

ALTA BEST PRACTICES MANUAL

Supporting Documentation to Address Regulatory Compliance
Guidelines for the: Consumer Financial Protection Bureau through
ALTA's Best Practice Framework "Title Insurance and Settlement
Company Best Practices"

*Green Label Title,
LLC*

Green Label Title, LLC
2517 Highway 35, Building B, Suite 102
Manasquan, NJ 08736
(732) 722-7373

Mission Statement

This Best Practices Manual has been developed by Green Label Title, LLC in accordance with guidelines set forth by the American Land Title Association and in compliance with both the Gramm-Leach Bliley Act and the Consumer Financial Protection Bureau established under the Dodd-Frank Act. The goal of this manual is to outline the policies and procedures set by Green Label Title, LLC in our commitment to protect the security of the consumers and continue to provide professional quality service to our clients.

Introduction

Green Label Title, LLC's Best Practices Manual follows the guidelines of the American Land Title Association which was developed in order to "to help members illustrate to consumers and clients the industry's professionalism and best practices to ensure a positive and compliant real estate settlement experience." The compilation of this manual draws from previously designed policies and procedures active with Green Label Title, LLC including our Information Security Manual. In further compliance with the new regulatory environment, Green Label Title, LLC is also an approved settlement agent with Secure Settlements, Inc.

American Land Title Association (ALTA) has created "best practices" that are intended to define a set of strong procedures that the title insurance and settlement companies can follow to protect consumer information and provide higher levels of efficiency. The framework of ALTA's "best practices" is designed with the expectation that a strong foundation will be established through adherence to the seven distinct pillars outlined in this manual.

The "best practices" of an industry are methods and techniques that are proven to produce superior results in achieving higher benchmarks. The purpose is to maintain consistent quality that serves as an enhancement to mandatory legislated standards and promote the industries adherence to compliance.

ISSUED AND APPROVED:

Dated August 2015



By: Steven M. Green, President

BEST PRACTICE ONE (1) - LICENSING

Definition: *Establish and maintain current license(s) as required to conduct the business of title insurance and settlement services.*

Green Label Title, LLC Policy and Procedures: We maintain all local, state and national required business and insurance licenses. All title insurance licenses are tracked maintained through the Administrative Department. Established in 2009, Green Label Title, LLC is active and in good standing in New Jersey. Copies of current insurance licensing is available in Appendix A.

- Licenses are renewed based on state regulations and at the earliest point that renewal becomes available (typically 60 days in advance).
- Annual Reports are filed and completed yearly with all applicable fees.
- Where applicable, continuing education credits are completed for agent licensing.

1.2 – TITLE INSURANCE LICENSE RENEWAL PROCEDURES

The state of New Jersey issued the current Title Insurance Agency (Producer) License #1229764 to Green Label Title, LLC on 06/01/2015. The license has been continually renewed since its initial issuance. The expiration date for the current license is 05/31/2017.

The Company is currently an authorized agent for First American Title Insurance Company, Westcor Land Title Insurance Company, Stewart Title Guaranty Company and Fidelity National Title Insurance Company.

ANNUAL PROCEDURES

The Company President reviews and determines state licensing requirements annually. The Company President maintains a License Log and current copies of all state required licenses in a single location along with evidence that the Company and its employees are compliant with current licensing requirements.

1. The Company President determines the states in which the company conducts the business of title insurance and settlement services. Presently, New Jersey is the only state we operate.
2. The Company President reviews the insurance licensing laws for states listed above annually and determines the business and individual licenses that are required. A Title License Log is then created and maintained by the Company President for the next twelve months.
3. The Company President obtains copies of all business and individual licenses listed on the Title License Log and maintains them in a folder with the Title License Log. The details of each license are entered onto the Title License Log (including name, license #, expiration date and CE requirements).

4. The Company President confirms the current appointment of the Company and each individual on the licensing log with the title insurance underwriter(s) that the company has an agency contract with.

MONTHLY PROCEDURES

1. The Company President reviews the Title License Log monthly to determine if any licenses are due for renewal within the next 30-60 days and to determine if any individuals need to take classes to ensure compliance with Continuing Education (CE) requirements.

2. The Company President ensures that individuals that are not yet compliant with CE requirements for licensing period have plans to attend classes that will fulfill requirements prior to expiration date.

3. The Company President applies for renewal of all licenses no later than 30 days prior to the current expiration dates shown on the Licensing Log.

4. The Company President obtains copies of renewal licenses and places them in the Licenses folder.

5. The Company President notifies its underwriter(s) of any individuals or entities that should no longer be appointed.

Supporting Documentation: Copies of insurance licenses.

1.3 – NOTARY LICENSE RENEWAL PROCEDURES

Green Label Title, LLC (“the Company”) shall only use currently licensed Notary Publics when Notary Public services are required in the conduct of the business of title insurance and settlement services.

The Company currently employs licensed Notary Publics who are utilized when Notary Public services are required.

1. A Notary Public License Log is maintained by the Company President for all commissioned Notary Publics that are employees of the Company. Copies of the licenses are maintained in a secure folder with the Log in the Company President’s office.

2. The Company President reviews the Log monthly to determine if any licenses are due for renewal within the next 30-60 days and coordinate the notary license renewal with the individual licensee.

3. The Company President ensures all necessary renewals are applied for no later than 30 days prior to the current expiration dates shown on the Log.

4. The Company President obtains copies of renewal licenses and places them in a secure folder with the Log.

5. If for any reason a Notary Public other than one employed by the Company is utilized due to circumstances beyond the Company's control, the Notary Public's current license is verified by researching the applicable state Notary verification website/database. Documentation of the Notary Public's license is maintained in the applicable settlement file.

1.4 – ALTA POLICY FORMS LICENSE RENEWAL

Green Label Title, LLC ("the Company") shall comply with the American Land Title Association (ALTA) requirement that all issuing agents of title insurance maintain a Policy Forms License or an Occasional Use Waiver. Green Label Title, LLC is a current member of ALTA.

ANNUAL PROCEDURES

1. The Company President shall determine if the Company will remain current dues paying member of the American Land Title Association (ALTA). If it does, the Company President will obtain a copy of the ALTA Membership Certificate and maintain it in a secure file in their office. An ALTA policy forms license is included with ALTA membership so the ALTA Membership Certificate is evidence of the Company's policy forms license.

2. If the Company is not a current dues paying member of ALTA, the Company President shall determine if the Company is eligible for an ALTA Occasional Use Waiver (issued less than 50 title insurance policies in the previous calendar year). If the Company is eligible for the Waiver, the Company President shall apply for one and once received maintain a copy of it in a secure file in their office.

3. If the Company is not eligible for an Occasional Use Waiver (issued more than 50 title insurance policies in the previous calendar year), the Company President will either 1) apply for an ALTA membership or 2) apply for an ALTA Policy Forms License. Once the ALTA membership certificate or ALTA Policy Forms License is received the Company President will maintain it in a secure file in their office.

4. This procedure will be repeated each year prior to the expiration date of the current ALTA membership certificate, ALTA Policy Forms License or Occasional Use Waiver.

BEST PRACTICE TWO (2) – ESCROW ACCOUNT CONTROLS

Definition: *Adopt and maintain appropriate written procedures and controls for Escrow Trust Accounts allowing for the electronic verification of reconciliation.*

Green Label Title, LLC Policy and Procedures: All escrow funds are maintained in separate designated accounts which are reviewed for reconciliation discrepancies on a daily basis. These accounts are monitored under the following controls:

- Daily reconciliation of all debts and credits to the account as well as available balances using the latest version of AccuTitle/ Title Desktop settlement software and Rynoh Reconciliation Software.
- Positive Pay and ACH Debt blocks setup on all accounts.
- Open escrow balances and outstanding checks are reviewed by management on a weekly basis.
- Three Way Reconciliations completed on a monthly basis and reviewed for accuracy by management.
- Appropriate authorization levels are set and maintained.

