FIDELITY NATIONAL TITLE GROUP

Pacific North West Field Compliance

Background Check: General Information and Requirements

FNTG's policy is that all independent contract notary vendors must successfully pass a criminal background check as a prerequisite to being added to the FNTG approved notary list with a re-check annually. This policy also supports many of our Lender/Client Service Agreements which require FNTG to obtain a clear criminal background check from each independent contract notary vendor.

A criminal background check is required for each individual notary and each individual is responsible for the cost of each background check. Below are the options and the requirements:

- National Notary Association (NNA) Background Check Certification (dated within 1 year). Upon submission of the certification to FNTG from the notary, FNTG will access the certification via the NNA website to confirm its authenticity. Visit www.nationalnotary.org or contact the NNA at 800-876-6827 for a copy of the certificate**;** OR
- Sterling Info Systems Criminal Background Check ordered through the FNTG approved portal.

If not obtaining the NNA background check, the only acceptable background check company is Sterling.

ORDER INSTRUCTIONS

To insure the proper routing of your background check results to the appropriate FNTG employee, please insure you are using the proper portal link below. These instructions are for notaries obtaining a background check for operations in Division Two and Three, which encompasses California (north of Santa Barbara) Washington, Oregon, Idaho, Hawaii, and Montana. Although your background check will be processed for this division, your addition to the approved notary list will extend throughout the country.

Go to: https://workforce.sterlingdirect.com/InvitationCodePage?InvitationCode=BDF0AA3299324D-9AF70398 leave in the invitation code provided and simply click "begin" to start. At the next screen, you will have to "create an account". Thereafter, follow the on-screen instructions provided.

FNTG has confirmed that Sterling Info Systems is an independent and qualified background check vendor. FNTG does not have any ownership interest in the vendor nor does FNTG receive any fee split, referral fee or other compensation from the vendor or its fees.

Please be certain to enter all of your information accurately, you will receive instructions about retrieving a copy of your background check for your records during the application process. The cost of the background check will range from $55 and up depending on the states that you have resided in within the last 7-10 years. You do not need to send FNTG a copy of the report. The background check reports include the following 10 year searches:

- Social Security Number Trace Search
- County Criminal Court Search
- Statewide Criminal Search
- Federal District Criminal Search
- National Sex Offender Database Search
- Enhanced National Criminal Database Search (with Validators)
- OFAC/Patriot Act Search (Office of Foreign Asset Control)
- Federal Excluded Parties List System (EPLS/LDP)

_____ _____

Signature Date

_____ _____

Print Name Background Check Vendor used

NOTICE, AUTHORIZATION AND RELEASE REGARDING EXISTING CERTIFICATES AND/OR INVESTIGATIVE CONSUMER REPORTS

I have or will provide to Fidelity National Financial, Inc. and/or its family of title companies (collectively, "FNF") a copy of my Background Screening Certificate from the GLBA-Compliant National Notary Association ("NNA") or other approved vendor.

I HEREBY AUTHORIZE FNF to release, disclose and/or provide a copy of any and all certificates, forms, questionnaires, investigative reports, background checks, evaluations, analysis or any other information that I have provided or caused to be provided to FNF, or which FNF has prepared, to any lender, bank, credit union, savings association or other financial institution (collectively, "Lender") for whom FNF provides services under a service agreement, so as to evidence that I meet the requirements, qualifications and standards imposed by such Lender on persons who receive or have access to consumer financial information or other confidential information.

I hereby agree and understand that this Notice, Authorization and Release will remain valid as long as I provide any services for or to FNF and throughout my affiliation with FNF. The matters and information which are covered by this Notice, Authorization and Release include, but are not limited to, information concerning my criminal history, motor vehicle history, my social security number, or any other information requested by a Lender. As used herein FNF means FNF and any other division of the Fidelity National Financial, Inc. family of companies, including any related companies, subsidiaries and/or affiliates thereof.

