AXIOM Politics

NOTARIZE

Attachment E

Please Vote NO on HB19-1167 as Introduced

This is not the Uniform Law Commission bill nor any other national model that has been adopted or enacted anywhere in the country.

HB1167 incorporates never-before discussed concepts and would have the adverse effect of actually not allowing Colorado remote notaries in practice. Colorado companies can and already use remote notaries in a range of financial transactions but CANNOT use Colorado notaries. This bill, if passed, will continue to ensure they will not use remote notaries in Colorado.

For the last three years, remote notarization has been a topic of conversation at the State Capitol. HB19-1167 was drafted and introduced without any input from the previous proponents of remote notary legislation.

The Uniform Law Commission, a non-partisan group of over 300 lawyers from across the country including Colorado, worked since 2016 on legislation to update the Revised Uniform Law on Notarial Acts across the country to include remote notarization.

The National Association of Realtors, the National Association of Secretary of States, U.S. Treasury Department, Mortgage Banks, American Land Title Association, The Federal Financial Protection Bureau all support report notary models like the ULC citing the benefits of consumer and data protections and additional security protections that remote notaries provide.

We simply request a robust stakeholder meeting so we may discuss these new concepts and strive for some middle ground. As written, HB19-1167 in unworkable.

Outstanding Issues for HB19-1167 include:

- Completely new approach than any other state or national model
  - ULC model legislation: the ULC has been writing the uniform law code on Notarial Acts since 1892. They are the experts and passed model remote notary legislation in summer of 2018.
  - Not one single model law and not one single state law has ever included language like the language that HB19-1167 proposes.
  - Other states that have enacted legislation adding remote notarization include: VA, VT, OH, TN, IN, MI, MN, MT, NV, TX. Utah just passed the ULC bill this week, and it is on the Governor's desk where he is expected to sign.
  - Other states with legislation pending (expected to expand since ULC has approved language): MA, NJ, MD, PA, KY, SC, GA, AL, FL, LA, OK, MO, IA, WI, ND, SD, NE, WA, OR, CA, UT, AZ, AK, HI

- New "Personal Information" Definition (page 4)
  - HB18-1128 (concerning data privacy and breach) codified a definition of Personal Information. HB1167 codifies a new and separate definition for "Personal Information." Why would remote notaries have a separate definition?
- "Remote Notarization System" Definition
  - The way it is written is so broad it encompasses way more than a software platform pertaining to remote notary – it includes virtually every software or service provider.

Significant issues that make HB19-1167 unworkable:

Script: (pages 9 – 12) For the first time in notarial history, as opposed to just dictating the things that the notary needs to do, this bill lays out 15 different scripts JUST FOR remote notarizations.

- Purpose of notary is to verify signature. Dictating specific scripts in statute will open the door for any legal challenge of a notary if they don't follow an exact script.
- What problem is this trying to "fix"? A notary, is a notary, is a notary. Remote notaries are not trying to change the role and function of a notarial act.

Recording: According to page 13 of HB1167: "The recording must include the information described in this subsection (10)(b), but must not include any other information. Any other information included on the recording is not admissible in any Colorado Court of Law"

- First: the two sentences are contradictory
- Second: for example, in the case of a mortgage, this would require a stop and start of the video, which would then result in a video with gaps/black space in between signatures, opening up more legal questions and threats of litigation.
- This language prevents users of the platform – lenders and title – from deciding how to manage the recording to comply with law and meet their needs

Data Privacy: Written in a way that is inconsistent with the way every other data law is written. It is written as a "Prohibited Notarial Act," so that EVERY remote notarization is invalid if the new and untested definition of "personal information" is violated in any way. Data privacy bills are broad, overarching applications of law for any entity that touches data. Putting separate data provisions in a specific notarial act is inconsistent and problematic for the overarching data privacy laws. Why should "use of data" rules in a mortgage transaction be different for a notary than for a title agent, lender or other party using the exact same data?

The ULC discussed data privacy at length throughout the drafting process of the uniform bill and agreed that data privacy is a key priority, but that no further privacy provisions needed to be added to the notary bill. Data privacy pertaining to notarial acts is already addressed by a host of existing federal and state laws of broad, general application and specific laws pertaining to certain transactions—e.g. both federal and state laws that dictate privacy during the entire course of mortgage transactions.

The ULC also determined that if a state wants to add additional data breach or privacy protections to its laws, it should do so (as many states are doing) in laws of general application covering ALL uses of data, and that putting privacy provisions in a notary law can create very adverse consequences. A data protection bill of general application is precisely what Colorado did last year with HB18-1128.

No other state bill or "model act" has included separate privacy provisions in a notary bill.

That being said, we want everyone to be assured that data privacy is a priority and are offering the alternative language:

- Alternative: "in accordance with applicable law" consistent with HB18-1128. A remote notarization system shall use all personal information collected in the course of performing a notarial act, as follows: (a) to complete the notarial act and related activities or in accordance with applicable law consistent with the requirements of CRS 6-1-713.5, (b) a notary public shall implement and maintain technical controls reasonably designed to protect personal identifying information from unauthorized access, modification, disclosure or destruction. (c) the Attorney General may promulgate rules, consistent with applicable law, concerning requirements for disclosure of intended uses and for consumer consent regarding use and security of personal information.

Unanswered Questions about SB 19-1167

- **Unlike other federal and state privacy statutes, why does the bill not take into account the countless existing laws and regulations under which disclosure of PII is either necessary or mandatory? *For example:***

  - to take precautions against liability or for use in anticipation of litigation
  - for use by businesses and individuals to investigate fraud, negligence or misconduct in order to protect consumers or reduce institutional risk
  - to provide information to oversight bodies, insurance rating bureaus, etc.
  - for use in business reorganizations, including under court-appointed receiverships or in bankruptcy proceedings, etc.
  - to enforce legal rights beyond the transaction, including damage claims for data breach, etc.
  - to audit both subject transactions and related ones
  - in response to consumer requests or complaints
  - ***And many, many more...***

- **How does this bill interact with and take into account the contradictory provisions of applicable federal law and the numerous required and permitted disclosures under these laws? *For example:***

  - Health Insurance Portability and Accountability Act (HIPPA)
  - Gramm-Leach-Bliley Act (GLBA)
  - Fair Credit Reporting Act (FCRA)
  - Drivers Privacy Protection Act (DPPA)
  - Children's Online Privacy Protection Act (COPPA)
  - CAN-SPAM Act
  - Telephone Consumer Protection Act (TCPA)
  - Electronic Communications Privacy Act (ECPA)
  - Computer Fraud and Abuse Act (CFFA)
  - ***And many, many more...***

- **How does this bill interact with and take into account the numerous incompatible provisions of Colorado law and the numerous required and permitted disclosures under these laws? *For example:***

  - Data Breach Notification Statute, C.R.S. § 6-1-716 (requiring breach notices to consumers, credit reporting agencies, law enforcement, etc.) [subject of current HB 18-1128]
  - Consumer Protection Act, C.R.S. § 6-1-101 et seq. (enforcing unfair or deceptive trade practices and incorporating Colorado's No-Call List Act and the Spam Reduction Act of 2008)
  - Student Data Transparency and Security Act (permitting disclosures under regulated conditions for research, educational testing, etc.)
  - Colorado's law on consumer document retention and disposal [subject of current HB 18-1128]
  - Colorado's law on confidentiality of SSNs, C.R.S. § 6-1-715 (with exceptions for certain application or enrollment processes)
  - Uniform Records Retention Act, C.R.S. § 6-17-102 et seq. (allowing reproductions of records to satisfy retention requirements)
  - Colorado's Division of Securities Cybersecurity Rules, 3 CCR 704-1 (governing privacy notices and consumer opt-out rules)
  - Many provisions of Colorado's Open Records Act, e.g. C.R.S. § 24-72-602 (permitting Department of Revenue to distribute medical information with consumer consent)
  - ***And many, many more...***

- **Why does this bill, unlike all other state and federal privacy laws, create new and "siloed" definitions of key terms? What do the following terms mean, and are they intended to follow some existing federal or state law or is the intent to create new definitions? *For example:***

- *"non-public personal information"*: This definition is not aligned with the definition of the same term in last year's HB 1128. How are they reconciled? How is this definition reconciled with federal law?
- *"as necessary to effect, administer, or enforce, service or process the transaction"*: A somewhat similar, but differently worded phrase is a defined term in GLBA, 15 U.S.C. § 6809(7)—which includes numerous sub-parts for a broad explanatory context—and in that Act's implementing regulations, 12 C.F.R. § 1016.14. Is the same definition intended here or a different one, given the different wording involved?
- *"financial product"*: Was this phrase taken from GLBA? Does it mean the same thing as in that federal law?

➢ **How is one supposed to interpret the provisions of this bill that contradict existing Colorado notarial law or even other provisions of this same bill? *For example:***

- Under C.R.S. § 24-21-519(5), a notary may make a copy of a journal entry of a notarial act for any other person for a fee. This provision, which makes the notarial journal a public record, would violate the proposed prohibition on use/sale of data.
- HB 19-1167 contemplates use of Public Key Infrastructure (PKI) technology to enable a customer who has been authenticated in a prior transaction a safe and simple method to verify identity in a future transaction. Use of PKI would be prohibited if an authentication from one notarial act cannot inform the authentication procedure in a future one.

➢ **How exactly is the information a person provides for identification purposes somehow less secure for remote notarizations that in the existing world of paper notarial acts? *For example:***

- When a person takes a "knowledge-based authentication assessment," they are answering questions complied using information *that the test taker already has*. (For example, Lexis Nexis.) These data providers have billions of data pieces, and they are the ones formulating the questions. In other words, they are just testing the person's knowledge about the claimed identity—not collecting any additional information about that identity that they do not already possess.
- The use of "credential analysis" likewise gathers no additional information than what a notary today collects and inserts in the journal entry required by C.R.S. § 24-21-519. As stated above, this information is already public information.