2.1 - ESCROW/ TRUST ACCOUNT CONTROLS

Green Label Title, LLC (“the Company”) has internal controls in place that apply to all custodial and fiduciary accounts (“Trust Accounts”) to meet client and legal requirements for the safeguarding of client funds and to minimize the exposure to loss of client funds.

ESCROW CONTROL PROCEDURES

The Company has two active Trust Accounts that are established and maintained in accordance with state regulations and its agency underwriter contract. All client funds collected as a fiduciary are deposited into these accounts. The Trust Account is maintained separate from all other Company accounts, including operating and personal accounts. The Company President maintains a log of all bank accounts in the Company’s name.

The Trust Accounts are maintained at Ocean First Bank and Investors Bank, a financial institutions whose deposits are insured by the FDIC. The accounts are titled and clearly identified as “Green Label Title, LLC Trust Account” on all bank statements, bank agreements, disbursement checks and deposit tickets. This is to confirm the fiduciary nature of the account.

DAILY PROCEDURES AND CONTROLS

1. All funds collected from parties at settlement are deposited into the Trust Account. Collected funds may be in the form of a wire, cashier’s check (for anything over \$500) or personal check (for anything under \$500).

2. All checks received at settlement are restrictively endorsed “For Deposit Only” upon receipt. A separate deposit ticket with corresponding file number is prepared for each file and the deposit is made within twenty-four hours of receipt.

3. Funds are only disbursed after the collected funds have been deposited into the Trust Account and irreversibly credited to it.
4. Incoming and outgoing wire confirmations are maintained in each file.
5. Each check written out of the Trust Account must reference the corresponding file number that it was written for. Copies of the checks are maintained in the file along with a current, detailed deposit and disbursement summary sheet.
6. All check stock is safeguarded in a secure, locked location that only authorized check signers can access. All check stock is accounted for by the Company President at the end of each business day.
7. Any instructions that the Company receives for specific handling of escrow funds from a particular party must be made in writing and kept in the transaction file. If a separate, interest bearing account is requested same will be established and be subject to the same procedures outlined here.
8. Inactive or dormant account disbursements must be approved by the Company President. This approval must be in writing and be maintained with the account's bank statements and reconciliations.
9. Disbursements from any file that is more than 180 days old must be approved by the Company President. This approval must be in writing and be maintained in the file.

MONTHLY PROCEDURES AND CONTROLS

All bank fees including service charges and wire fees are reimbursed with funds from the Company's operating account.

2.2 - ESCROW/ TRUST ACCOUNT AUTHORIZATIONS

Green Label Title, LLC ("the Company") has internal controls in place to ensure that only employees that have passed background checks are authorized to sign checks, initiate wires, and approve bank account transactions for all custodial and fiduciary accounts ("Trust Accounts") and further that all Trust Account transactions are initiated or approved only by such authorized employees.

Currently, Steven M. Green (President/Owner) is the only authorized signatory with access to our Escrow Account, sign checks and initiate wires.

TRUST ACCOUNT AUTHORIZATION PROCEDURES

1. At the beginning of each calendar year, the Company President/Owner considers if any additional employees should be authorized to approve financial transactions, sign checks and initiate wires for the Company's Trust Account. At the same time the Company President considers limits for each employee that would be authorized.

2. Should additional employees be authorized, the Company President would create a Trust Account Authorizations Log to be maintained for the entire calendar year with any authorized employees' names, respective authorizations and limits.

3. All employees authorized to process Trust Account transactions must undergo and pass a background check at the time of hiring and/or prior to being authorized. The background check will include criminal and consumer credit reports that cover a period of not less than five (5) years. Established employees with Trust Account authorizations will undergo a background check at least every three (3) years. The results of the background checks will be maintained in a secure personnel file in the President's office.

4. When an authorized employee leaves the Company or when the Company President decides to cancel an employee's authority, all of their Trust Account authority is canceled immediately; any necessary bank paperwork is completed immediately and the Trust Account Authorizations Log is updated.

5. The Company has the following controls in place to ensure that Trust Account bank transactions are conducted by authorized employees only:

- The Company does not permit the use of signature stamps on Trust Account checks
- All checks require the "wet" signature of the Company President/Owner
- All outgoing wires require dual authorizations with password (key fob) verification
- All check stock is maintained in a locked cabinet that only authorized employees have access to.

7. Per the Company's instructions, the bank has a block on the Trust Account for Automated Clearing House (ACH) Transactions.

8. Per the Company's instructions, the bank has a block on the Trust Account for International Wire Transactions.

9. The Trust Account is set-up with Positive Pay so that the bank only clears checks after verifying them with the Company's check register.

2.3 – TRUST ACCOUNT RECONCILIATION PROCEDURES

Green Label Title, LLC ("the Company") shall have procedures and controls in place to ensure Three-Way Reconciliations are performed on all custodial and fiduciary accounts ("Trust Accounts") monthly basis; that same are reviewed and signed off by management and that appropriate follow-up is performed on outstanding and trial balance items.

DAILY PROCEDURES AND CONTROLS

1. When the Company conducts a settlement, all funds collected are deposited into the Company's Trust Account.

2. Funds are only disbursed by an authorized employee after they have verified that the collected funds have been deposited and irreversibly credited to the Account and that the collected funds are sufficient to cover the disbursements.

3. A separate receipt and disbursement ledger is printed and maintained in each settlement file detailing every receipt and disbursement including date, amount, payee/payer and description.
4. The ledger should indicate that the file balances (Receipts = Disbursements) or there should be documentation to support any difference (i.e. – escrow agreement for funds being held).
5. The Company President or their designee performs a daily reconciliation through Rynoh of all Trust Account receipts and disbursements.

MONTHLY PROCEDURES AND CONTROLS

1. The Trust Account bank statement is delivered to and opened by the outside CPA who is responsible for performing a Three-Way Reconciliation of the Account. The outside CPA is not an authorized signer or wire initiator on any of the Company's bank accounts.
2. Within ten (10) days of receiving the bank statement, the outside CPA completes a Three-Way Reconciliation of the account in accordance with approved Three-Way Reconciliation Procedures.
3. Deposits in transit and outstanding checks on the previous month's Three-Way Reconciliation are checked against the current bank statement to determine what has cleared and what remains outstanding.
4. Upon completion of the Three-Way Reconciliation, the outside CPA prints the following reports:
 - Summary page with Register/Book Balance, Trial Balance, Adjusted/Reconciled Bank Balance
 - Cleared Transactions/Proofing Register
 - Deposits in Transit
 - Outstanding Checks
 - Trial Balance (Unbalanced Files)
 - Reconciling items
 - Voided Checks
 - Outstanding checks from previous month
5. Within one day of completion of the Three-Way Reconciliation Reports the outside CPA provides them to the Company President who reviews them for completeness and accuracy. The Company President Initials and dates the front page to document their review.
6. The Company President, outside CPA and staff work together to immediately research and resolve any of the following items reflected by the Reconciliation Reports:
 - Deposits in Transit older than five (5) days
 - Incoming Wires in Transit older than two (2) days
 - Payoff and Proceeds checks outstanding for more than ten (10) days
 - Recording checks outstanding for more than thirty (30) days
 - Checks for taxes and/or hazard insurance outstanding for more than thirty (30) days
 - Underwriter premium checks outstanding for more than sixty (60) days

- All other checks outstanding for more than ninety (90) days
- Reconciling items

Documentation of all resolved items is maintained with the statement and reconciliation reports.