I hereby release FNF, to the full extent permitted by law, from any liability or claims arising from releasing, disclosing, providing and/or reporting information concerning me to any party pursuant to this Notice, Authorization and Release.

I agree that a copy or fax of this document shall be as valid as the original.

_____ _____

Signature Date

_____

Print Name

_____

City, State & Zip

FIDELITY
NATIONAL TITLE GROUP

FNTG NOTARY PUBLIC'S PROFESSIONAL RESPONSIBILITY & REQUIREMENTS AGREEMENT

Fidelity National Title Group, Inc. and its affiliated companies (collectively, "FNTG" or "Company") are committed to protecting the privacy of its clients and customers and avoiding fraud. Although your notary services are governed by state law, FNTG has developed the following general requirements, which notaries must adhere to while providing services to or at the request of the Company.

1. Notary shall hold a current notary commission for each state in which Notary performs the notary services, and Notary must have a current understanding of the laws, practices, and requirements of the state's notarial office by obtaining any necessary training to do so.

2. Notary shall maintain errors and omissions insurance with coverage of not less than $100,000.00. Notary shall renew such coverage prior to the expiration date, and Notary understands they will not be able to provide services to the Company until such renewal documents are received by the Company.

3. Notary is required to conduct all services in a professional and courteous manner. Notary shall wear business attire and otherwise maintain a professional appearance during a signing appointment.

4. From time to time, the Company may develop required training courses for independent notaries. Company may condition assignment of new orders to Notary upon Notary's completion of the required training course(s). Training requirements of the Company are in addition to any training requirements of the states in which Notary is commissioned.

5. Notary shall not use or be under the influence of drugs or alcohol before or during a signing appointment.

6. Notary shall not carry a firearm to a signing appointment.

7. Notary shall be responsible for ensuring that the signing party(ies) sign, initial and otherwise complete all documents. Notary is responsible for correcting, at his/her own expense, any notarized, executed, or initialed documents that the Company determines be incomplete or unsatisfactory.

8. Notary shall act as an impartial third party and shall not profit or gain from any document or transaction requiring his/her services other than by the fee earned for such services as allowed by statute and agreed upon by the Company.

9. Notary shall not execute a false or incomplete certificate nor be involved with any document or transaction that he/she knows is false, fraudulent or deceptive.

10. Notary shall safeguard his/her seal and notary journal (if such journal is required by state law or maintained at the option of the notary) at all times to prevent unauthorized use of such seal and/or journal.

11. Notary shall not notarize any documents that a signing party did not sign in the presence of the Notary. The notary must personally observe the execution of each document by the signing party and notarize the documents in the signing party's presence.

12. Notary shall maintain the privacy of each signer and not divulge or use any personal, confidential or proprietary information to which the Notary may have access while performing the services, all as more particularly described in and controlled by the FNTG Third-Party Notary Confidential Information Agreement executed by Notary.

13. Notary, as a government officer and public servant, shall serve the public in an honest, fair, and unbiased manner. Notary shall give precedence to state law over the expectations of any individual or entity.

14. Notary shall not give advice to any signatory. If the signing party asks you any substantive questions regarding the transaction or the content of the documents signed or to be signed, the Notary must refer the signing party back to the Company escrow officer or Company personnel designated in the closing package transmittal.

15. Notary shall only accept documents for signing directly from the Company escrow officer or Company personnel designated in the closing package transmittal; Notary shall never accept documents from a mortgage broker, realtor or anyone else without first obtaining the approval of the Company escrow officer or other Company personnel designated in the closing package transmittal.

16. At the Company's request, Notary may accept a cashier's checks or other such negotiable instrument from a signing party; provided that the check or instrument is made payable to the FNTG entity closing the transaction. NOTARY IS PROHIBITED FROM HANDLING ANY FUNDS, ESCROW OR OTHERWISE.