Examples in Practice
Just by way of highlights, here are the simplest points about how that language is problematic:

1. The "you can't sell data" language assumes that you can prohibit ANY use of data and then add back in bits and pieces as needed; but in doing so, you by definition DEPRIVE the consumer of the ability to use services they actually want and like, and you PREVENT holders of data from complying with a vast range of legal requirements for use of data which weren't on the list of "add backs" drafted by the Bar.

2. For example, the language would prohibit a company from:

a. Complying with ANY of the data security and breach notifications required under HB18-1128, or ANY of the data breach notifications required under federal law;

b. Complying with the system change notification requirements under the federal E-Sign Act;

c. Letting a consumer access their documents online to view or forward their notarized documents at a later date, including for example at tax time when they were preparing their returns and wanted to see about prepaid interest, etc.

d. Letting a Bank review a notarial record to decide whether or not it should accept a Power of Attorney.

NOT ONE SINGLE MODEL LAW AND NOT ONE SINGLE STATE LAW HAS EVER INCLUDED LANGUAGE LIKE THE LANGUAGE PROPOSED.

See highlighted on page 2

Nearly 3 dozen cybersecurity breaches reported in Colorado since start of consumer data-privacy law

Since S
reporte
the Col
is a bri
(Anth

More than 90,000 Coloradans private data has been breached – at least that's what we know of thanks to a new state law

FEB 13, 2019 5:00AM MST **BUSINESS**

Tamara Chuang *@gadgetress*

The Colorado Sun — tamara@coloradosun.com
Tech+Business+Economy
See more

More

Credibility Indicators

These are selected by the writer and confirmed by the editor

T

Rarely does a week go by without hearing of another cybersecurity breach that exposed piles of private consumer data to strangers. At least Coloradans can take comfort that should this happen to their own personal data, the attacked company must notify them within 30 days.

The state law, which went into effect Sept. 1, has as of Feb. 5 resulted in 33 organizations reporting consumer data breaches and notifications sent to 91,235 Coloradans, according to the Colorado Attorney General's office.

That may seem low, considering that also since September, data breaches affected 500 million Marriott International customers, 50 million Facebook users and others. But it's unknown how many companies are in compliance with Colorado law — or even know about it.

"We've had a few" breaches, said Benjamin Hase, a Colorado attorney and information manager for the Employers Council, which helps companies with employment law. "We've had (members) get hacked. We've had people with stolen laptops."

But companies are only required to tell the attorney general's office if it impacts more than 500 Coloradans. The law, which began as House Bill 1128, passed quickly in the state legislature last year and is considered one of the strictest in the nation because of the 30-day notification period (Florida's is also 30 days, but the industry standard is more like 45 to 60 days). Many companies probably still aren't familiar with the new law, though those who learn about it want to comply, Hase said.

MORE: Colorado has one of nation's strictest consumer data protection laws. Are you ready?

"We've issued a few of these (notices) but nothing so big that it's required telling the AG's office," Hase said. "Factor that in with the many organizations that still don't know about this and who knows how many (breaches) are out there?"

Companies that store private data of any citizen in Colorado are included, even if the company is located outside of the state. The law also requires companies to protect consumer data, manage it and delete it when it's no longer needed. It's part of the Consumer Protection Act, which defines personal data as a name plus another identifier, such as a health insurance number, biometric data or a security question that unlocks a user's account.

The 30-day notification system has been the tough part for many businesses, said Esteban Morin, an attorney specializing in privacy and data security for the Denver office of Brownstein Hyatt Farber Schreck.

"A lot of times, you don't know the full scope of what information was

affected and you have to get cyber forensics to get in there. That can take a lot of time, but you're on this very rigid clock," Morin said. "It's caused us to make some complicated decisions."

Morin said some clients might have to notify customers in waves as the breach investigation continues. As more affected accounts are discovered, the notice goes out, even if it's after the 30-day deadline.

"You might be in danger of violating the 30-day statute, but it's the best you can do. The 30-day (deadline) is challenging and has caused a lot of stress," he said. "But at the same time, I understand it does represent personal information and the compromise of that can cause harm to a person's identity and finances."

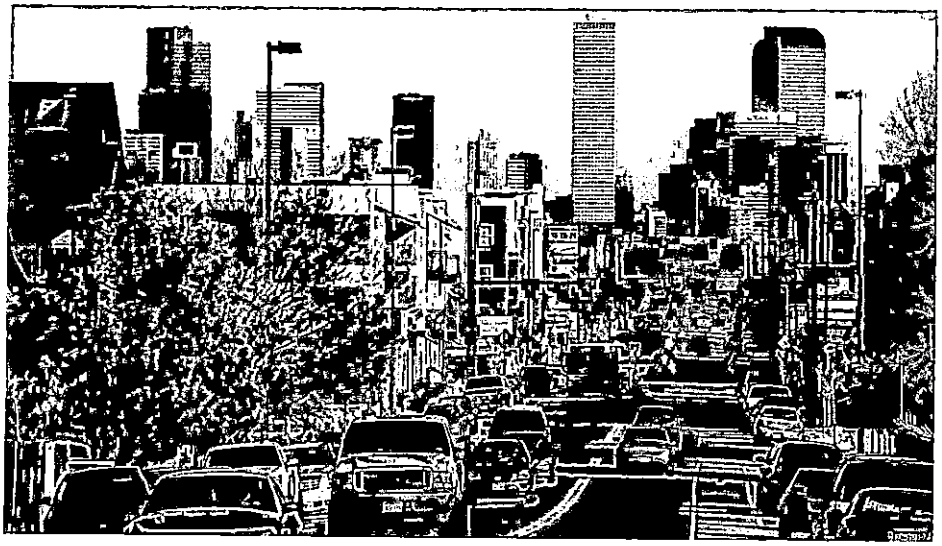
While it's time consuming to develop a plan to manage consumer data — and figure out what personal data needs to be deleted — it needs to be done, said Phil Weiser, the state's attorney general.

"There are times when businesses, think Target and Equifax, have been complacent and failed to take reasonable measures that expose consumers to harm. Identity theft is rising year to year because it's so attractive to hackers to steal consumer information and abuse it," Weiser said. "We need to make sure we're doing everything we can. I'm going to make it this a top priority for my administration."

Colorado Attorney General Phil Weiser (Jesse Paul, The Colorado Sun)

Weiser declined to share which organizations reported data breaches since cases are under investigation. But his office said common methods included phishing emails with malicious links or point-of-sale systems and online shopping carts infected with malware. Types of sites ranged from travel companies and banks to retailers. Another common target? Rewards-program databases.

The city of Denver, which was dinged twice in city auditor reports for some insecure network folders and outdated policies, has addressed most of the auditor's issues. One piece it's still working on is classifying all the stored private consumer data to figure out what needs to be kept or deleted, said Dawn Summers, the city's first chief data protection officer. The city also adjusted its notification period to 30 days.



The city of Denver, which was dinged twice in city auditor reports for some insecure network folders and outdated policies. A view of downtown Denver on Jan. 15, 2019. (Jeremy Sparig, Special to The Colorado Sun)

"I like to use the analogy of a house. (Colorado law) says your house is information security and you have to lock it. If someone breaks in, you have to fix it. And you have to take out the trash," said Summers, adding that she expects the city's more robust data privacy process will take three to five years to implement. "...Privacy and data protection is a little different from information security. It's changing how our work culture thinks about how we're using people's information."

Some businesses found it easy to comply with the new law. Gusto, a payroll and benefits company with co-headquarters in Denver and San Francisco, already met regulations like HIPAA, the Health Insurance Portability and Accountability Act; and HITECH, the Health Information Technology for Economic and Clinical Health Act.

"We shrugged our shoulders and said we already comply with HIPAA and HITECH," said Rick Chen, a spokesman with Gusto. "Anytime there's any data privacy or security type of legislation or regulation, we always take a look to make sure we're in compliance. If there's anything we're missing, we'll take time to figure it out."

Gusto tweaked its policy to notify Coloradans within 30 days. But it expects more changes are coming with future laws.

The California Consumer Privacy Act goes into effect in January 2020 and would make it easier for consumers to find out what personal information has been collected and request it be deleted. And a federal bill proposed by U.S. Sen. Ron Wyden, D-Oregon, would allow Americans to find out who is buying their personal data. Chen said companies like Gusto realize they must stay on top of new laws.

"As a general rule, we tool processes toward the most strict requirement to fully comply with all relevant laws and regulations," Chen said.

The attorney general's office has a FAQ page online to guide businesses that need to comply. The Employers Council also provides advice on creating policies.

Weiser is also moving ahead to adopt stronger consumer protections. On Monday, he joined attorneys general from about 30 states to urge the Federal Trade Commission to update identity theft rules to clamp down on thieves using available data to, for example, get a credit card in someone else's name. Weiser is also working on getting a group of local business and cybersecurity leaders to collaborate on best practices.

"There is, I believe, a real opportunity for us here in Colorado, for us to be at the forefront of developing better cybersecurity, better data privacy and better security practices," Weiser said.

If anything, Colorado's law has helped companies reevaluate data management policies, find risks and make sure they're deleting personal user data when it's no longer needed, Morin said.

"Honestly, pound for pound, there are some complications with the 30-day deadline," Morin said, "but I think all around, the fact is that it's sparked additional conversations and has spurred companies to examine the big picture and talk about what risks do we face if there's a security incident or how much trouble are we in."

More from The Colorado Sun

- Building something real on the blockchain comes down to collaboration, better tech and pizza
- Cañon City seeks a makeover to become a destination, not just a drive-through prison town
- Colorado co-op's fight for renewable energy could upend how rural communities are powered
- Nearly 3 dozen cybersecurity breaches reported in Colorado since start of consumer data-privacy law
- Colorado's first-in-the-nation outdoor MBA program is hitting its stride just as the industry needs it to

Tags:

lotarize achieves SOC 2 ompliance – delivering ne most secure latform for life's most nportant transactions

sica Meher on February 7, 2018

We believe life's most sensitive and important transactions require the most secure platform.