7. Any escrow shortages are immediately funded from the operating account.

8. All bank fees are reimbursed on a monthly basis from the operating account.

9. Copies of the bank statement and Three-Way Reconciliation Reports are made available electronically to the Company's title insurance underwriter.

10. The Company President periodically reviews cancelled checks and the check register for unusual items.

ANNUAL PROCEDURES

Each year the Company President and outside CPA review the outstanding checks and file ledger balances for reissue or escheatment to the State as required by law.

BEST PRACTICE THREE (3) – INFORMATION AND DATA PRIVACY

Definition: *Establish and maintain a written privacy and information security program to protect Non-Public Personal information as required by local, state and federal law.*

Green Label Title, LLC Policy and Procedures: Green Label Title, LLC has a comprehensive security program designed to insure that all necessary information security safeguards are in place and adequately address GLBA requirements. All employees of the Company are expected to contribute to this program and report any incidents that may affect the security of the organization's information systems. The following policies are addressed within Green Label Title, LLC's Information Security Policy.

- Controlled access to physical and electronic storage as well as secure destruction of physical documents
- Secure transmission of information
- Monitoring of third party service providers access
- Physical entry controls to prevent unauthorized access
- Network guidelines and access controls including restrictions on user authentications and authorization
- Remote access controls and restrictions
- Up to date virus management software and firewall controls against malicious software, viruses and unauthorized websites
- Business Continuity Plan for disaster preparedness
- Security Incident Reporting and Resolution
- Background checks on all personnel
- Training of employees to ensure compliance with program
- Restrictions and the appropriate uses of company systems

3.1 – Information Security and Privacy Management Procedures

Green Label Title, LLC ("the Company") is committed to protecting non-public, personal, and/or sensitive information ("Private Information") as required by local, state, and federal law. The Information Security and Privacy Management Policies outlined herein have been adopted by the Company to ensure compliance with the applicable laws and to ensure Private Information is properly safeguarded.

The Company has created and adopted written procedures and an Information Security Program to ensure that it is compliant with federal, state, and local laws and able to best protect its clients' confidential, personal, and/or Private Information. This written **Information Security Program** is outlined in procedure reference no. 3.4 herein. It specifically addresses protection of non-public Private Information and provides direction for managing and protecting the confidentiality, integrity and availability of all of the Company's information assets. Following are additional components of the Company's Information Security and Privacy Management policies.

1. Background Checks / Hiring Practices – The Company seeks out and hires only qualified employees with verified education credentials, work history and reputations. The Company performs background checks, including criminal history, on employees and temporary staff that have access to Personal Information. Such employees will have a background check at least every three (3) years. The results of background checks are maintained in the employee’s personnel file as per the Company’s document retention and destruction guidelines.

2. Acceptable Use of Information Technology Policy - The Company’s Acceptable Use of Information Technology Policy is outlined in procedure reference no. 3.4.1 herein describing the ways and circumstances under which employees may use Company owned technology.

3. Access to Private Information - Private Information held by the Company is restricted to only those employees whose job duties require access to this information. Access to Private Information is granted and authorized by the Company’s President. These access rights are reviewed annually to ensure the correct permissions are granted to the Company’s employees.

4. Clean Desk and Clear Screen Policy - The Company has a Clean Desk and Clear Screen Policy that is further outlined in procedure reference no. 3.4.2 herein.

5. Data Security- Removable Media - The Company has a removable media policy outlined in procedure reference no. 3.4.3 herein that restricts the use of USB devices, CD/DVD writeable drives and other storage devices.

6. Record Retention and Disposal Policy - The Company has a Record Retention and Disposal Policy that is further outlined in procedure reference no. 3.5 herein.

7. Approval - The Company’s Information Security and Privacy Management has been approved by the Company President. It is communicated to all employees annually by the office manager and all employees are required to sign an acknowledgment of their receipt. The acknowledgment is retained in each respective employee’s personnel file. The Company ensures that all employees are aware of their individual roles in the protection of Private Information by routine staff meetings, training session and continuing education seminar presented by our underwriters.

Limited exceptions to any of the Company’s policies may be approved by the Company President. Exceptions to policies are documented in a designated file and retained as per the Company’s document retention and destruction guidelines. Employees who violate any of the Company’s policies are subject to disciplinary action up to, and including termination.

8. Policy Review - The Company’s Information Security and Privacy Management Policies are reviewed as further outlined in the Company’s Policy Review Procedures Policy (procedure reference no. 3.1.1 herein) to determine if updates are necessary to reflect changes in operations, legal and regulatory requirements, industry best practices and available technology. Changes to any of the Company’s policies are tracked and maintained as further described in that Policy Review Procedures Policy.

9. Customer Privacy Notice - The Company has a Customer Privacy Policy Notice, which is provided to customers with the delivery of the title commitment by email. The customer must

initial or sign the Notice to acknowledge their receipt it and the initialed or signed copy is retained in the Company's transaction file.

10. Privacy Statement - The Company's website contains a Privacy Statement, which includes details regarding information, if any, that may be collected.

3.1.1 – IS Policy Review Procedures

Green Label Title, LLC ("the Company") reviews and updates all Information Security and Privacy Management Policies on a regularly scheduled basis to determine if updates are necessary to reflect necessary to reflect changes in operations, legal and regulatory requirements, industry best practices and available technology.

1. Review Team - The Policy Review Team will, on an annual basis and more frequently when required, meet to review all Information Security and Privacy Management Policies. The Policy Review Team will consist of the Company President and Cloudstar, our outside IT Consultant. Changes to the policies are only made after these meetings.

2. Review Criteria - A variety of criteria will be used by the Policy Review Team at the time of review. These items will include reviewing the policy to determine if changes to any of the following have been made:

- Company operations;
- Legal and Regulatory requirements;
- Industry Best Practices;
- Available Technology

3. Communication - Upon completion of the review and necessary revisions to any Company policies, updated policy versions will be placed in the company's official policy manual, replacing the outdated version. The updated policies will be communicated to all staff members, as well as any clients, when appropriate. All staff members are required to review and acknowledge receipt of the new policy manual via the company's policy acknowledgment form. Said acknowledgment will be retained in the employee's personnel file.

3.2 – Risk Identification and Assessment Procedures

Green Label Title, LLC ("the Company") is committed to protecting non-public, personal, and/or sensitive information ("Private Information") as required by local, state, and federal law through its Information Security and Privacy Management policies. Operations are regularly reviewed to identify and assess current or suspected external and internal risks that could compromise the Private Information stored by the Company.

The Company has created and adopted written policies and procedures with the goal of identifying and assessing current or potential risks which could have a negative effect on the Company, its systems, or clients, including risks that could compromise Private Information held by the Company. Private Information is defined under this policy as any privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the Company. These procedures include the regular

review by Policy Review Team of the Company's operational functions to identify potential or actual risks.

This review will include examination of:

- The types of Private Information the Company maintains;
- The location in which Private Information is stored;
- How information can be accessed;
- Which employees have access to Private Information;
- Which non-employees have access to the office

Risk Assessments performed by Policy Review Team includes internal and external risks. The risk analysis review encompasses the Company's entire computer networking system(s) and physical security tools including but not limited to alarm system, entrance and interior door locking mechanisms (key pad) and locks on file cabinets.