17. Notary shall at all times keep any and all documents and information safe and secure in his/her possession.

18. Upon completion of the signing, Notary shall promptly return the original, executed documents in accordance with the instructions set forth in the transmittal letter from the Company. If the Company requires the Notary to send an electronic copy of the signed documents back to the Company, Notary shall not email documents unless Notary has the ability to send encrypted emails or to encrypt the scanned documents. If Notary is unable to send encrypted emails or to encrypt the documents, Notary shall contact the Company to discuss options for secure, electronic transmission of the documents.

19. Notary shall not subcontract the signing services to another notary. If Notary is personally unable to complete the notary service, Notary shall immediately contact the Company escrow officer or other designated Company personnel to allow the Company to select a new notary.

20. Notary shall not use FNTG or Affiliates' names, logos or other marks, or any abbreviation, contraction or simulation thereof, in any advertising, publicity, websites or other marketing materials, whether printed or digital. Notary shall not represent themselves as being approved or endorsed by FNTG or its Affiliates.

21. IN THE EVENT OF A BREACH OR SUSPECTED BREACH IN SECURITY (LOSS AND/OR IMPROPER DISCLOSURE OF DOCUMENTS OR CUSTOMER INFORMATION), WHETHER PHYSICAL OR ELECTRONIC, THE NOTARY SHALL IMMEDIATELY ADVISE THE COMPANY ESCROW OFFICER OR OTHER COMPANY PERSONNEL DESIGNATED IN THE CLOSING PACKAGE TRANSMITTAL OF SUCH BREACH AS REQUIRED BY THE FNTG THIRD-PARTY NOTARY CONFIDENTIAL INFORMATION AGREEMENT, SO FNTG CAN PROMPTLY ADDRESS SUCH BREACH OR SUSPECTED BREACH.

By signing below, I hereby certify that:

I have read, understand and agree to comply with the above responsibilities and requirements (the "Requirements"), and I acknowledge that my performance as a Notary Public ("Notary") on FNTG and its Affiliates transactions will be monitored by FNTG for compliance with the Requirements. I understand that my Failure to comply with these Requirements, the FNTG Third-Party Confidential Information Agreement or FNTG's transactional instructions may result in my removal from FNTG's approved notary network. Further, if I fail to provide proof to the Company of the renewal of my commission, E&O insurance, or my background check prior to expiration, I will be immediately disqualified from being an approved notary. I also understand that being approved to join FNTG's approved notary network does not obligate FNTG or its Affiliates to use my notary services now or in the future.

Signature _____ Date _____

Print Name _____

Address _____

City _____ State _____ Zip _____

Email _____

FIDELITY
NATIONAL TITLE GROUP

FNTG THIRD-PARTY NOTARY CONFIDENTIAL INFORMATION AGREEMENT

Pursuant to the privacy regulations and information security guidelines issued by federal financial regulators pursuant to Title V of the Gramm-Leach-Bliley Act ("GLBA") covered financial institutions and service providers with access to confidential data are required to ensure that all service providers and marketing partners who have access to customer information provide for the confidentiality and security of such information. To enable the Company to demonstrate compliance with the privacy requirements of GLBA, you hereby agree to the following, which will apply to all information and data provided to you in any format by Fidelity National Title Group, any of its Affiliate companies or our customers (collectively the "Company").

As used herein, the term "**Customer Information**" means any "nonpublic personal information" and /or "personally identifiable financially information" about "customers" and "consumer" (as those terms are used in Title V of the Gramm-Leach-Bliley Act and the privacy regulations adopted thereunder) provided to you by the Company or otherwise received by you in connection with a Company transaction. "Service Provider" means the party signing this Agreement.