That is why we are relentlessly focused on protecting our customer's data. Whether documents include a Deed of Trust, Promissory Note, or Closing Disclosure, our mission is to make legal notarization more convenient, secure, and verifiable. To achieve this, we've built out a comprehensive information security program that incorporates leading practices into every aspect of our operations.

Today, we're pleased to announce that we've completed our SOC 2 audit and have received our Type I attestation report from internationally-recognized accounting firm Kirkpatrick Price. This credential provides clear evidence that Notarize has a strong commitment to deliver high quality services for our clients by demonstrating we have the necessary internal controls and processes in place.

SOC 2 audits are completed based on the AICPA's Trust Services Principles: security, availability, processing integrity, and confidentiality. With

successful completion of a SOC 2 audit, we've shown that the design and operating effectiveness of our organizational controls meet the criteria for these principles.

We fundamentally believe that online notarization (and Notarize specifically) is infinitely better at identifying people (and proving it) than the in-person notarization approach that's been relied upon for centuries.

The online approach enables us to perform multi-factor identity verification, record a live video of the signing session, and collect a comprehensive digital audit trail of the electronic signature process. Not only is this unparalleled convenience for the signer (anytime, anywhere) but it also enables authorized third parties to obtain independent confirmation of a transaction's validity.

Every document that's executed on our platform has a digital signature (using Public Key Infrastructure in accordance with the X.509 standard) applied to ensure data security and document integrity. After a notarization is performed and the document is fully complete, it is easy for a third party to verify the notary's identity and use the tamper-evident seal to confirm the document hasn't been altered since it was signed.

Why Notarize is the most secure solution for the mortgage industry:

- In today's post-TRID environment, the need for strong information security compliance has never been more apparent. Mortgage industry

participants are under tremendous pressure to ensure data privacy and enact tight operational controls.

- We have a detailed document audit trail that shows exactly how each document is interacted with throughout its lifetime, so that Lenders and Title companies can easily meet the needs of external auditors who are increasingly looking for evidence of compliance.
- By closing with Notarize, you can significantly reduce the amount of NPI-handling across the whole transaction. No more printing paper or FedEx.

But this new online approach to notarization only works if the data that's collected is protected with proper care. Our SOC 2 milestone demonstrates that we've invested heavily in the people, process, and technology to make our security controls a reality. And we'll continue to invest daily and remain ever vigilant.

See how Notarize works or schedule a demo here.

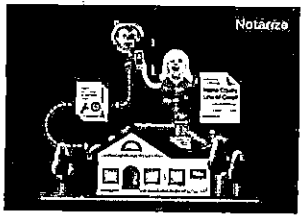
About Kirkpatrick Price:

Kirkpatrick Price is a licensed CPA firm, PCI QSA, and a HITRUST CSF Assessor, registered with the PCAOB, providing assurance services to over 600 clients in more than 48 states, Canada, Asia, and Europe. The

firm has over 11 years of experience in information security and compliance assurance by performing assessments, audits, and tests that strengthen information security and internal controls. KirkpatrickPrice most commonly provides advice on SOC 1, SOC 2, HIPAA, HITRUST CSF, PCI DSS,ISO 27001, FISMA, and CFPB frameworks.

Posted in: new features security business

You have notarization questions, we have notarization answers. While we at Notarize pride ourselves on providing helpful resources (like this blog!) to demystify notarization, we're not lawyers and don't give legal advice. Pro tip: always check with your own attorneys, advisors, or document recipients if you have further questions about notarization or digitally notarized docs.



Close Home Equity Loans, Online – Announcing Notarize for HELOC Transactions

10 million.

READ MORE

Get it Notarized!

On your computer or iPhone.
It's free to sign up.

LET'S GET STARTED

Notarize for Business

Collect notarizations from your clients.

LEARN MORE

ABOUT NOTARIZE

Careers

Join Notary Network

Privacy Policy

Terms of Use

SOLUTIONS

Business

Enterprise

Mortgage

Title Agents

Developers (API)

RESOURCES

Verify a Document

Availability

Blog

SUPPORT

Knowledge Center

Customer Support

FAQ's

Stamping docs and talking

We at Notarize pride ourselves on providing helpful resc
notarization. We are not lawyers, and don't give legal ac
your own attorneys, advisors, or document recipients if
questions about notarization or digitally notarized docun

Stamping deed and talking shop

Interested in hearing more announcements and industry news? Enter your email below to be the first to know.

name@example.com

Notarize

Privacy Policy

EFFECTIVE DATE: June 27, 2018

Notarize, Inc. ("**Notarize**," "**we**," "**us**" or "**our**") values your privacy. We maintain a website at https://notarize.com (the "**Site**") and a mobile software application (collectively, the "**Platform**"), through which users can obtain electronic notarization, e-signature, identity verification and other services (the "**Services**"). In this Privacy Policy ("**Policy**"), we describe how we collect, use, and disclose information that we obtain about visitors to the Site or that is collected through the Platform. Our Privacy Policy applies to any visitor to the Site or the Platform, including (i) casual visitors who do not sign up for an account ("**Site Visitors**"), and (ii) users who have registered through the Platform to receive the Services ("**Subscribers**") or who have been designated by Subscribers to sign documents or otherwise participate in Services on on the Platform ("**Signatories**" and "**Witnesses/Participants**"). Collectively, all the foregoing are referred to as "**You**."

By visiting the Site or the Platform, or using any of our Services, you acknowledge that your personal information will be handled as described in this Policy. Your use of our Site or Services, and any dispute over privacy, is subject to this Policy and our Terms of Use, including its applicable limitations on damages and the resolution of disputes. All defined terms used in this Privacy Policy and which are also used in our Terms of Use have the meanings set forth in the Definitions in our Terms of Use.

1. THE INFORMATION WE COLLECT ABOUT YOU

We collect information about you directly from you as well as automatically through your use of our Site, Platform or Services.

Information We Collect Directly From You. Most content on the Site is accessible without an account. However in order to use the Services on the Platform,

you must create an account and become a Subscriber, Signatory or Witness/Participant. Different Services require that you provide somewhat different forms or types of information, but in general the minimum mandatory information that you (or, with respect to certain information, a Subscriber creating a Transaction on your behalf) must provide is:

(i) your name;

(ii) your address;

(iii) your e-mail address;

(iv) your phone number;

(v) the last four digits of your Social Security number (for Notarial Acts);

(vi) a government-issued form of photo identification;

(vii) depending upon the Transaction, a secondary form of identification document;

(viii) documents relating to the Services requested; and

(ix) other Transaction information required to provide and complete the Services.

Where you do not provide this information, we are unable to provide the Services to you.

The registration process provides Subscribers with a user name and password to enable access to the Services on the password-protected portions of the Platform.

In order to provide certain of the Services, including

Notarization and Identity Verification Services, we provide on the Platform a live video link between you and a Provider Notary or Identity Verification Designated Agent, so that the Notary or Agent can interact with you and, as applicable, make determinations about your identity and witness the signing of relevant document(s) (the "**Session Video**"). This means that we will capture images of Subscribers, Signatories, Witnesses and other Participants who make use of the Services and whatever content is displayed during the Session Video. By requesting and participating in the Services, you confirm that all persons depicted in the Session Video are authorized and permitted to participate and have consented to do so.

Information We Collect Automatically. We automatically collect the following information about Site Visitors or Subscribers through cookies and other web tracking technologies: your IP address (the Internet address of your computer), your computer's name, the type and version of your web browser, referrer addresses and other generally-accepted log information. We may also record page views (hit counts) and other general statistical and tracking information, which will be aggregated with that of other users in order to understand how our Platform is being used, and for security and monitoring purposes. We may combine this information with other information that we have collected about you, including, where applicable, your name, location and other personal information such as your browsing patterns. Please see the section "Cookies and Other Tracking Mechanisms" below for more information.

Information we collect from Public Sources.

For Subscribers, Signatories and Witnesses/Participants, as applicable in the specific context of use of the Platform and delivery of Services, in order to verify identification information as part of our legal and contractual obligations, we will collect and review personal information and identity credentials provided by you through use of identity database services provided by third party service providers such as, for example, Lexis Nexis.

Information Collected by Third Parties.

Our Site and Services contain a link to a third-party payment provider to enable you to make payment for any Services (in the event your payment obligations to us are not managed through invoicing and other methods of payment). This company acts as separate entity and Controller (as that term is defined by applicable law) in relation to any billing or credit card information, and its processing is not governed by this Policy. We do not hold your billing data, other than records of actual charges and related information, and we are not responsible for the information practices of such third party.

2. HOW WE USE YOUR INFORMATION

We use your personal information for the following purposes, subject to any limitations in applicable law or our contracts with Subscribers and third parties:

A. To provide our Services to you, to communicate with you about your use of our Services, to respond to your inquiries, and for other customer service and

opportunity purposes.

B. To record information generated in the course of providing the Services including information provided by you as well as session and audit trail information and the Session Video.

C. To maintain the availability and security of our Site, to tailor the content and information that we send or display to you, to offer personalized help and instructions to you, and to otherwise personalize your experiences while using the Site or our Services.

D. For our own marketing and promotional purposes. For example, we may use your email address to send you newsletters about events or special offers and promotions, or to otherwise contact you about products or services we offer which we think will interest you. You have the right to opt-out of these emails at any time.

E. To better understand how users access and use our Site and Services, both on an aggregated and individualized basis, in order to improve our Site and Services and respond to user desires and preferences, and for other data analytical purposes. In particular, we allow you to voluntarily participate in surveys and questionnaires which we will use for the purposes of monitoring and improving the use and appeal of the Platform and the Services.

F. To monitor responses on any blog, message board system, or review capability available on our Platform.

G. To comply with legal obligations, such as the

requirements of notarial law including identity verification and recordkeeping, e-signature law, and other laws applicable to transactions on our Platform; as part of our general business operations; and for other business administration purposes.

H. Where we believe necessary to investigate, prevent or take action regarding illegal activities or situations involving potential threats to the safety of any person or violations of our Terms of Use or this Policy.

