe the remotely located individual's lower body movements without asking. The Notary can ask the person to wave their hands, clap, or shrug their shoulders. While these voluntary actions introduce friction into the notarial process that could be considered overly intrusive, not to mention tip off the impostor, they may indicate signs that the person shown onscreen is not human.[38]

---

[29] When applied to the Notary Public, the term "satisfied" in state law demonstrates that the Notary must use discretion, judgment, and prudence in performing the notarial act.

[30] See, e.g., N.J. Stat. Ann. § 52:7-10.17.a(4); Or. Rev. Stat. § 194.245(1)(c).

[31] See, e.g., Del. Code Ann. tit. 29 § 4322(a)(1); Iowa Code Ann. § 9B.8.1.a; Md. Code Ann. (St. Gov't) § 18-207(1).

[32] See, e.g., N.M. Stat. Ann. § 14-14A-7.A(2); Vt. Stat. Ann. tit. 26, § 5372(a)(2); Wash. Rev. Code Ann. § 42.45.060(1)(b).

[33] The term "reasonable" when applied to the Notary also demonstrate that the Notary must use discretion in performing the notarial act.

[34] See Ark. Code Ann. § 21-14-310(b)(1); Fla. Admin. Code 1N-5.002(2); Ill. Admin. Code § 176.830 a); Minn. Stat. Ann. § 358.645 Subd. 4(c)(1); Nev. Admin. Code § 240.665.1; Okla. Stat. Ann. tit. 49 § 206.C.1.

[35] See Ark. Code Ann. § 21-14-309(c); Haw. Admin. R. § 5-11-71(a)(4); Kan. Admin. R. § 7-43-22(c); Ky. Rev. Stat. Ann. § 423.355(9)(b); La. Rev. St. § 35:628(1); Minn. Stat. Ann. § 358.645 Subd. 7(c); Mont. Code Ann. § 1-5-603(10)(c)(i); Neb. Rev. Stat. § 64-411(3); Nev. Admin. Code § 240.665.4; Tenn. Code Ann. § 8-16-310(b); Okla. Stat. Ann. tit. 49, § 208.A.2; Tex. Gov't Code § 406.110(c).

[36] Recreating natural facial movements and eye blinking are challenges to deepfake creators.

[37] Henley, Jon. "Real-time deepfakes are a dangerous new threat. How to protect yourself." *Los Angeles Times*, May 11, 2023. https://www.latimes.com/business/technology/story/2023-05-11/realtime-ai-deepfakes-how-to-protect-yourself. Last viewed on June 20, 2024.

[38] The absence of or unnatural lower body movements is another sign of a deepfake.

Finally, the Notary can adopt a strategy experts recommend to counter online meeting scams. Individuals meeting online can share a secret keyword among themselves in advance. When the impostor attempts to infiltrate a video meeting, the individual on the other end of the camera can ask the impostor for the keyword. Similarly, the Notary and true person for whom the remote notarial act is being performed could share a secret keyword in advance of the remote notarial act and exchange it at the beginning of the remote notarial session.

The Ultimate Solution. The fail-safe solution to averting the threat of deepfakes in remote notarial acts may be the most radical: Invoke the analog option[39] and insist on meeting physically with the Notary Public instead of by live streaming video.[40]

No doubt this solution proposes regress in the face of progress. It is supported, however, by remote notarial act laws in all forty-seven states and the District of Columbia which unambiguously declare remote notarial acts are permissive, not mandatory. Remote notarial acts are a convenience and choice. A Notary Public is neither obligated nor required to perform remote notarial acts, and neither are people seeking notarial acts obligated to request or use them for their documents. In the face of the deepfake threat and until effective countermeasures are devised to neutralize it, Notaries who desire to protect their customers' documents from fraud may elect not to offer remote notarial act services and the public may choose to sacrifice the convenience of remote notarization because they perceive a notarial act in the physical presence of a Notary Public is safer, especially with respect to high-value notarial acts such as mortgages, property conveyances, powers of attorney, adoptions, and estate documents.

CONCLUSION

Deepfakes are an insidious new form of impersonation that threatens the integrity of remote notarial acts because actors can assume the lifelike appearance and speech of virtually any individual using photos and voice clips mined from social media and tools that are available on the dark web. Despite near universal enactment of remote notarial act laws across the country, no one could have anticipated the risk deepfakes pose to remote notarial acts, but here we are. Solutions for mitigating the deepfake threat include no longer allowing personal knowledge to be used as a means of identification for remote notarial acts, utilizing artificial intelligence, the Notary Public exercising discretion and reasonable care in vigilantly screening remotely located individuals during remote notarial act sessions and, ultimately, forgoing remote notarial acts altogether for valuable documents and instead meeting physically with a Notary Public.

---

[39]Henley, supra note 37: "... the most reliable way to smoke out deepfakes may be to insist on an in-person meeting."

[40]Notarial acts may be performed on electronic records in the Notary's physical presence (so called "in-person electronic notarization" or IPEN). Any benefits of using remote notarial acts to sign and notarize electronic records may be achieved by IPEN.

ABOUT THE NATIONAL NOTARY ASSOCIATION

Established in 1957, the National Notary Association (NNA) is the leading professional authority on the American Notary office and is dedicated to educating, serving and advocating for the nation's 4.4 million Notaries. The NNA published the *Model Notary Act* and the *Model Electronic Notarization Act* to help lawmakers enact effective legislation, and created *The Notary Public Code of Professional Responsibility*, a standard for best practices and professional conduct. To learn more, visit NationalNotary.org.

Government Inquiries

Bill Anderson, Vice President, Government Affairs
(818) 739-4064 banderson@nationalnotary.org

Media Inquiries

Phillip Browne, Vice President, Communications
(818) 739-4039 pbrowne@nationalnotary.org

Main

(800) US NOTARY (1-800-876-6827)