1. Service Provider agrees that, except as may be reasonably necessary in the ordinary course of business to carry out the activities to be performed by Service Provider under its agreement(s) with the Company or as may be required by law or legal process, Service Provider will not disclose any Customer Information to any third party without the written consent of the Company.
2. Service Provider agrees that it will not use any Customer Information other than to carry out the purposes for which such Customer Information was disclosed to Service Provider by the Company unless such other use is (a) expressly permitted by a written agreement executed by the Company, or (b) required by law or legal process.
3. Service Provider agrees to take all reasonable measures, including without limitation such measures as it takes to safeguard its own confidential information, to ensure the security and confidentiality of all Customer Information to protect against anticipated threats or hazards to the security or integrity of such Customer Information and to protect against unauthorized access to or use of such Customer Information.
4. Throughout the term of the Agreement, Service Provider shall implement and maintain appropriate safeguards, as that term is used in Section 314.49(d) of the FTC Safeguard Rule, 16 C.F.R. Part 314 (the "FTC Rule"), for all Customer Information, as that term is defined in Section 314.2(b) of the FTC Rule, owned by the Company and delivered to the Service Provider pursuant to this Agreement.
5. Service Provider shall notify the Company immediately upon discovering or suspecting any loss, unauthorized disclosure, unauthorized access, or misuse of Customer Information. Such notice shall be in writing unless such writing will cause a delay in notification in which case the initial notification may be oral. Such notice shall be provided to the Company contact or representative that assigned the transaction to Service Provider or as designated in the Company's transmittal instructions provided to Service Provider.

Initial _____

FIDELITY NATIONAL TITLE GROUP

6. Service Provider shall not reproduce, store or save any Customer Information in any form except to the extent required by the laws governing the Service Provider's notarial services or as required by any Company instructions provided to Service Provider. To the extent Service Provider retains any Customer Information pursuant to the preceding sentence, such copies will only be retained for as long as required by such law or Company instruction and such information or documents shall remain subject to this Agreement. Upon request Service Provider shall provide the Company with written certification regarding the destruction of Confidential Information.
7. Service Provider agrees that while any Customer Information is in his/her possession or control it will be (i) stored in a physically and logically secured and controlled environment, only accessible by Service Provider and (ii) downloaded only into physically and logically secured and controlled systems only accessible by Service Provider where it will stay encrypted while in storage and in transit.
8. Service Provider agrees to indemnify, defend and hold Company harmless for any security breaches, violations of GLBA or breach of this Agreement caused by Service Provider's negligence, misconduct and/or loss or material alteration of Customer Information.
9. Service Provider represents and warrants that he/she will comply with the laws, regulations and requirements for document retention applicable to the notarial services which Service Provider is providing to or for the Company. Once the required retention period has expired Service Provider represents and warrants that he/she will destroy all Confidential Information and any Company related work product via shredding or other recognized secure disposal means.
10. Service Provider acknowledges that a breach of this Agreement will cause irreparable harm or damage to the Company, its customers or consumers. Service Provider agrees that the Company is entitled to seek injunctive relief for a breach of the Agreement and other relief as may be granted by a court of competent jurisdiction.
11. Service Provider agrees that if any provision of this Agreement is unenforceable or invalid the unenforceability or invalidity shall not render this entire Agreement unenforceable or invalid.

In Witness Whereof, the undersigned Service Provider agrees to all of the terms and provisions of the foregoing Agreement.

_____
Signature

Name: _____
City, State & Zip: _____
Date: _____

Fidelity National Title Group
Consumer Complaint Handling Procedures for Third Party Notaries

From time to time, a consumer may express dissatisfaction to you, the notary, about some aspect of the transaction for which you are providing signing services. The subject matter of the consumer's dissatisfaction may be in regards to some aspect of the loan, the closing process or even your performance as a signing agent. If the consumer expresses dissatisfaction to you at any point during the signing appointment, you must comply with the procedures outlined below for responding to the consumer and for reporting the complaint to the title/escrow/settlement company.

Definitions

Complaint
For the purpose of this procedure, a "Complaint" is any situation or matter where a Consumer or their representative expresses an issue or concern, either verbally or in writing, to a third-party notary in the ordinary course of the signing service, which does not involve one or more of the risk factors listed in the definition for Escalated Complaint (defined below).