3. HOW WE SHARE YOUR INFORMATION

We share your information as follows:

- ***Designated Recipients and Transaction Participants with required permissions.*** Documents, the Session Video and other information resulting from the Transaction and our Services will be shared with you and any party with the required permissions to see such information after the Transaction is completed. This could include a Designated Recipient set up at the time a Subscriber created a Transaction, or other parties to the Transaction with necessary permissions. For example, in a real estate transaction, this could include your lender or title agent.
- ***To those with a legal right to see such information.*** We will share your information with regulatory agencies, enforcement authorities, parties with a legal subpoena, or members of the public or other parties with the legal right to compel us to provide such information for their review. (Note that notarial journals are available

for public review under specified conditions and circumstances in certain states.) All such sharing by us will be in accordance with the requirements of applicable law.

- ***Support Community Users.*** If you upload feedback to any public blog, message board system, or review capability available on our Platform or the Site, your user name and any information that you post, including, without limitation, reviews, comments, and text will be available to, and searchable by, all users of the Site. Messages you send in our Support channel, to us, will be viewable only by you and us.
- ***Service Providers.*** We disclose the information we collect from you to service providers, contractors or agents who perform services for us. For example, we engage third parties to provide database identity verification support services, and a third-party vendor to provide the live video link necessary to create the Session Video (the "**Video Vendor**"). Once we receive the Session Video, the Video Vendor is required to delete its copy of the Session Video.
    - ***Platform Vendors.*** We may employ other companies to perform IT functions on our behalf, such as hosting or maintaining the Platform (collectively, "Platform Vendors").
- ***Affiliates.*** We may disclose the information we collect from you to our affiliates or subsidiaries, including Notarize, LLC; however, if we do so, their use and disclosure of your personal information will be subject to this Policy.
    - ***Business Transfers.*** If we are acquired by or merged with another company, if substantially all

of our assets are transferred to another company, or if we are involved in any bankruptcy proceedings, we will transfer the information we have collected from you to the other company.

- ***In Response to Legal Process.*** We might also disclose the information we collect from you in order to comply with the law, a judicial proceeding, court order, or other legal process, such as in response to a court order or a subpoena.
- ***To Protect Us and Others.*** We will disclose the information we collect from you where we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Terms and Conditions or this Policy, or as evidence in litigation in which Company is involved.
- ***Aggregate and De-Identified Information.*** We may share aggregate or de-identified information about users with third parties for research purposes.

4. OUR USE OF COOKIES

We use cookies and other tracking mechanisms to track information about your use of our Site or Services.

Cookies. Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your web browser for record-keeping purposes. Some cookies allow us to make it easier for you to navigate our Site and Services, while others are used to enable a faster log-in process or to allow us to

track your activities at our Site and Service. There are two types of cookies: session and persistent cookies.

- **Session Cookies.** Session cookies exist only during an online session. They disappear from your computer when you close your browser or turn off your computer. We use session cookies to allow our systems to uniquely identify you during a session or while you are logged into the Site. This allows us to process your online transactions and requests and verify your identity, after you have logged in, as you move through our Site.
- **Persistent Cookies.** Persistent cookies remain on your computer after you have closed your browser or turned off your computer. We use persistent cookies to track aggregate and statistical information about user activity.

We may use cookies to track your use of the Platform and to recognize you when you return to our Platform. In addition, we use "pixel tags", small graphic images (also known as "web beacons" or "single-pixel GIFS"), to tell us what parts of our Platform have been visited or to measure the effectiveness of searches customers perform on our Platform. Pixel tags also enable us to send email messages in a format customers can read, and they inform us whether emails have been opened, to help ensure that our messages are of interest to our customers.

Disabling Cookies. Most web browsers automatically accept cookies, but if you prefer, you can edit your browser options to block them in the future. The Help portion of the toolbar on most browsers will tell you

how to prevent your computer from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Visitors to our Site who disable cookies will be able to browse certain areas of the Site, but some features may not function.

Do Not Track. Currently, our systems do not recognize browser "do-not-track" requests. You can, however, disable certain tracking as discussed in this section (e.g., by disabling cookies).

5. SECURITY OF YOUR PERSONAL INFORMATION

We have put in place security systems designed to prevent unauthorized access to or disclosure of the personal information you provide to us, and we take all reasonable steps to secure and safeguard this personal information. Our Platform's password-protected section requires users to give us unique identifiers such as their user name and password. Notarize employees are required to acknowledge that they understand and will abide by our policies with respect to confidential and private information. Additionally, we evaluate our third party service providers based upon the type of information they receive and process for our customers and then, based upon our security guidelines, require key vendors to confirm with us their confidentiality obligations and use of security processes. Moreover, permissioned access to our databases containing personal information is governed by our internal security policy.

Our security systems are structured to deter hackers and others from accessing information you provide

to us. However, due to the nature of Internet communications and evolving technologies, we cannot provide assurance that the information you provide us will remain free from loss, misuse, or alteration by third parties who, despite our efforts, obtain unauthorized access. Accordingly, you should take steps to protect against unauthorized access to your password, phone, and computer by, among other things, signing off after using a shared computer, choosing a robust password that nobody else knows or can easily guess, and keeping your log-in and password private. We are not responsible for any lost, stolen, or compromised passwords, or for any activity on your account via unauthorized password activity, or for any improper uses of your account or password which you permit others to make.

User Generated Content: If you post content to our Site, all of the information that you post will be available to all visitors to our Site. We cannot prevent such information from being used in a manner that violates this Policy, the law, or your personal privacy.

6. MODIFY MY PERSONAL INFORMATION

Subscribers are able to modify personal information submitted by logging into your account and updating your profile information. You can also email us at the email address below in order to change your personal information.

7. DIRECT MARKETING BY US.

Where you have agreed to receive newsletters or similar materials from us, we will send periodic

promotional or informational emails to you. You can opt-out of such communications by following the opt-out instructions contained in the e-mail. If you opt-out of receiving emails about recommendations or other information we think may interest you, we will still send you service messages about your account or any Services you have requested or received from us or other notices as required by law.

8. CHILDREN UNDER 16

Our Services are not designed for children under 16 years of age (16). If we discover that a child under 16 has provided us with personal information, we will delete such information from our systems.

9. ADDITIONAL INFORMATION FOR EU INDIVIDUALS

Certain rights may be held by those who access the Platform or our Services and who are residents of the European Union ("EU"). The following information is provided for the benefit of such users and in the event it may affect their rights:

The Data Controller of the information collected through the Services is Notarize, Inc. which is headquartered in the United States at 745 Boylston Street, Unit 600, Boston, MA 02116. To exercise any rights that you have with regard to your personal information, you can contact us using the following details: support@notarize.com

The legal bases for using your personal Information. We collect your information as a Data Controller when we have a legal basis to do so. The following

legal bases pertain to our collection of data:

- Our use of your personal information is necessary to perform a **contract** or take steps to enter into a contract with you. This applies to our processing activities described in Section 2 above, including sections A and B.
- Our use of your personal information is in our **legitimate interest** as a commercial organization to make improvements to our Services, to expand our business and increase revenue and business opportunities, and to ensure that we maintain a reputable status. This applies to our processing activities described at Section 2 above, including sections C,D,E and F.
- Our use of your personal information is **necessary to comply with a relevant legal or regulatory obligation** that we have. This includes performing compliant Transactions and providing compliant Services; forming and maintaining required records; providing legally required access to information; providing required notices; maintaining secure systems; tracking and managing use of data; and disclosing information where required to a court, authority, agency or regulatory body or member of the public with a right of access. This applies to our processing activities described at Section 2, including sections A,B,C,D, G and H.
- Our use of your personal information is in accordance with your **consent**. This applies to our processing activities described at Section 2, including sections A,B and D.

If you would like to find out more about the legal bases on which we process personal information, please contact us.

Legal Rights Which May Apply to Users from the EU. Subject to certain exemptions; subject to applicable US federal and state law (including without limitation notarial law and e-signature law) and the obligations imposed upon us thereunder regarding use of data, recordkeeping, notifications and other compliance requirements; and dependent upon the processing activity we are undertaking; European Union individuals may have certain rights in relation to personal information. These may include:

Right to access, correct, and delete your personal information: If applicable, you have the right to request access to the personal information that we hold about you and: (a) the source of your personal information; (b) the purposes, legal basis and methods of processing; (c) the data controller's identity; and (d) the entities or categories of entities to whom your personal information is transferred. You also have the right to request that we correct any inaccuracies or (subject to other controlling law) delete your information. We are not required to comply with your request to erase personal information if the processing of your personal information is necessary for compliance with a legal obligation or for the establishment, exercise, or defense of legal claims.

Right to restrict the processing of your personal information: If applicable, you have the right to restrict the use of your personal information when (i) you contest the accuracy of the data; (ii) the use is

unlawful but you do not want us to erase the data; (iii) we no longer need the personal information for the relevant purposes, but we require it for the establishment, exercise, or defense of legal claims; or (iv) you have objected to our personal information use which we have justified based on our legitimate interests verification as to whether we have a compelling interest to continue to use your data. In addition to other rights we have under law, we can continue to use your personal information following a request for restriction, where: (a) we have your consent; or (b) to establish, exercise or defend legal claims; or (c) to protect the rights of another natural or legal person.

Right to data portability: To the extent that we process your information (i) based on your consent or under a contract; and (ii) through automated means, you have the right to receive such personal information in a structured, commonly used, machine-readable format, or you can ask to have it transferred directly to another data controller.

Right to object to the processing of your personal information: If applicable, you can object to any processing of your personal information which has our legitimate interests as its legal basis, if you believe your fundamental rights and freedoms outweigh our legitimate interests. If you raise an objection, we have an opportunity to demonstrate that we have compelling legitimate interests which override your rights and freedoms

Right to lodge a complaint with your local supervisory authority: You have a right to lodge a complaint with your local supervisory authority if you

have concerns about how we are processing your personal information. We ask that you please attempt to resolve any issues with us first, although you have a right to contact your supervisory authority at any time.