All employees play a major role in the identification and elimination of risks to the Company. Employees receive training on ways they can help identify risks and ways to avoid compromising the Private Information for which they have access. Employees of the Company may create unintended risk while performing normal business functions for the Company. The Company takes steps to limit the risk created by employees which may include:

- Limiting the amount of information each employee may access to only that information needed to perform the duties associated with the employee's position;
- Reviewing how information is communicated to clients, lenders, vendors, and all other third parties involved in the transaction to ensure that transmission is safe, encrypted, and otherwise protected during transit;
- Identifying ways information is and may be protected when it is accessed outside of the Company's office(s) by Company employees, including mobile devices, laptops, etc.

The Company President is responsible for authorizing each employee's access to Private Information. The Company has controls in place to prevent improper access of Private Information by all employees who have not been granted the appropriate security permissions. These controls are regularly tested by the Company President or their designee.

The Company's President documents the risk analysis results and records changes made to the Company's information security network or operations to eliminate or reduce risk for the Company. This documentation, including all change management records, is retained in a designated file as per the Company's document retention and destruction guidelines.

3.3 – Employee Training, Management and Responsibilities Procedures

Green Label Title, LLC ("the Company") is committed to protecting non-public, personal and/or sensitive information ("Private Information") as required by local, state, and federal law through its Information Security and Privacy Management policies. All Company employees are trained on the Company's Information Security and Privacy Management policies to ensure they fully understand the importance of adherence to the Company's policies and the protection of Private Information.

All Company employees have the responsibility to understand how to protect confidentiality, integrity, and availability of information systems. Awareness training improves the user's awareness of the company's Information Security policies and procedures and the need to protect information resources. Training makes the system users aware of their role in protecting information, their security responsibilities, defines the user's role in the security process and helps the user develop skills and knowledge so that they may perform their jobs securely.

New employee training: All employees hired by the Company or individuals employed on a temporary basis will undergo specific training programs relating to the Company's Information Security Program including the following subjects:

- Security Awareness;
- Risk Analysis;
- Privacy Issues;
- Clean Desk and Clear Screen Policy (procedure reference no. 3.4.1 herein)
- Identification of Private Information;
- Responsibilities every employee has to protect Private Information including controls and procedures to prevent Private Information disclosure to unauthorized parties;
- Consequences for non-compliance;
- Acceptable use of the Company's computer system, network, equipment, and devices;
- Proper use of computer networks and passwords;
- Methods for proper disposal of documents containing Private Information

New employees are given copies of all of the Company's policies and procedures relating to Information Security, Protection of Private Information and Acceptable Use of Information Technology on the first day of employment with the Company. An acknowledgment of receipt and comprehension of these procedures will be executed by the employee and maintained by the Company President or their designee.

All employees of the Company will be provided with updates to these policies immediately after the updates are made to these policies and procedures. Employees will receive training, at least annually, on the Company's information security policies and procedures and will complete a training acknowledgment form every time an updated training session is completed. An Information Security Training Log is maintained by the Company President or their designee.

Training that is performed at least annually and training of new employees will include the following items related to the information security policies:

- Security Awareness;
- Risk Analysis;
- Privacy Issues;
- Clean Desk and Clear Screen Policy (procedure reference no. 3.3.1 herein)
- Identification of Private Information;
- Protecting Private Information including controls and procedures to prevent Private Information disclosure to unauthorized parties;

- Consequences for non-compliance;
- Acceptable use of the Company's computer system, network, equipment, and devices;
- Proper use of computer networks and passwords;
- Methods for proper disposal of documents containing Private Information

3.4 – Information Security Procedures

Green Label Title, LLC (“the Company”) is committed to protecting non-public, personal, and/or sensitive information (“Private Information”) as required by local, state, and federal law. The Information Security Policy outlined herein has been adopted to ensure compliance with the applicable laws and to ensure Private Information is secure. The Company's Information Security Policy provides direction for managing and protecting the confidentiality, integrity and availability of all of the Company's information assets, including the Company's network, systems, equipment and other devices. The Company has several policies in place, including but not limited to the ones outlined herein to protect against unauthorized access to physical files and systems the Company uses to store or process Private Information is properly safeguarded.

1. Statement of Responsibility - The Company President is responsible for the administration of this policy and responsible for maintaining procedures; user access, updating systems and documentation; providing appropriate support and guidance; reviewing the policy annually;

Company employees are responsible for adhering to the policies and procedures for notifying the Company President of any issues or violations.

2. Violations - Employees found to be in violation of this policy are subject to disciplinary action that is commensurate with the severity of the violation.

3. User Access – The Office Manager and Company President determine the level of access for each employee of the Company and coordinate same with the staff of Cloudstar. Access is limited to only employees that need access to carry out their daily job functions. Access privileges are reviewed annually by the Company President. Access privileges are adjusted immediately anytime an employee is terminated or changes job functions and anytime contractor or third-party severs its relationship with the Company.

4. User IDs and Passwords – Unique user IDs and passwords are issued to all employees accessing the Company's systems. Each employee must safeguard their User ID and Password from all other persons including other employees. Compromised passwords must be reported immediately to the Company President. Systems are configured to record the user ID used to access them. Passwords must be at least seven (7) characters long and contain at least one Capital letter, one number and one special character. Monitors lock after five (5) minutes of inactivity requiring a password to unlock. Passwords must be changed every 60 days. After five (5) invalid login attempts the user ID will be suspended. It can only be re-activated by System Administrator.

5. Acceptable Use of Information Technology – See procedure reference no. 3.4.1 herein

6. Data Security – See **Clean Desk and Clear Screen Policy** (procedure reference no. 3.4.2) herein and **Data Security – Removable Media Policy** (procedure reference no. 3.4.3) herein

7. Data Backup – Servers are backed up daily via AccuTitle /Title Desktop's staff/system through their cloud based settlement software website in accordance with the terms of our agreement. AccuTitle/ Title Desktop application provides a redundant off-site duplicate database.

8. Physical Security - The Company limits access to its office to only those individuals who require access for legitimate business functions. Access to the office is limited including unique locks, key pad access, restricted access and alarm system. Restricted areas are marked by signage restricting access to authorized personnel only. If an employee with access rights is terminated or otherwise leaves employment of the Company, the Company President retrieves all office keys and terminates all access and passwords through administrative rites.

9. Electronic Security - Security Controls are in place to prevent unauthorized access, misuse, or corruption of Private Information by secure Cloudstar firewall tools with detection and prevention features, complex password protocols, Microsoft Security Essentials anti-virus software and secure Cloudstar email transmission. These controls are in place for the data-base/network access and email systems. These controls are in place for information during the electronic transmission of the data as well as when the information is held in storage.

10. Equipment - Employees may be granted use of the Company's equipment, including items such as laptops, smartphones containing the Company's email or other network information. The Company prohibits the use personal equipment to access the Company's data. All employees who have the authority to use equipment belonging to the Company off-site must immediately report loss or theft of these items to the Company President.

All equipment, hardware and software assigned to employees, contractors or other third-parties must be returned immediately upon their separation or termination from the Company.

11. Network Security Controls -

Firewall Protection - The Company uses firewalls to protect all network entry points The Company utilizes Cloudstar Firewall tools that include network intrusion detection and prevention features to protect the network. Our network is continuously monitored by Cloudstar who receives and re-acts to any alerts or intrusions detected.

Anti-Virus Protection - The Company uses Anti-virus Software to protect the Company's network systems (servers, workstations and laptops) and data against malicious threats. The Company utilizes Microsoft Security Essentials Anti-virus software to prevent, detect and eradicate threats to the network. Scans are set to run nightly with updates pushed automatically. Microsoft Security Essentials is installed for protection at the server level as well as individual workstations.

12. Remote user access ("Remote Access") – Remote Access to the Company's network and or data is strictly prohibited by employees. The Company President must approval any exceptions to this policy.