Escalated Complaint
For the purpose of this procedure, an "Escalated Complaint" is any Complaint that:

1. has the potential to cause harm or hardship to a Consumer;
2. poses imminent legal or regulatory risk to FNTG or the lender;
3. indicates that the Consumer may have or may contact the media, a lawyer, a consumer advocacy group, or the Better Business Bureau in regards to the issue or concern; or
4. alleges unfair or deceptive trade practices, violation of law, or similar violation;

An "Escalated Complaint" also includes any Complaint in which the Consumer requests to go on record as being dissatisfied or requests to escalate the handling of the Complaint.

Complaint Handling Procedure

1. **For any Complaint other than an Escalated Complaint**, you should ask the consumer if he or she would like to speak with the title/escrow/settlement officer or loan officer before proceeding with the signing.
    - If the consumer would like to speak with the title/escrow/settlement officer or loan officer, you must contact the title/escrow/settlement officer or loan officer during the signing appointment to provide a warm hand-off to the consumer.
    - If the consumer does not want to speak with the title/escrow/settlement officer or loan officer, you should ask if the consumer desires to proceed with the signing and proceed accordingly.
    - Regardless of the outcome, you must document the facts and notify the title/escrow/settlement office of the complaint at the conclusion of the signing appointment.

2. **For an Escalated Complaint**, you should advise the Consumer that you are unable to address his or her concerns directly and contact the title/escrow/settlement officer by phone before proceeding with the signing.

Initial _____

If the borrower signer requests to proceed with the signing before you are able to reach the title/escrow/settlement officer, you must advise the signer that you cannot proceed without the title/escrow/settlement officer's clearance. At the conclusion of the signing appointment, you must document the facts and notify the title/escrow/settlement office of the complaint.

Annual Acknowledgment

I have read, understand and agree to the procedures set forth herein, and I acknowledge that my performance will be monitored by FNTG for compliance. I understand that failure to comply with these *Consumer Complaint Handling Procedures* may result in my removal from FNTG's approved notary network.

Date

Signature

Printed Name

City, State and Zip

Email

Trade Vendor Information Security Requirements and Recommendations

As a Trade Vendor for Fidelity National Financial, Inc., its majority-owned subsidiaries, and controlled affiliates (collectively referred to as "FNF" or the "Company"), the Company is entrusting you with sensitive personal information about our customers. To protect the privacy and confidentiality of Customer Information, FNF requires all Trade Vendors to implement the security controls described in *Section 1 – Minimum Security Requirements* of this document. FNF strongly recommends that all Trade Vendors implement the security controls in *Section 2 – Basic Security Recommendations* of this document. In addition, all Trade Vendors must receive and acknowledge this document at least annually.

This document contains footnotes that provide links to guidance for implementing the requirements and recommendations. Much of the guidance is found in the GCA Cybersecurity Toolkit for Small Business Handbook[1] and website[2] (the "Toolkit") and the FTC Tips and Advice for Protecting Small Businesses[3] (the "FTC Website").

Scope

All Trade Vendors (as defined below) providing services to, or on behalf, of FNF.

Purpose

The purpose of these Trade Vendor Information Security Requirements and Recommendations (hereinafter, "this document") is to establish threshold controls that Trade Vendors must implement, as well as additional recommendations, to protect the security, integrity, and availability of Customer Information.

Definitions

"**Customer Information**" means any "nonpublic personal information" and/or "personally identifiable financial information" about "customers" and "consumers" (as those terms are used in Title V of the Gramm-Leach-Bliley Act and the privacy regulations adopted thereunder) provided to Trade Vendor by FNF, or otherwise received by TV (as defined below) in connection with an FNF transaction.

"Trade Vendor" and "**TV**" mean notaries, signing service companies, closing attorneys/agents providing notarization and/or signing services to consumers.