How to Exercise Your Rights: If the above rights apply to you and you would like to exercise them, please send us a request to support@notarize.com. In your message, please indicate the right you would like to exercise and the information to which it relates. We will ask you for additional information to confirm your identity and for security purposes before disclosing to you any requested personal information. We reserve the right to charge a fee where permitted by law, for instance if your request is manifestly unfounded or excessive. We will not always be able to fully address your request, for example if it would affect the duty of confidentiality we owe to others, or if we are legally entitled to deal with the request in a different way.

Cross-border Transfer of Information. We maintain servers and systems in the United States hosted by third party service providers. As a result, where the personal information that we collect through or in connection with the Services is processed in the United States, we will take steps to ensure that the information receives the same level of protection as if it remained within the European Union/EEA. You have a right to receive details of any safeguards that we have where your data is transferred outside the European Union (e.g. to request a copy where the safeguard is documented, which may be redacted to ensure confidentiality).

Retention. We will keep your information in a secure manner, as set forth above. We will retain your data for the period necessary to fulfill the different purposes outlined in section 2, including without exception to meet legal, regulatory and contractual requirements. We will endeavor to maintain an accurate record of your dealings with us in the event of any complaints or challenges, and if we reasonably believe there is a possibility of legal action relating to your data or dealings.

10. CALIFORNIA PRIVACY RIGHTS

California residents have the right to request and obtain from us once a year, free of charge, information about the personal information (if any) we disclose to third parties for their own direct marketing purposes in the preceding calendar year. If applicable, this information would include a list of the categories of personal information that was shared and the names and addresses of all third parties with which we shared information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to support@notarize.com.

11. CONTACT US

If you have questions about the privacy aspects of our Services or would like to make a complaint, please contact us at support@notarize.com.

12. CHANGES TO THIS POLICY

This Policy is current as of the Effective Date set

forth above. We may change this Policy from time to time, so please be sure to check back periodically. We will post any changes to this Policy on our Site at https://notarize.com/privacy/. If we make any changes to this Policy that materially affect our data privacy practices with regard to the personal information we have collected from you, we will provide you with notice in advance of such change.

We at Notarize pride ourselves on providing helpful resources to help demystify notarization. We are not lawyers, and don't give legal advice, so always check with your own attorneys, advisors, or document recipients if you have unanswered questions about notarization or digitally notarized documents.

Common Questions: Remote Notarization

The purpose of the notarial act is (a) to identify the signer, (b) to accept the signer's acknowledgment and (if applicable) to place the signer under oath, and (c) for the notary to complete a notarial certificate and place her seal.

In each of these functions, the remote notarization process provides dramatic improvements in identity validation, transparency and record-keeping, transaction and document security, and verifiability and enforcement.

A. Identity Validation:

Most problems with the notarial act involve identity fraud. Currently, the only tool available to the notary is visual review of an identity credential. Notaries are not expert document examiners, and sophisticated fraudsters have developed numerous ways to mock up or improperly obtain genuine-looking photo ID's. (Moreover, in a study conducted by the National Notary Association, a panel of notaries were unable to identity almost 30% of individuals from a lineup by looking at their photo ID).

In a remote notarization, a host of new technology-based tools are available to the notary to dramatically improve identity validation. In our processes, all signers go through a multi-phase identity validation process: First, their name and identity data is checked against a host of identity databases, and then they must pass a knowledge-based authentication process which uses "out of wallet" questions generated from a range of historical databases; then they must upload the front and back of an unexpired photo ID to which a software-based forensic analysis is applied (which can detect and provide the notary with information about key elements of a modern ID); then the notary herself views a high-resolution image of the photo ID and compares it to the signer to her satisfaction. If the signer fails any of these processes, or if the notary does not feel comfortable with the ID or the individual , the notary can terminate the transaction at any time.

B. Duress and Coercion — Transparency and Record-Keeping:

Not only must the signer passes the above identity validation processes, but the entire notarial transaction itself is conducted in a real-time audio-video session where the signer and notary can see and hear each other throughout and also can see each others' actions on the subject document at the same time, together. The entire audio-video session is recorded, as is all the key transaction information about

the session (geo-location, IP address, identity validation information, a copy of the photo ID, and a copy of the notarized document itself).

While no process can guarantee no fraud will be successfully committed, this is a dramatic improvement over the current process — and a dramatic deterrent to a fraudster, very few of whom want to have their activities tracked and recorded on high-res audio-video.

With respect to duress, our notaries (many of whom have many years of real-life experience) tell us that this process is a dramatic improvement over their former way of performing notarial acts. As you know, duress is not something notaries are trained to detect — they are not professional psychologists. Indeed, the vast majority of states have no requirement that a notary determine that a signer is acting based on "free will." Nonetheless, all our notaries use their judgement. On our platform, they engage the signer in conversation (chit chat) to see if the signer is behaving normally. They ask if the signer understands what the signer is signing. And they ask, explicitly, if the signer is proceeding of his or her own free will. They can ask the signer to pan the camera around their room if they are concerned about anyone being nearby.

All of these interactions are fully recorded on audio-video.

At any time, if the notary is concerned, she can terminate the transaction.

The key point is that, in the current process, this entire "evaluation" of free will is done in a completely non-transparent, "black box" manner. No one has any idea what the notary asked, whether they really checked about "free will," and what kinds of behavior the signer displayed. Months or years later, if someone contested the signer's free will, the only way to "check" — in our current-day process — on what the notary did or did not do is to call the notary and the signer as witnesses and to ask their recollection, if they have any. Of course, in the current world, a signer may be being coerced by someone at home or in the car or outside the room. The notary will never know. Nor will WE ever know what the notary did to evaluate any of these issues.

Now, by contrast, we have a clear and permanent record of the entire process.

It is for this reason that audio-video recordings have now become the standard Best Practice in all trusts and estates matters, where attorney routinely video their clients signing key documents and talking about their capacity and intent — in order to create a clear record for later review, evaluation and enforcement.

C. Record-keeping, Data Security and Document Security:

In the current process, notaries keep very little in the way of records. More than half the states have no journal requirement at all, and those that do require only a paper journal with basic information: signer name, type of ID, signature, document type, etc.

In the remote notarization process, the "record" of the transaction is dramatically improved as set forth above. It contains a host of additional transaction information, plus all identity information and a copy of the photo ID, plus a copy of the document itself, plus the video of the transaction. Instead of the current system where a paper journal kept in a desk drawer (usually unlocked), in a remote notarization such as we perform the entire audio-video session is encrypted and all resulting stored data and information is then encrypted and stored in data centers using financial industry compliant security.

In the remote process, the notarized document itself is electronically signed and sealed by the notary. Full audit trail information for the signer's review and each signature is embedded in the document. The notary then applies her x.509 "digital certificate," which renders the document forever tamper-evident, so that any change, no matter how minor, will be evident to any reviewer. This is a far greater protection than in the current process, where a fraudster can take a document which has been notarized and erase, white out, modify or change elements on the document without any clear record of having done so.

D. Verifiability and Enforcement:

Any attorney who has ever had to litigate a case involving a dispute about a notarization knows that it is very difficult to find the notary, to obtain their paper journal records (which if they have a journal at all, has often been lost or damaged), to get them into court, and to have them testify about their "recollection" of an event years earlier. The entire process can be extraordinarily costly and uncertain.

In the remote notarization context, the entire transaction record, including the video and the identity validation information and other transaction information, is permanently maintained in digital format. It is all encrypted and access is protected by passwords, but it is readily available for authorized parties, attorneys, courts and law enforcement.

Moreover, the notarized document itself is retained behind these same firewalls. Accordingly, even years later, a disputed document can be compared to the digital copy of the document notarized by the notary on the day of the notarial session.

We make all this information available, on a password-protected basis, on our Verification Portal.

E. Access, Error Checking, and Security and Safety of the Notary:

First, current notarial practices provide limited access to notarial services for those in rural areas, on military deployment, on travel, with disabilities or other limitations, etc. The remote notarization process fundamentally brings notarization into alignment with the accessibility provided by the digital economy.

Second, notaries are human and make mistakes. In the current process, these mistakes can have serious consequences including invalidating important transactions. In the modern remote notarial context, systems can be put in place to error check documents before they are completed to ensure that all fields are properly and completely filled in before the document is completed and signed and sealed.

And third, many of our notaries are women. For years they have traveled into unfamiliar locations and into unknown peoples' homes to perform notarial acts. All have stories of feeling uncomfortable or unsafe. All our notaries say what a huge relief it is to be able to interact with their customers and serve their legitimate notarization needs while also feeling personally safe and secure.

F. Demo:

For those who have not seen Notarize's remote notarization process, we have a short video which provides an excellent introduction and overview of the process and its key features.

Notarize for Consumers
https://vimeo.com/182025753
Password: FutureOfNotary

Common Questions: Remote Notarization

The purpose of the notarial act is (a) to identify the signer, (b) to accept the signer's acknowledgment and (if applicable) to place the signer under oath, and (c) for the notary to complete a notarial certificate and place her seal.

In each of these functions, the remote notarization process provides dramatic improvements in identity validation, transparency and record-keeping, transaction and document security, and verifiability and enforcement.

A. Identity Validation:

Most problems with the notarial act involve identity fraud. Currently, the only tool available to the notary is visual review of an identity credential. Notaries are not expert document examiners, and sophisticated fraudsters have developed numerous ways to mock up or improperly obtain genuine-looking photo ID's. (Moreover, in a study conducted by the National Notary Association, a panel of notaries were unable to identity almost 30% of individuals from a lineup by looking at their photo ID).

In a remote notarization, a host of new technology-based tools are available to the notary to dramatically improve identity validation. In our processes, all signers go through a multi-phase identity validation process: First, their name and identity data is checked against a host of identity databases, and then they must pass a knowledge-based authentication process which uses "out of wallet" questions generated from a range of historical databases; then they must upload the front and back of an unexpired photo ID to which a software-based forensic analysis is applied (which can detect and provide the notary with information about key elements of a modern ID); then the notary herself views a high-resolution image of the photo ID and compares it to the signer to her satisfaction. If the signer fails any of these processes, or if the notary does not feel comfortable with the ID or the individual , the notary can terminate the transaction at any time.