13. Wireless Devices – The Company strictly prohibits the use of Wireless Devices to access the network/database. The Company does not allow any personal devices such as laptops, computers mobile devices, smartphones, etc. to connect to our wireless network via the wireless technology or wired technology. Unless provided by the firm, no devices are allowed to connect to the enterprise network.

14. Separation of Duties – Cloudstar (outside IT Consultant) is not authorized to perform transactions within any of the Company’s systems that contain Private Information.

15. System Modifications - The Cloudstar (our IT Consultant) is responsible for performing regular updates to install patches and other software updates/fixes designed to keep systems current and to mitigate known security flaws. New or updated technology, including hardware or software, is tested before it is implemented. Updates made to software or hardware is documented and maintained by the Company President.

16. Additional Measures

The Company has the following additional policies in place to protect against additional information security concern:

- Risk Analysis and vulnerability testing;
- Access logging

3.4.1 – Acceptable Use of Information Technology Procedures

Green Label Title, LLC (“the Company”) has the following Acceptable Use of Information Technology Policy to ensure that the use of the Company’s electronic based communication systems and business equipment including e-mail, voice mail, and internet access and accounting systems is consistent with the business interests of the Company and in the interest of its clients.

1. Communications - All communications are the property of the company. They are business records and may have legal and operational effects identical to those of traditional hard copy documents. Accordingly, all electronic communications should be treated as though they may later be viewed by others. Employees should have no expectation that any information transmitted over company facilities or stored on company computers is or will remain private. The company may access, monitor, disclose or distribute any communication associated with any electronic equipment or system employed by the company. It is also possible that non-employees may gain access to company communications through on-line services or specific access to our hardware or systems. For these reasons, it is very important to use good judgment in creating, distributing and retaining e-mail, voice mail, internet/intranet or other electronic documents and messages.

Password protection is required for any of your network communications, and employees must follow all protocols and procedures. Never disclose your password to anyone unless that person has the proper clearance and a legitimate need to know. The Company President or their designee may authorize use of an employee’s password during temporary absences for illness or vacations. Passwords must be changed upon the employee’s return to work.

2. Conditions of Use of the Information Technology System

Definition: The term **Information Technology System** is used as a synonym for computers and computer networks used to store, retrieve, transmit, or manipulate data, but it also encompasses other information distribution technologies such as television and telephones.

The Information Technology Systems are the property of the company, and users should understand that any use of these systems is not private or confidential.

2.1. Prohibited Use of Information Technology Systems - Transmitting, storing or accessing obscene, vulgar, profane, insulting or offensive material or messages (such as ethnic slurs or sexually explicit words, photographs and/or drawings) or other material that could be construed as disparaging to any person based upon that person's sex, race, age, national origin, disability or religion.

Receiving, printing, transmitting, or otherwise disseminating proprietary data, client information, PII (personal identifiable information) company secrets, or other confidential information in violation of company policy or proprietary agreements is strictly prohibited. Downloading inappropriate material such as picture files, music files, or video files for personal use is also strictly prohibited.

The Company strictly prohibits the use of all Company equipment (internet, phone and email system) for personal use. The Company permits the use of personal cell or smartphones during breaks and lunch time.

3. Monitoring Usage of Information Technology Systems - The Company may, from time to time at its sole discretion, monitor use of the Information Technology Systems. Such monitoring may include the interception of telephonic communication and voicemail messages, printing and reading data files (including personal documents, E-mail, messages and attachments) and monitoring internet usage (including a review of time spent on the internet and a review of specific web sites visited).

4. Restricted Internet Traffic - The Company's Internet system is restricted and intended only for business purposes. The Company strictly prohibits the use of the Company internet system by employees for personal use. Employees are permitted to access the internet through personal smartphones or tablets during breaks and lunchtime. Our Cloudstar firewall restricts access to questionable sites and content.

5. Blogging Policy – The Company prohibits employees from blogging in the Company's name.

The above policy applies to all other forms of social networking media or technology on the Internet, radio, television or in print media. It is the company's right to protect itself from unauthorized disclosure of information or distribution of information or opinions that are detrimental to the company.

6.0 Software Code of Ethics - Unauthorized duplication of copyrighted computer software violates the law and is contrary to our company's standards of conduct. We disapprove of such copying and recognize the following principles as a basis for preventing its occurrences:

- The making or using of unauthorized software copies is not permitted under any circumstances.
- Legally acquired or purchased software required by the company will be provided to meet the legitimate software needs in sufficient quantities for company computers.

8.0 Violations - Employees who violate this policy are subject to disciplinary action including training, probation and termination.

3.4.2 - Clean Desk and Clear Screen Policy

Green Label Title, LLC (“the Company”) is committed to protecting non-public, personal and/or sensitive information (“Private Information”) as required by local, state, and federal law through its Information Security and Privacy Management policies. All employees are responsible for following the Clean Desk and Clear Screen Policy outlined herein to reduce the threat of a security breach, fraud and information theft of electronic and physical documents located on the Company’s premises.

1. Purpose - This policy will establish a culture of security and trust for all employees and clients by ensuring the company is taking the appropriate responsibility for the Private Information in its care. It reduces the risk of unauthorized access to, loss of, or damage to information, thereby reducing the chance of breach of client confidentiality and theft of intellectual property. Additionally, a clean desk will provide a professional and positive image to office visitors, including clients, by ensuring an appropriate office appearance while meeting health and safety considerations.

2. Responsibilities - The Company President is responsible for implementation and enforcement of this policy. All employees must comply with the terms of this policy as they pertain to their specific job responsibilities.

3. General Requirements - Each employee must:

- Lock, with Password Protection, the computer system every time a workstation is left unattended for any period of time.
- Set the computer's automatic locking feature to lock, with Password Protection, the idle computer after 15 minutes of system inactivity.
- Log off the computer system at the end of each work day.
- Remove all files, documents, and/or Information Technology (IT) devices containing Confidential Information, as further defined in the Company Information Security Policy, from the work space and lock these items in a drawer when the workstation is left unattended or at the end of the work day. The key for the locked drawer is to remain with the employee at all times and may not be left unattended. A second key for the locked drawer will remain with the Company President and may not be left unattended.
- Lock file cabinets or drawers containing Confidential Information when not in use.
- Keep the workstation and any other accessible areas clear from Sensitive Information. Sensitive Information is any privileged or proprietary information which, if compromised, could cause serious harm to the Company. This Sensitive Information may include, but is not limited to, user ids, passwords, and account numbers. This Sensitive Information is maintained and kept secure in the employee's locked desk and with a copy maintained in the Company President's secure file cabinet.
- Immediately remove printed documents that may contain Confidential Information from printers, copiers and/or facsimile machines and place these items into the appropriate secured physical file. These items may be temporarily secured in the employee's locked drawer referenced above until the time when said file is actively being processed, but must be put into the appropriate file before the end of the business day.

- Shred any document containing Confidential Information as soon as the document is no longer needed via our shredding vendor or the company shredding machine located in the office.

4. Enforcement - Employees are expected to follow the spirit and intent of this policy. Periodic sweeps of work areas may be conducted by the Company President or a designee to verify adherence to this policy. Violations of this policy may result in disciplinary actions, up to and including termination.

5. Revisions - This policy will be reviewed on an annual basis and appropriate changes will be made accordingly.

3.4.3 – Data Security- Removable Media

Green Label Title, LLC (“the Company”) is committed to protecting non-public, personal and/or sensitive information (“Private Information”) as required by local, state, and federal law through its Information Security and Privacy Management policies. All employees are responsible for following the Data Security Policy outlined herein to minimize the risk of loss or exposure of sensitive data maintained by the Company and to reduce the risk of acquiring malware infections on Company computers.