Section 1 - Minimum Security Requirements

1.1 **Secure Your E-mail Accounts**

You must use an e-mail service with the following security features fully enabled:

a. Two factor authentication (2FA[4])

[1] https://gcatoolkit.org/wp-content/uploads/2021/06/GCA-Toolkit-Handbook.pdf
[2] https://gcatoolkit.org/smallbusiness/know-what-you-have/?_tk=identify-your-devices
[3] https://www.ftc.gov/business-guidance/small-businesses
[4] Two-Factor Authentication (commonly referred to as Multi-Factor Authentication, MFA and 2FA) – Please refer to Toolbox 3.2 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/?_tk=tools-for-2fa#toolkit.

b. Encryption of data stored on your devices [5]
c. Encryption of data during transit[6]: end-to-end encryption via the most current Pretty Good Privacy (PGP) protocol available
d. User ID unique to a specific individual (no shared user IDs/accounts)
e. Complex passwords, which meet the password requirements section below

1.2 **Use Strong Passwords; Password Requirements**

You must protect your e-mail account, and any device and/or system that you use to process or store Customer Information by using strong passwords.

a. Except for passwords for mobile devices and tablets that do not support these requirements, a strong password must be at least 8 characters and contain a minimum of 3 of the following:
   i. At least one upper case letter (A-Z)
   ii. At least one lower case letter (a-z)
   iii. At least one number (0-9)
   iv. At least one special character (for example, !$#%)
b. Never store your passwords in any format, including written, electronic, or plain text[7] formats. You should never share your passwords with anyone in any format. Your passwords should be known to you, and only you.
c. For devices, systems, applications, and accounts that you use to access, send, receive, or store Customer Information, you must:
   i. Change passwords every 180 days, and
   ii. Use unique passwords for each device, system, application, or account. For example, you should not use the same password for all access points

1.3 **Keep Your Devices and Systems Up-To-Date and Use Antivirus/Antimalware Programs**

To secure the devices and systems you use to process and/or store Customer Information, you must:

a. Ensure that your devices (desktops, laptops, tablets, mobile devices, etc.) are continually updated with the latest, fully supported operating system for each device[8]. FNF recommends turning on automatic updates for devices that provide an automatic update option.
b. Only use versions of your operating system that are supported and still receiving updates from the developer[9]. You can visit www.support.microsoft.com or www.support.apple.com to determine current operation system versions available to you.

---

[5] Encryption of Data Stored on Your Devices – Please refer to Toolbox 2.2 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/update-your-defenses/?_tk=encrypt-your-data#toolkit.

[6] Encryption of Data in Transit – Please refer to Toolbox 2.2 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/update-your-defenses/?_tk=encrypt-your-data#toolkit.

[7] Never Share Your Passwords or Store Them in Plain Text – Please refer to Toolbox 3.1 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/?_tk=strong-passwords#toolkit.

[8] Ensure Your Devices Are Up to Date – Please refer to Toolbox 2.1 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/update-your-defenses/?_tk=update-your-devices-and-applications#toolkit.

[9] Only Use Versions of Your Operating System That Are Supported by the Developer – Please refer to Toolbox 2.1 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/update-your-defenses/?_tk=update-your-devices-and-applications#toolkit.

c. Continually apply all available patches and updates to your applications and other systems to ensure they are free of known vulnerabilities[10]. FNF recommends turning on automatic updates for applications that provide an automatic update option.
d. Update antivirus/antimalware programs on your smartphones, tablets, laptops, and desktops on a regular basis[11].

1.4 **Be Mindful of Where You Store Customer Information**

You should never store Customer Information unless you are required to do so to perform the services you provide to the Company. For information you are required to store:

a. You must encrypt all Customer Information regardless of where you store such data
b. You should enable device encryption[12]
c. If you are using cloud storage[13] to store Customer Information, you should use a cloud storage account with the following features fully enabled:
    i. Encryption of data in storage
    ii. Encryption of data during transit: end-to-end encryption via the most current transport layer security (TLS) protocol version(s) available
    iii. User ID unique to a specific individual (no shared user IDs/accounts)
    iv. Complex passwords that meet the password requirements section above

1.5 **Securely Destroy All Customer Information and Any Hardware Used to Store Customer Information**

You must have an information retention and destruction policy that meets or exceeds the requirements in your industry relevant to the services you are providing. Information should be destroyed as soon as it is no longer needed and in accordance with FNF requirements; this includes information in written or electronic format. Similar controls must be applied for hardware destruction as well[14].