B. Duress and Coercion — Transparency and Record-Keeping:

Not only must the signer passes the above identity validation processes, but the entire notarial transaction itself is conducted in a real-time audio-video session where the signer and notary can see and hear each other throughout and also can see each others' actions on the subject document at the same time, together. The entire audio-video session is recorded, as is all the key transaction information about

the session (geo-location, IP address, identity validation information, a copy of the photo ID, and a copy of the notarized document itself).

While no process can guarantee no fraud will be successfully committed, this is a dramatic improvement over the current process — and a dramatic deterrent to a fraudster, very few of whom want to have their activities tracked and recorded on high-res audio-video.

With respect to duress, our notaries (many of whom have many years of real-life experience) tell us that this process is a dramatic improvement over their former way of performing notarial acts. As you know, duress is not something notaries are trained to detect — they are not professional psychologists. Indeed, the vast majority of states have no requirement that a notary determine that a signer is acting based on "free will." Nonetheless, all our notaries use their judgement. On our platform, they engage the signer in conversation (chit chat) to see if the signer is behaving normally. They ask if the signer understands what the signer is signing. And they ask, explicitly, if the signer is proceeding of his or her own free will. They can ask the signer to pan the camera around their room if they are concerned about anyone being nearby.

All of these interactions are fully recorded on audio-video.

At any time, if the notary is concerned, she can terminate the transaction.

The key point is that, in the current process, this entire "evaluation" of free will is done in a completely non-transparent, "black box" manner. No one has any idea what the notary asked, whether they really checked about "free will," and what kinds of behavior the signer displayed. Months or years later, if someone contested the signer's free will, the only way to "check" — in our current-day process — on what the notary did or did not do is to call the notary and the signer as witnesses and to ask their recollection, if they have any. Of course, in the current world, a signer may be being coerced by someone at home or in the car or outside the room. The notary will never know. Nor will WE ever know what the notary did to evaluate any of these issues.

Now, by contrast, we have a clear and permanent record of the entire process.

It is for this reason that audio-video recordings have now become the standard Best Practice in all trusts and estates matters, where attorney routinely video their clients signing key documents and talking about their capacity and intent — in order to create a clear record for later review, evaluation and enforcement.

C. Record-keeping, Data Security and Document Security:

In the current process, notaries keep very little in the way of records. More than half the states have no journal requirement at all, and those that do require only a paper journal with basic information: signer name, type of ID, signature, document type, etc.

In the remote notarization process, the "record" of the transaction is dramatically improved as set forth above. It contains a host of additional transaction information, plus all identity information and a copy of the photo ID, plus a copy of the document itself, plus the video of the transaction. Instead of the current system where a paper journal kept in a desk drawer (usually unlocked), in a remote notarization such as we perform the entire audio-video session is encrypted and all resulting stored data and information is then encrypted and stored in data centers using financial industry compliant security.

In the remote process, the notarized document itself is electronically signed and sealed by the notary. Full audit trail information for the signer's review and each signature is embedded in the document. The notary then applies her x.509 "digital certificate," which renders the document forever tamper-evident, so that any change, no matter how minor, will be evident to any reviewer. This is a far greater protection than in the current process, where a fraudster can take a document which has been notarized and erase, white out, modify or change elements on the document without any clear record of having done so.

D. Verifiability and Enforcement:

Any attorney who has ever had to litigate a case involving a dispute about a notarization knows that it is very difficult to find the notary, to obtain their paper journal records (which if they have a journal at all, has often been lost or damaged), to get them into court, and to have them testify about their "recollection" of an event years earlier. The entire process can be extraordinarily costly and uncertain.

In the remote notarization context, the entire transaction record, including the video and the identity validation information and other transaction information, is permanently maintained in digital format. It is all encrypted and access is protected by passwords, but it is readily available for authorized parties, attorneys, courts and law enforcement.

Moreover, the notarized document itself is retained behind these same firewalls. Accordingly, even years later, a disputed document can be compared to the digital copy of the document notarized by the notary on the day of the notarial session.

We make all this information available, on a password-protected basis, on our Verification Portal.

E. Access, Error Checking, and Security and Safety of the Notary:

First, current notarial practices provide limited access to notarial services for those in rural areas, on military deployment, on travel, with disabilities or other limitations, etc. The remote notarization process fundamentally brings notarization into alignment with the accessibility provided by the digital economy.

Second, notaries are human and make mistakes. In the current process, these mistakes can have serious consequences including invalidating important transactions. In the modern remote notarial context, systems can be put in place to error check documents before they are completed to ensure that all fields are properly and completely filled in before the document is completed and signed and sealed.

And third, many of our notaries are women. For years they have traveled into unfamiliar locations and into unknown peoples' homes to perform notarial acts. All have stories of feeling uncomfortable or unsafe. All our notaries say what a huge relief it is to be able to interact with their customers and serve their legitimate notarization needs while also feeling personally safe and secure.

F. Demo:

For those who have not seen Notarize's remote notarization process, we have a short video which provides an excellent introduction and overview of the process and its key features.

Notarize for Consumers
https://vimeo.com/182025753
Password: FutureOfNotary

SIGNiX

WHY REMOTE E-NOTARIZATIONS ARE THE WAY OF THE FUTURE.

Company Name Gives You Power To Create Something Beautiful

hy Remote E-
otarizations are
ıe Way of the

< PREVIOUS NEXT >

Future ...

PROJECT INFO

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum maximus, tellus ut dictum luctus, sem mauris tristique orci, ac sagittis diam est vitae magna.

CLIENT: John Doe

PROJECT URL: www.clickray.eu

CATEGORY: Classic

After decades of the traditional, inconvenient, paper-laden approval process, official notarizations are now being performed electronically and remotely. And the technology behind it all is starting to gain national attention by some of the biggest names in the notary, finance and government industries.

The National Notary Association (NNA) recently published a white paper about the growing support for e-notarization and how it works. (And to demonstrate the remote e-notarization process for white paper readers, the NNA featured SIGNiX's demo video of a remote e-notarization.)

According to the NNA's white paper, several influential industry organizations have voiced their support of e-notarization technology, especially in the mortgage finance industry. In 2015, the Consumer

Contact Us!

No one rejects, dislikes, or avoids pleasure itself because it is pleasure.

GET IN TOUCH

Financial Protection Bureau stated that electronic loan closings are beneficial to consumers. And in 2016, Fannie Mae, Freddie Mac and Quicken Loans endorsed the use of both e-notarization and remote e-notarization. In a joint statement, Fannie Mae and Freddie Mac—government-sponsored enterprises in the mortgage financing market—concluded that the technology would improve "the assurance, authentication, security and documentation of notarial acts."

And these are only a handful among others. The National Association of Secretaries of State, the Electronic Signature & Records Association and the American Land Title Association are among the many others that are opening up conversations about e-notarization, remote e-notarizations and their potential benefits for an increasingly digitally focused society.

Why the momentum?

Because remote e-notarizations offer a host of benefits—including security, efficiency, cost savings and the freedom to notarize documents on-demand.

"Electronic and remote webcam notarization systems can transform your business processes by creating new efficiencies reliably and securely." – National Notary Association

Remote e-notarizations are highly secure and help mitigate the risk of forgeries by requiring the signer to verify his identity and the notary to archive the audio-video recording of the notarization. Businesses that offer remote e-notarization are able to give their clients a secure, convenient method to have documents notarized electronically, which in turn reduces paper usage, eliminates the need for paper storage and saves money. Remote e-notarizations are also a big time-saver for both signers and notaries as the approval process can be completed from anywhere with an internet connection.

Because the traditional requirement of physically appearing before a

notary is replaced by *digitally appearing* before a notary, extra security procedures have been put in place to ensure the signer is who he says he is. For example, knowledge-based authentication (KBA) presents questions to the signer based on information found in 30 years of public records, such as details from credit reports, town hall records, public health records and more. The signer must answer a certain number of questions correctly within a designated amount of time to verify his identity and be permitted to access and sign the document.

Electronically notarized documents also come with a unique layer of security that traditional paper-based notarizations simply don't have. If an individual ever alters a document, tamper-evident technology found in digital signatures, or Independent E-Signatures™, will immediately identify the suspicious activity. Additionally, each signed document is accompanied by a complete audit trail, which indicates the date and time a document was signed, the signer's IP address and more. This ensures that the evidence of a signature is captured and fully accessible for years to come.

For a deeper analysis of e-notarization and remote e-notarization, be sure to read the NNA's white paper about this emerging technology. Highlights of the white paper include:

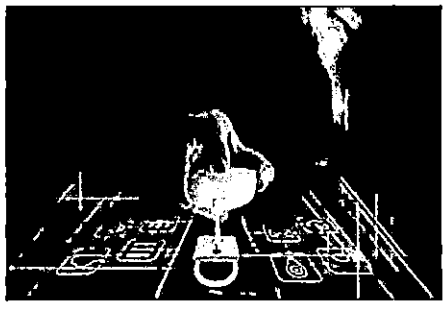
- ☐ Essential elements of paper-based and electronic notarizations
- ☐ Benefits of e-notarization
- ☐ Benefits of remote e-notarization

Ready to make your move to remote e-notarization? Click here to get a free quote!

2018 was a watershed year for data and network security

Sponsored Content Jan 3, 2019

Data breaches and identity theft are now everyday events. That state of affairs doesn't make them any less dangerous, distasteful and annoying. However, most people with an online footprint understand that at some point in their lives they are going to be the victim of an internet crime, that is, if they have been fortunate enough to avoid it to this point.



IPOPBA
Implemented in May 2018, the GDPR is the clearest, most comprehensive and forceful statement yet by a government entity regarding an individual's rights to his or her own personal data.

What made 2018 different was seeing the pendulum begin to swing toward a new approach to privacy rights and a disruption of the digital status quo. There were several significant events and tipping points that marked 2018 as an important year in the history of cyberspace.