1. The Company prohibits the use of any removable media (i.e. – CDs, DVDs, Flash/Thumb drives) for the purpose of making a copy of Company data. Exceptions may be granted by President. Any such exceptions must be documented. Any removable media device should be encrypted to prevent access by unauthorized parties.
2. CDs and Flash/Thumb drives should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they should be locked in a secure location.
3. CDs and Flash/Thumb drives should be kept away from environmental hazards such as heat, direct sunlight and magnetic fields.
4. Critical computer equipment is protected by uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
5. Environmental hazards to hardware (i.e. – food, liquids, smoke, high or low humidity and extreme heat or cold) should be avoided.

3.4.4 - Information Sensitivity Policy

Green Label Title, LLC (“the Company”) is committed to protecting non-public, personal, and/or sensitive information (“Private Information”) as required by local, state, and federal law. The Information Sensitivity Policy outlined herein has been adopted to ensure employees understand what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the Company without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means, including: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect the Company Private Information, as defined below, (e.g., Confidential Information should not be left unattended in conference rooms).

Scope. All information is categorized into two main classifications:

- “Public Information” contains all information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the systems.
- “Confidential Information” contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Confidential Information also includes information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.
- A subset of Confidential Information is “Third Party Private Information”. This is Private Information belonging or pertaining to another corporation or individual which has been entrusted to the company by that third party under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive information to information about the fact that we have connected a supplier / vendor into a network to support our operations.

Company employees are encouraged to use common sense judgment in securing Confidential Information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, then the employee should contact the appropriate manager.

Sensitivity: Generally - The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these Sensitivity Guidelines as a reference only, as Confidential Information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of information in question.

- **Minimal Sensitivity:** General corporate information; some personnel and technical information. This information is to be designated and always treated as “Confidential”. All employees approved to view and access Non-Public Information may have access to and process this information. This information may be sent outside the office by U.S. Mail, encrypted email or overnight courier.
- **More Sensitive:** Business, financial, technical, and most personnel information. This type information is to be designated and treated as “Sensitive Confidential”. Access to and the processing of this information is restricted to employees assigned to process the file or task. This information may be sent outside the office to authorized recipients by encrypted email or overnight courier with a unique tracking number. This information

should be destroyed/shredded at the earliest point when it is no longer needed. Violators will be subject to discipline including termination.

- **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company is to be designated and treated as “most sensitive confidential”. Access to and the processing of this information is only authorized by the Company President. This information may only be sent outside the office by the Company President or his approved designee. Violations to this section, whether deliberate or inadvertent, are subject to termination. Retention and destruction of this information is at the sole discretion and direction of the Company President.

Information Sensitivity and Computer Usage - To minimize risk to the company from an outside business connection: Computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access corporate information, the amount of information at risk is minimized. The Company utilizes secure Cloudstar firewall tools with detection and prevention features, complex password protocols, Microsoft Security Essentials anti-virus software, AccuTitle/ Title Desktop’s redundant network backup procedures and secure Cloudstar email system.

Information Sensitivity and company-to-Other Business Connections - Connections, such as third-party service providers, must be set up to minimize the information available to other businesses. The company ensures that these third-party providers see only the information necessary to complete the contracted services.

Delivery of Sensitive Information - Sensitive information should always be delivered in person or by secure email.

Enforcement - Any employee found to have violated this policy may be subject to disciplinary action including training, probation and termination.

3.5 – Retention & Destruction of Private Information

Green Label Title, LLC (“the Company”) is committed to protecting non-public, personal, private and/or sensitive information (“Private Information”) as required by local, state, and federal law through its Information Security Program. The retention and destruction of Private Information in the Company’s care will be handled in accordance with the procedures outlined herein which have been derived in compliance with applicable law and contractual requirements.

The Company has created this Retention and Destruction of Private Information Procedure for all official documents containing, or suspected to contain, Private Information. All Company employees and contractors are informed of their responsibilities regarding the handling, protection and destruction of Private Information prior to being assigned any job duties that involve handling of same.

Definition of Private/Non-public Information for the purposes herein - Personally identifiable data such as information provided by a customer on a form or application, information about a customer’s transactions, or any other information about a customer which is otherwise unavailable to the general public. Private information includes first name or first initial and last

name coupled with any of the following: Social Security Number, driver's license number, state-issued ID number, credit card number, debit card number or other financial account number(s).

How Private Information is Obtained - Documents with Private Information are obtained by the Company within the course of its normal business operations. These procedures were created in accordance with the requirements of all applicable laws and contractual obligations to ensure that official records no longer needed are discarded at the appropriate time. The procedures provide guidelines concerning the length of time official records should be retained under ordinary business circumstances.

Retention and Destruction - When documents that may contain non-public personal information are determined to be no longer needed for the transaction or service for which it was provided will be destroyed by the company shredding machine or by Planet Shred, our third-party shredding vendor, who provides a certificate of destruction with each monthly pick-up. This type information must be placed in the locked collection bin provided by the shredding vendor at the earliest determination that the information is no longer required to be in paper form.

Hard drives located in the Company's equipment, including computers and copiers are removed and physically destroyed before equipment is disposed or reused. Hard drives located in equipment that has been leased by the Company are removed and physically destroyed prior to being returned. All other information technology media including stand-alone hard drives, tapes, flash drives, or other types of removable media include physically destroying hard drives or scratching the surfaces and breaking into pieces for media such as disks and CD-ROMs.

Inactive documents containing financial information, which may include account information, are retained indefinitely but always for a period of not less than seven (7) years. This type information is retained off-site in locked file cabinets until destruction is to occur. After this retention period, documents containing financial information will be placed in Planet Shred's locked collection bin until picked-up. Planet Shred provides a certificate of destruction for each pick-up. The Company President oversees this process and reviews the information annually for destruction.

Inactive documents containing personal information, which may include personnel records, are retained for a period of not less than seven (7) years. This type information is retained in locked file cabinets in the Company President's office until destruction is to occur. After this retention period, documents containing personal information will be placed in Planet Shred's locked collection bin until picked-up. Planet Shred provides a certificate of destruction for each pick-up. The Company President oversees this process and reviews this information quarterly as well as annually for destruction.

Old transaction files, or documents pertaining to those files, are retained for a period of not less than ten (10) years. Upon full completion of the file, paper files are scanned into AccuTitle/ Title Desktop and transfer to off-site storage with restricted access, security system and unique locks. After the retention period, paper copies of transactional files are placed in Planet Shred's locked shredder bin until picked-up. Planet Shred provides a certificate of destruction for each pick-up. The Company President oversees this process and reviews this information annually for destruction.

After this retention period, old transaction files will be reviewed annually by the Company President for eligibility for destruction. Eligible file will be picked and destroyed up by Planet Shred who provides a certificate of destruction.

3.6 – Overseeing Service Providers Policy

Green Label Title, LLC (“the Company”) is committed to protecting non-public, personal, private, and/or sensitive information (“Private Information”) as required by local, state, and federal law through its Information Security Program and written procedures. Any third-party service providers used by the Company that require access to Private Information will be subject to the oversight procedures outlined herein.

Third party service providers utilized by the Company to assist with operation or other business functions, and/or to provide services for real estate transactions may require access to non-public personal information in order to perform the services they provide. These vendors may include but are not limited to:

- Title Examiners;
- Surveyors;
- Shredding/Destruction Services;
- Credit Reporting Services;
- Information Technology Vulnerability Testing Companies
- Title Insurance Underwriters (Auditors and Agency Representatives)

The Company performs reasonable, due diligence checks on all vendors prior to use, which may include:

- background checks and/or reference checks;
- review of information policies and procedures, financial resources and references;
- review of outside audits or Statement on Standards for Attestation Engagements (SSAE-16);

The Company prefers to use known industry leaders for services provided. Vendors are required to maintain errors and omission coverage which, at a minimum, meet any state, industry, and contractually obligated requirements.