1.6 **FNF Right to Audit**

FNF may conduct or engage a third party to conduct periodic reviews of your environment, processes, and controls. FNF has the right to immediately terminate your services (and all associated contractual agreements) upon your failure to cooperate or the failure of your environment to conform with the minimum-security requirements set forth in Section 1 of this document.

---

[10] Continually Apply Available Patches and Updates to Applications and Systems – Please refer to Toolbox 2.1 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/update-your-defenses/?tk=update-your-devices-and-applications#toolkit.

[11] Update Antivirus and Anti-Malware Programs on All Devices; Ensure Default Antivirus Solutions are Turned On, or Where There are no Default Solutions, Install an Antivirus Solution – Please refer to Toolbox 4.1 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/prevent-phishing-and-malware/?tk=anti-virus#toolkit.

[12] Device Encryption – Please refer to Toolbox 2.2 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/update-your-defenses/?tk=encrypt-your-data#toolkit.

[13] Cloud Storage – A search engine query for "free and secure cloud storage" will provide guidance.

[14] Data Retention and Destruction – Please refer to Item 4 – "Pitch It" on the FTC Website, located at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business#PitchIt.

1.7 **Logging on Your E-mail Account and Other Systems That You Use to Provide Services to FNF**

Computer operating systems and business applications record, or "log", events, and tasks as they happen on your computing device and applications. There may come a time when FNF needs to obtain and examine your logs in order to meet its regulatory and client obligations. Should that need arise, FNF will provide you with general instructions on how to access and provide those logs. If you do not reasonably cooperate with a request for logs, FNF shall have the right to immediately terminate your services (and all associated contractual agreements).

Section 2 - Basic Security Recommendations

2.1 **Maintain a Dedicated E-mail Account for FNF Orders**

You should strive to maintain a dedicated business e-mail account for receiving and sending orders. This e-mail account can be used for your other notary customers, but it should remain separate and distinct from your personal e-mail account.

2.2 **Secure Your E-Mail Account**

In addition to the e-mail account requirements in Section 1, FNF recommends that you enable filtering capabilities for phishing e-mails and e-mails with malicious payloads or hyperlinks[15].

a. Click here for instructions on enabling advanced filtering in Gmail.
b. Click here and here for instructions on enabling advanced filtering in Yahoo.

2.3 **Protect Customer Information and Your Devices with Physical Security Controls**

You should strive to implement adequate physical security controls to securely store Customer Information when not in use and to protect Customer Information from the view of visitors or other persons without a need to know to complete the TV services. For example, you should keep your work area tidy and free of documents containing Customer Information when not in use.

2.4 **Avoid Using Public/Shared Wireless Networks**

FNF strongly advises against the use of public/shared wireless networks. When connected to Wi-Fi, FNF recommends that you use a secured/private wireless network or hotspot to access, send, or receive Customer Information. A cellular connection is considered private and acceptable.

2.5 **Avoid Using External Storage Devices**

You should never store Customer Information unless you are required to do so to perform the services you provide to the Company. For information you are required to store:

a. You should avoid storing Customer Information on removable media, such as CDs, DVDs, USBs, thumb/flash drives, external hard drives, or personal tablets or mobile devices. Removable media presents unique security risks. Most forms of removable media are small and easily transportable, lending themselves to being easily lost or stolen. Additionally, removable media can unknowingly spread malicious software and viruses.

[15] Filtering Capabilities – Please refer to Toolboxes 4.1 thru 4.3 of the Toolkit; it may be accessed directly through the following link https://gcatoolkit.org/smallbusiness/prevent-phishing-and-malware/?_tk=anti-virus.

As of the date below, Trade Vendor hereby acknowledges receipt and understanding of these Minimum Information Security Requirements and Recommendations for Trade Vendors.

Signature: _____

Print Name: _____

Date: _____