The General Data Protection Regulation (GDPR). As the first transnational attempt to regulate the processing and movement of personal data, the European Union's GDPR was truly a landmark piece of regulation. Implemented in May 2018, the GDPR is the clearest, most comprehensive and forceful statement yet by a government entity regarding an individual's rights to his or her own personal data. The GDPR squarely puts the regulatory burden of maintaining these rights on the back of business enterprises engaged in handling data and allows for substantial penalties if such burdens are not met. Notably, the GDPR implements a comprehensive framework within its member countries for the commercialization of personal data by:

Providing a robust definition of what constitutes personal data.
Establishing national supervisory authorities to enforce GDPR.
Establishing the parameters for lawful data processing.
Mandating that data controllers establish default procedures and processes that allow for the highest possible degree of data privacy.
Establishing additional individual data privacy rights, such as the right to access one's own data and

the 'right to erasure'.
Establishing uniform data breach protocols.
Establishing the ability to impose substantial sanctions upon companies for failure to comply with the law.

As one might imagine, the GDPR received a decidedly less enthusiastic response from some in the U.S. business community, many of whom felt that the regulations were aimed at reining in the power and dominance of U.S.-based businesses. This charge is not altogether untrue, especially given Europe's fitful embrace of economic nationalism. However, GDPR's significance far outstrips such provincial concerns and, given the global nature of data-intensive businesses, is already having an impact on the way data is collected, handled, stored and commercialized.

California Consumer Privacy Act. One such follow-on event to the GDPR is the new California Consumer Privacy Act, signed into law in July 2018. It is one of the first state-level attempts in the U.S. to articulate individual rights regarding the collection and use of personal data. Similar to the GDPR, the law establishes four basic rights:

A right to know what personal data has been collected, where it was sourced, and to whom it has been disclosed and for what uses.
An opt-out right to disallow third-party use purchase and use of personal information.
A right to erasure that compels businesses to delete personal information upon request.
A right to equable pricing of services despite the assertion of the rights listed above.

The similarities of the California law with the GDPR are noteworthy and provide some reason to believe that the GDPR has started a snowball of momentum in setting the parameters for the data privacy conversation.

Evolving Discourse on Data Privacy. Partly due to the GDPR, this past year witnessed a stark change in the tone and substance of how we talk about data privacy. Until 2018, the bedrock principle of how the "free" internet operated was largely unchallenged in mainstream discourse. That is, people largely accepted that, in order to access the plethora of free services online, the providers of those services collected personal data and commercialized it. But the GDPR has changed this balance in Europe and it will be interesting to see whether these norms required by the GDPR continue to proliferate across the globe, particularly in view of the continuing exposures of data breaches involving personal data.

There have been many recent high-profile disclosures of misappropriation of data, namely Facebook (including its Cambridge Analytica revelations), Marriott, MyFitnessPal, and even the U.S. Postal Service. There are also continuing inquiries into the use of personal data to target social media messages to users in order to interfere in the 2016 U.S. electoral cycle. These politically charged events — in concert with daily revelations of data mishandling — have led to a reappraisal of the free internet business model and have underscored the rapid implementation of data privacy regulation.

Striking the Right Balance. The GDPR by itself would have caused a global re-evaluation of the competing rights of business enterprises and individuals, but the context into which the GDPR (the regulations were adopted two years ago) came to life, and the continued exposure of personal information through data breaches, have reinforced the notion that something important has changed in consumers' approach to data privacy.

We have reached, it seems, an inflection point, and the conversation to follow will likely be more serious and practical than those that came before, particularly in view of the expanded data collection

necessary to realize the benefits offered through the internet of things and the proliferation of connected devices. Given that we have only scratched the surface of what is possible in the wired and networked world we have created—a world in which our devices speak to one another in a language we cannot hear, generating even more data—the turn toward informed and serious conversation as to how to protect individuals while also recognizing important commercial benefits that support continued innovation was long overdue.

See highlights on Pg. 2

DRAFT AMENDMENT TO SECTION 14A OF THE REVISED UNIFORM LAW ON NOTARIAL ACTS

Purposes and Issues

The Draft: This proposed amendment to the Revised Uniform Law on Notarial Acts authorizes notaries public to perform notarial acts in the state in which they are commissioned for remotely located individuals using audio-visual communication technology regardless of where the individual may be located. This amendment is not limited to foreign located individuals; it extends the authority to any remotely located individuals.

This amendment was prepared in response to a rapidly emerging trend among the states to authorize the performance of notarial acts by means of audio-visual technology. Currently such laws are in effect in Indiana, Minnesota, Montana, Ohio, North Dakota, Tennessee, Texas, and Virginia, and have been introduced for consideration in at least 12 other states and the District of Columbia. The ability of notaries public to perform notarial acts by audio-visual technology is being promoted by the American Land Title Association and the Mortgage Bankers Association. They have prepared a Model On-Line Notary Act which contains provisions very similar to these RULONA amendments, but which are not incorporated into the framework of RULONA.

Purpose: Traditionally an individual has been required to physically appear before a notary public in order for a notary public to perform a notarial act on behalf of that individual. The objectives of that appearance have been to enable the notary public to verify the identity of the individual and to assess the competency of the individual and whether the individual's acts are knowingly and voluntarily made. In recent years, technology and commercially available identification services have made it possible to accomplish these goals by means of synchronous communication technology, thus allowing the performance of notarial acts for persons who are not in the physical presence of a notary public. This amendment authorizes notaries public to perform notarial acts for remotely located individuals using communication technology provided its requirements have been fulfilled.

Summary of amendment: Subsection (b) provides that an individual may appear before a notary public by means of communication technology and thereby comply with the provisions of RULONA Section 6 calling for appearance before the notary public. Subsection (a)(1)(A) defines communication technology as any means or process that allows a notary public and a remotely located individual to communicate with each other simultaneously by sight and sound. This definition would allow a notary public and a remotely located individual, both of whom have and employ video screens with microphones and speakers, to comply. Inasmuch as communication technology will undoubtedly grow and change in future years, specific technology is not identified in the amendment. When necessary and consistent with other applicable law, communication technology also permits the use of alternative or additional devices or processes that facilitate communication with a remotely located individual who has a vision, hearing, or speech impairment. Subsections (h)(1), (2), and (3) authorize a commissioning officer to adopt rules prescribing the means of performing such a notarial act, establish standards for communication technology, and establish requirements or procedures for approving the providers of communication technology.

Subsection (c)(1) specifies the means by which a notary public must identify a remotely located individual. Subsection (c)(1)(A) permits a notary public to identify a remotely located individual by personal knowledge as provided in Section 7(a) of RULONA.

Subsection (c)(1)(B) permits a notary public to identify a remotely located individual from satisfactory evidence provided by the oath or affirmation of a credible witness. The witness may physically appear before the notary public and execute the oath or affirmation as provided in Section 7(b) of RULONA. The remotely located witness also may appear before a notary public by means of communication technology. In that case, the witness is subject to the same identification and other requirements as a remotely located individual.

Subsection (c)(1)(C) permits a notary public to identify a remotely located individual by at least two different types of identity-proofing processes or services. Although identity proofing continues to evolve, with today's technology it involves a third-party service provider who is able to verify the identity of an individual by a review of personal information from public or private sources (see subsection (a)(3)). This may include having a remote individual answer a number of questions for which there is a very high probability that only the true individual would be able to answer correctly. The third-party service provider might also use technology such as biometric identification technology or credential analysis. Subsections (h)(2) and (3) authorize, but do not require, the commissioning officer to establish standards for identity proofing and requirements and procedures to approve providers of identity proofing.

The Drafting Committee considered, but rejected, suggestions that the legislation should not take effect until standards are adopted by a state. Some of the Committee's advisors representing state agencies objected to a mandate to develop such standards. The Committee also concluded that processes being utilized under current standards to identify remotely located individuals may better and more reliably identify persons than occurs in face-to-face notarizations which rely on tangible identity credentials that may be fraudulent. Standards have been adopted by the National Association of Secretaries of State [NASS] and technical standards are being drafted by MISMO, the Mortgage Industry Standards Maintenance Organization.

Subsection (c)(2) requires that the notary public be reasonably able to identify the record before the notary public as the same record in which the remotely located individual made a statement or on which the remotely located individual executed a signature. For example, a notary public might compare a record she or he has with the record the remotely located individual displays on the video screen. Or the notary public may verify the record by means of a secure electronic signature tied to an electronic record which he or she is notarizing.

Subsection (c)(3) requires that an audio-visual recording of the performance of the notarial act be created. Subsection (f) requires that the notary public or his or her representative retain the audio-visual recording for a period of at least 10 years or as otherwise required by rule of the commissioning officer or agency under subsection (h)(4).

The Drafting Committee considered, but rejected, suggestions that these recordings and other material relating to the performance of notarial acts by means of audio-visual communication be protected from any disclosure or use by the remotely located individual. The Committee concluded that drafting confidentiality requirements for personal information was outside of its scope of authority and presented difficult issues that apply not only to notarial acts

performed by means of communication technology, but also to face-to-face notarial acts. Action on the rejected suggestion also would require analysis of whether action at the state or federal level would have to address the European Union's recent implementation of the General Data Protection Rule.

Subsection (c)(4) deals with a remotely located individual who is located outside the United States. It sets forth essentially the same requirements as were contained in the 2016 amendment to RULONA.

Subsection (d) provides that the certificate of notarial act required under Section 15 must indicate that a notarial act performed in accordance with this Section was done by means of communication technology. Subsection (e) provides that a short-form certificate set forth in Section 16 complies with this requirement if it contains language substantially as follows: "This notarial act involved the use of communication technology." Under subsection (h)(1), the commissioning officer or agency may adopt rules setting other requirements for the certificate.

Before a notary public may perform her or his first notarial act under this Section, subsection (g) requires that the notary public must notify the commissioning officer or agency that the notary public will be performing notarial acts facilitated by communication technology and identify the technology. If the commissioning officer has adopted standards for the approval of communication technology or identity proofing, the communication technology or identity proofing must comply with those standards.