All third party service providers are required to execute a Confidentiality Agreement addressing the security and protection of Private Information before any services are provided and before access to potential Private Information is granted.

All third party vendors are required to maintain, at a minimum, the same information security procedures as the Company. The procedures include requirements for the vendor to maintain a written Information Security Program. The vendor’s program may include policies for:

- Physical and Electronic Security;
- Acceptable Use Policies;
- Password Policy;
- Business Continuity and Disaster Recovery Policies;
- Risk Analysis;

- Retention and Destruction;
- Security Awareness;
- Change Management

The Company President is responsible for managing all vendor relationships. These responsibilities include oversight of each vendor and ensuring that all of the vendor's insurance coverage declaration records maintained by the Company are kept up to date. This type information is retained in a designated file in the Company President's office. The Company President or their designee monitors the vendor's service level, pricing, and contractual obligations to ensure that the vendor is performing services securely, accurately, and professionally. Vendors are contractually obligated to the Company to remedy privacy or other performance requirements; otherwise they risk termination of services.

3.7- Data Breach Incident Reporting Policy

Green Label Title, LLC ("the Company") is committed to protecting non-public, personal, private or sensitive information ("Private Information") as required by local, state, and federal law through its Information Security Program and written procedures. Any data breaches or other information security incidents (intentional or unintentional) will be handled in accordance with the procedures outlined herein.

The Company has tools in place to limit its exposure to incidents involving data breaches or other inappropriate access to sensitive information including Cloudstar Firewall tools that log any intrusion attempts and provides an IP address including a timestamp, Microsoft Security Essentials anti-virus software for virus detection and prevention and SSL encryption prevents personal information from being transmitted in clear text avoid security incidents. The Company monitors external threats (attacks/intrusions) to its information network and systems by continuous monitoring by Cloudstar, our outside IT Consultant.

All employees are required to attend training regarding incident response as part of their Information Security Program training. This training includes information on how actual and suspected data-breach incidents are to be reported, investigated, and handled. Employees receive copies of all written policies and procedures relating to incident response as part of this training program.

When a potential attack or intrusion is discovered, Cloudstar receives notifications and responds according to the level of threat detected. Include who receives report of the attack internally. The staff of Cloudstar is responsible for collecting data for the incident response including audit trails and access logs. Investigations of incidents are handled by Cloudstar and when appropriate, escalates information relating to these attacks the Company President to determine whether the incident must be officially reported per federal, state, and local laws and/or contractual agreements.

Employees found in violation of any of the Company's information security policies will be subject to disciplinary action up to, and including, termination.

3.8 – Business Continuity & Disaster Recovery Plan

Green Label Title, LLC (“the Company”) has adopted the Business Continuity and Disaster Recovery procedures outlined herein as part of the Company’s Information Security Program. These procedures are in place to assist the Company in a timely resumption of business activities should it experience an unexpected information system failure, including emergency or disaster situations.

The Company’s Disaster Recovery Plan provides written instructions that address the prevention of interruptions to business activities and the timely resumption. It includes procedures to address recovery of electronic data from loss, damage, theft or compromise and includes plans for all of the Company’s critical business processes, physical facilities and equipment. Specific timelines for tasks to be completed and services recovered are outlined in the Disaster Recovery Plan and are prioritized by order of importance.

The Disaster Recovery Plan has been distributed to all employees that may be called upon to play an active role during an emergency situation. These employees, and their roles for executing the plan during a disaster recovery event, are further outlined within the Disaster Recovery Plan.

The Company’s Disaster Recovery plan includes current contact information for all employees, contractors, vendors, and clients. It is the responsibility of the Company President or their designee to keep the Disaster Recovery Plan’s contact information updated at all times.

The Disaster Recovery Plan includes a schedule of tasks and list of services (in order of priority) to be recovered. It also contains information regarding the testing schedule of the plan, including types of tests that may be performed and the frequency for which testing is completed. Documentation of testing performed for the Disaster Recovery Plan is included within the policies and procedures of the plan.

3.8.1 – Disaster Recovery Plan

Green Label Title, LLC (“the Company”) has adopted the Business Continuity and Disaster Recovery procedures outlined herein as part of the Company’s Information Security Program located in Appendix B. These procedures are in place to assist the Company in a timely resumption of business activities should it experience an unexpected information system failure, including emergency or disaster situations.

BEST PRACTICE FOUR (4) – SETTLEMENT POLICIES AND PROCEDURES

Definition: *Adopt standard real estate settlement policies and procedures that help ensure compliance with Federal and State Consumers Financial laws as applicable to the settlement process.*

Green Label Title, LLC Policy and Procedures: Green Label Title, LLC use of software and technology allows us to track a file through each step of the closing process and provide complete transparency of the work being done on each file. As such we are able to verify that each part of the closing process adheres to accurate company procedures and that check and balances are in place to monitor these procedures. These include:

- Obtaining proper information required prior to closing
- Up to date access to premium rate information
- Complete review of closing instructions
- Proper processing of mortgage payoffs
- Accurate disbursement of proceeds and handling of escrow funds
- Timely and accurate recording guidelines
- Conducts an updated title search prior to settlement

4.1 – RECORDING PROCEDURES

Green Label Title, LLC (“the Company”) has procedures to ensure the timely recording of all documents related to settlements conducted by the Company. These procedures meet all legal and contractual obligations as well as State, Federal, local, and industry standards and regulations that govern the settlement process.

The Company issues title insurance policies in connection with settlements conducted by the Company. The Company is responsible for the recording of all documents from the settlements it conducts.

Documents that need to be recorded from each settlement are delivered to the appropriate governmental office within forty-eight (48) of settlement or disbursement. Prior to such delivery the following procedures are followed:

1. Drafts of all documents (Deeds, Mortgages, etc.) that need to be executed and recorded pursuant to the title insurance commitment are reviewed and proofed by the Assistant Manager prior to settlement for the following:

- Documents are in appropriate format (size, margins, etc.) and correct order for the County/State;
- Document Date;
- Amount of Consideration;
- Names of grantee, grantor, mortgagor, mortgagee, etc.;
- Marital status of all natural persons;
- Tenancy;
- Representative capacity of individuals signing on behalf of entities;
- POA, Trust, Probate, Estate language, if applicable;
- Legal Description of the property;
- Parcel I.D.;
- Signatures and Witnesses;
- Notary/Acknowledgement clauses are complete and accurate;
- Return to name and address;
- Riders;
- Attorney/Preparer Certification;
- Affidavits

Any errors or omissions discovered with the document drafts are corrected prior to settlement.

2. Upon completion of each settlement conducted by the Company, the entire file is returned to the Assistant Manager along with the check(s) for recording fees, recording taxes and transfer taxes.

3. Within twenty-four (24) hours of settlement, the Assistant Manager reviews all of the executed documents to make sure they are the same as the drafts that were approved; that they were fully and properly executed and that they are ready for recording.

4. The Assistant Manager reviews the check(s) to make sure the payees and amounts are correct.

5. If any errors or omissions are discovered with the documents or checks, immediate measures taken to correct them.

6. Upon approval of the documents and check(s), copies are made for the file and transmitted daily by overnight courier with a return envelope to the appropriate county recorder's office.