The Drafting Committee considered, but rejected, recommendations that all technologies used in the performance of notarial acts by means of communication technology should first be reviewed and approved by the commissioning officer or agency. The Committee concluded that because technologies used for performance of notarial acts involving electronic records and signatures do not require state approval, a mandate for prior approval should not be imposed on technologies used in the performance of notarial acts using communication technology, which will in most cases involve the use of electronic records and signatures. In addition, the Committee concluded that the proposed legislation provides adequate authority for states to adopt rules requiring the approval of technologies if they believe approval is necessary to prevent the use of inappropriate technologies.

Subsection (h) provides that the commissioning officer may adopt rules regarding the performance of notarial acts for remotely located individuals in addition to those authorized in Section 27. Subsection (i) provides that before adopting, amending, or repealing a rule governing the performance of a notarial act regarding a remotely located individual the commissioning officer or agency must consider the most recent standards promulgated by national standard-setting organizations and the National Association of Secretaries of State; the standards, practices, and customs of other jurisdictions that have laws substantially similar to this Section; and the views of governmental officials and entities and other interested persons.

DRAFT AMENDMENT TO SECTIONS 4 AND 20 OF THE REVISED UNIFORM LAW ON NOTARIAL ACTS

Purposes and Issues

Draft: These two subsections, in combination, allow a notarial officer to certify that a tangible or paper copy of an electronic record is an accurate copy of an electronic record and authorize the recorder to accept that tangible or paper copy for recording.

Purposes: Since the promulgation of the Uniform Electronic Transactions Act, the Uniform Real Property Electronic Recording Act, and the Revised Uniform Law on Notarial Acts, the use of electronic records has increased considerably. Many of these records involve transactions that must or should be recorded in the local land records office. However, in many cases, local recorders are not equipped or authorized to accept electronic records. These subsections allow a notarial officer to certify that a tangible or paper copy of a record is an accurate copy and authorize the recorder to accept this "papered-out" copy for recording.

Summary of amendment: Section 4(c) allows a notarial officer to certify that a tangible or paper copy of an electronic record is an accurate copy of the electronic record. The notarial officer may be the same notarial officer who performed the notarial act regarding the electronic record or another notarial officer who has the ability to read the electronic record and compare it with the tangible or paper copy.

Section 20(c) authorizes the local recorder to accept the tangible or paper copy of the electronic record for recording. The "papered-out" copy satisfies any requirement that a record be an original in order to be recorded.

https://www.notarypublicstamps.com/articles/notary-journals-raise-issues-about-public-records-versus-privacy-/

Notary Journals Raise Issues about Public Records versus Privacy

Tuesday, July 28, 2015 by American Association of Notaries

Notaries public have access to many items of personal information in order to do a proper job of notarizing. We have to see the entire document to make sure the signer is able to freely and willingly sign. We have to briefly review the document to gather some specifics to record in our notary journals. We have to examine the satisfactory evidence presented that establishes the identity of the signer and record details of that evidence in our journals. Other specific information about the circumstances of the notarization (as covered in other articles in this series) has to be written into the journal as well.

While the notary may forget the details of the notarization as time passes, whatever the notary has written in her notary journal becomes her official record of her acts as a notary. So much legal weight is given to the information recorded in the notary journal that it is considered prima facie evidence, which means it is presumed to be true unless proven otherwise. A growing number of states have passed statutory laws requiring that their notaries public keep an official record and many more have rules or laws on how the journals will be handled or disposed of, yet very few have addressed the issue of privacy.

Are notary journals a public record subject to state or federal freedom of information act requests? Are they private business records subject to the myriad array of state and federal laws dealing with privacy? Or are they something in between?

Among the more well-known federal laws that contain privacy provisions, the list includes the Graham-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Privacy Act, the Privacy Protection Act, and the Freedom of Information Act. Many others apply in specific instances or regulate specific industries or commercial or government practices.

The Consumer Privacy Guide lists 27 federal statutes that protect the privacy of consumers in specific instances. Robert Ellis Smith, attorney and publisher of the **Privacy Journal** has written a book that lists more than 800 federal and state privacy laws as of 2013 -- and he has stated that more than 60 laws on the topic were passed within the 12 months after that book was published.

While European law gives consumers broad rights over their personal

information and these rights apply across the board, the USA follows a more piecemeal approach. Unless you are a specialist in privacy law, the American approach means that you are very unlikely to know when the privacy rights of your signers or other parties may be a legal issue.

It would be helpful if state governments examined the issue of public access to official records versus the public's right to privacy as set forth in state and federal law as these issues relate to notary journals and notary practices in general, especially if such an examination led to specific rules to guide us notaries in the performance of our duties.

Unfortunately, only a few states have even addressed the issue of who may access the notary journal, let along other privacy concerns. If you are commissioned in Arizona, California, Hawaii, Maryland, Massachusetts, Mississippi, Nevada, or Texas, contact your Secretary of State's office to see what the rules are for access to notary journals in your state.

Those of us in the other 42 states may need to take this matter up with our respective state legislators. Meanwhile, we should probably treat all the information in our journals as we would want our own information to be treated: consider it private unless ordered by a court to release it.

If you need a notary journal, please see the store at **http://www.notarypublicstamps.com**.

This article is part of the series that began with ***What Does a Notary Public Do?***

-- **Tim Gatewood** is a Contributing Writer with the American Association of Notaries

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Financial Institutions and Customer Information: Complying with the Safeguards Rule

TAGS: Credit and Finance | Privacy and Security | Gramm-Leach-Bliley Act | Finance
RELATED RULE: Safeguards Rule

Under the Safeguards Rule, financial institutions must protect the consumer information they collect. Learn if your business is a "financial institution" under the Rule. If so, have you taken the necessary steps to comply?

Many companies collect personal information from their customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Gramm-Leach-Bliley (GLB) Act requires companies defined under the law as "financial institutions" to ensure the security and confidentiality of this type of information. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. But safeguarding customer information isn't just the law. It also makes good business sense. When you show customers you care about the security of their personal information, you increase their confidence in your company. The Rule is available at ftc.gov.

Who Must Comply?

The definition of "financial institution" includes many businesses that may not normally describe themselves that way. In fact, the Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The Safeguards Rule also applies to companies like credit reporting agencies and ATM operators that receive information about the customers of other financial institutions. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

For more information on whether the Safeguards Rule applies to your company, consult section 313.3(k) of the GLB Privacy Rule and the Financial Activities Regulations. Both are available at www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/privacy-consumer-financial-information.

How To Comply

The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are designed to be flexible. Companies should implement safeguards appropriate to their own circumstances. For example, some companies may choose to put their safeguards program in a single document, while others may put their plans in several different documents — say, one to cover an information technology division and another to describe the training program for employees. Similarly, a company may decide to designate a single employee to coordinate safeguards or may assign this responsibility to several employees who will work together. In addition, companies must consider and address any unique risks raised by their business operations — such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network.

Securing Information

The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: Employee Management and Training; Information Systems; and Detecting and Managing System Failures. One of the early steps companies should take is to determine what information they are collecting and storing, and whether they have a business need to do so. You can reduce the risks to customer information if you know what you have and keep only what you need.

Depending on the nature of their business operations, firms should consider implementing the following practices: Employee Management and Training. The success of your information security plan depends largely on the employees who implement it. Consider:

- Checking references or doing background checks before hiring employees who will have access to customer information.

- Asking every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.
- Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
- Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.)
- Using password-activated screen savers to lock employee computers after a period of inactivity.
- Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.
- Training employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
    - Locking rooms and file cabinets where records are kept;
    - Not sharing or openly posting employee passwords in work areas;
    - Encrypting sensitive customer information when it is transmitted electronically via public networks;
    - Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
    - Reporting suspicious attempts to obtain customer information to designated personnel.
- Regularly reminding all employees of your company's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.
- Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
- Imposing disciplinary measures for security policy violations.
- Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

Information Systems. Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal:

- Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:
    - Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.
    - Store records in a room or cabinet that is locked when unattended.
    - When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and is kept in a physically-secure area.
    - Where possible, avoid storing sensitive customer data on a computer with an Internet connection.

- Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area.
- Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.

- Take steps to ensure the secure transmission of customer information. For example:
  - When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit.
  - If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
  - If you must transmit sensitive data by email over the Internet, be sure to encrypt the data.
- Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule. For example:
  - Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
  - Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.
  - Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.

  Detecting and Managing System Failures. Effective security management requires your company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:

- Monitoring the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses.
- Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:
  - check with software vendors regularly to get and install patches that resolve software vulnerabilities;
  - use anti-virus and anti-spyware software that updates automatically;
  - maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations;
  - regularly ensure that ports not used for your business are closed; and
  - promptly pass along information and instructions to employees regarding any new security risks or possible breaches.
- Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to:
  - keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;
  - use an up-to-date intrusion detection system to alert you of attacks;

- monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
- insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.

- Taking steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs:
  - take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet;
  - preserve and review files or programs that may reveal how the breach occurred; and
  - if feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.
- Considering notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:
  - notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;
  - notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
  - notify the credit bureaus and other businesses that may be affected by the breach. See Information Compromise and the Risk of Identity Theft: Guidance for Your Business; and
  - check to see if breach notification is required under applicable state law.

For More Information

Additional guidance is available at www.ftc.gov/privacy/glbact. Resources at that site may alert you to new risks to information security and give people whose information may have been compromised important first-things-first advice for responding. Visit www.onguardonline.gov for information that can help you train your employees in safe computing practices on the job and at home. In addition, the following organizations have information to help you implement appropriate safeguards for your customer data:

- Computer Security Resource CenterNational Institute for Standards and Technology (NIST) http://csrc.nist.gov
- National Strategy to Secure Cyberspace, Department of Homeland Security http://www.dhs.gov/files/publications/editorial_0329.shtm
- The SysAdmin, Audit, Network, Security (SANS) InstituteThe Twenty Most Critical Internet Security Vulnerabilities www.sans.org/top20
- United States Computer Emergency Readiness Team (US CERT) www.us-cert.gov/resources.html
- Carnegie Mellon Software Engineering Institute CERT Coordination Center www.cert.org

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

April 2006

ftc.gov