7. The Company tracks all documents sent for recording to ensure timely recording. The Company retains all files during the recordation process in a designated locked file cabinet. Entries are made to the Document Recording Log and tracked daily by the Assistant Manager. The Assistant Manager monitors/reviews the outstanding check list and custom reports generated from Rynoh's reconciliation software that identifies recording checks outstanding for more than ten (10) days. The Assistant Manager contacts the county recorder's office for any file not return within the normal business cycle. The Assistant Manager requests a Post-Closing

update (rundown) to the title search to verify proper recordation and indexing and to determine any intervening matters exist.

8. If a document is rejected for any reason, it is returned immediately to the Assistant Manager who takes the necessary measures to correct the problem within two (2) business days. Once the problem has been corrected, the document is resubmitted without delay and in no case, no more than thirty (30) days.

9. All documents are returned to the Company after recording and delivered to the Assistant Manager. The Assistant Manager reviews the recorded documents to make sure they were recorded in the proper order and properly indexed by the Courthouse.

10. Copies of the documents with the recording stamps (date, time, book and page/instrument no.) are made for the file.

11. The policies and documents are prepared for delivery to the insured in accordance with procedure reference no. 5.1 herein.

12. The Company President reviews the Company's Document Recording Log monthly to ensure all documents are recorded. Any exceptions are addressed and resolved immediately.

4.2 – PRICING PROCEDURES

Green Label Title, LLC ("the Company") has procedures to ensure that customers are charged the correct title insurance premium and other charges for settlement services provided by the Company. Premiums and charges for services are determined by legal and contractual obligations as well as State, Federal, local, and industry standards and regulations which govern the settlement process.

1. The Company's Closers prepare the HUD-1 Settlement Statements and are responsible for ensuring the correct title insurance premium is charged for each transaction. At all times, Closers maintain access to the company's AccuTitle/Title Desktop settlement software and to the Underwriter's on-line rate calculator as well as complete copies of the current underwriter's Rate Manual(s). They are familiar with premiums, rules and discounts. Upon notification from the state or an underwriter that changes have been made to the Rates, the Closers are immediately provided with the new Rate Manual and the Company's settlement service software vendor is contacted to confirm they have updated their software.

2. The Company's underwriter's rates are incorporated into the Company's AccuTitle/Title Desktop settlement service software. The rates are identical to the ones provided to the settlement service software vendor by the underwriter. The software calculates the policy premium based on the policy types, amounts, rate type and endorsements entered by the Closer.

3. The Closers also utilize the underwriter's online rate calculator program to determine/double check the proper charges to collect on the HUD-1 settlement statement for the policy(ies), endorsements and Closing Protection Letter, if any. A printout from the settlement software or underwriter's online rate calculator program is maintained in the file to document the calculation.

4. Prior to settlement, each buyer/borrower is provided with notice of any Reduced Rates which provides them with notice of documentation that will entitle them to a reduced rate if the

documentation is provided to the Company prior to settlement. If the buyer/borrower provides such documentation prior to settlement, the Closer ensures that the applicable reduced rate is charged on the HUD-1 settlement statement. The settlement software's rate calculator program is utilized to verify the calculation and a printout is maintained in the file to document the calculation.

5. The Company's Closers are also responsible for ensuring all additional fees the Company collects for services (i.e. – Settlement Fee, Overnight Delivery, Wire Fees, Tax Certifications, Notary) are correctly charged for each transaction. Fees payable to third party service providers are charged in accordance with the third party service provider's invoice.

6. A post-settlement review of charges is performed by the Office Manager when preparing the monthly premium report of remittances due to the underwriter. If any over-charges are discovered, the Office Manager has the Company President review the file. If the Company President confirms there was an over-charge, a refund check is issued immediately and same is documented in the file.

7. If the Company's underwriter notifies the Company of an over-charge discovered during their processing of premiums and/or policy copies, the Company immediately issues a refund check and documents same in the file.

4.3 – RECORDING AND PRICING TRAINING

Green Label Title, LLC ("the Company") has policies and procedures relating to document recording and pricing of title insurance policies and settlement services to ensure a settlement process that is compliant with legal and contractual obligations as well as State, Federal, local and industry standards and regulations. All employees involved in the settlement process shall undergo initial and ongoing training with respect to the Company's recording and pricing procedures.

New employee training: All employees hired by the Company will undergo specific training programs including:

- Document recording policies and procedures;
- Pricing policies and procedures

New employees whose duties will include recording functions will have additional training on specific recording functions, including the use of recording checklists. These employees are given a copy of all the Company's recording policies and procedures, and recording checklists before they begin performing these duties for the Company.

New employees whose duties will include pricing functions, including post-closing rate/fee pricing verification functions, will have additional training on quality control checks and other rate pricing guidelines. These employees are given a copy of all the Company's policies and procedures, and will receive specific training on rate manuals and online calculators utilized by the Company before they begin performing these duties for the Company.

BEST PRACTICE FIVE (5) – TITLE PRODUCTION

Definition: *Adopt and maintain appropriate procedures for the production, delivery, reporting and remittance of title insurance policies designed to meet both legal and contractual obligations.*

Green Label Title, LLC Policy and Procedures: Green Label Title, LLC policy is to deliver all policies to customers within the guidelines set forth by the underwriters' agency contracts (generally by the end of the first full month following closing). Policies are prepared and delivered following review that all terms and conditions of the title insurance commitment have been satisfied and all closing documents and necessary releases have been recorded. The Company is an authorized title insurance agency/agent for Fidelity National Title Insurance Company, Stewart Title Guaranty Company, Westcor Land Title Insurance Company and First American Title Insurance Company.

5.1 – TITLE POLICY AND DELIVERY PROCEDURES

Green Label Title, LLC (“the Company”) shall issue and deliver all title insurance policies to the insured parties within thirty days of the later of (i) the date of settlement, or (ii) the date that the terms and conditions of the title insurance commitment are satisfied.

DAILY PROCEDURES

1. A title insurance commitment must be prepared and delivered to all proposed insured parties before settlement is conducted and any title insurance policy is delivered to them. When the Company is conducting settlement in connection with the transaction, the commitment is delivered at least five business days prior to settlement.
2. All title insurance commitments are prepared after a careful examination of the title and determination of insurability in strict accordance with the Company's underwriter guidelines by one of the Company's authorized signatories.
3. Settlement may be scheduled and conducted once the Company is satisfied that all commitment requirements have been met or will be met at settlement.

4. After settlement is conducted, the file is reviewed by the Closer immediately after disbursement of the settlement funds.

5. The commitment is marked-up by the Closer to identify which requirements and exceptions on Schedules B-I and B-II have been satisfied and which ones will remain on the final policies as exceptions.

6. If additional documentation is needed for any of the commitment requirements, the file processor works to obtain same.

7. Once all of the requirements on Schedule B-I have been marked-up as being satisfied, the Office Manager reviews the title insurance policy section of the loan closing instructions; generates the necessary policy jackets via the underwriter's online system and prepares the policy schedules and endorsements in accordance with the loan closing instructions.

8. After the policies are prepared, the Office Manager signs the policy or gives the entire file to an authorized policy signatory. Within five days of receiving the file, the authorized signatory reviews the file along with the prepared policies. If there are any issues detected by the authorized signatory, they will meet with the Closer to resolve them.

9. Once the authorized signatory is satisfied that the file is complete and all of the title insurance commitment conditions and requirements have been met, the policies and endorsements are signed and the file is then returned to the Office Manager.

10. The Office Manager types cover letters to be sent to the insured parties with the original policies and original, recorded insured instruments (Deeds and/or Mortgages).

11. Two copies of the policies and endorsements are made. One copy is maintained in the file, the other copy and it is placed a secure file labeled "Underwriter Policy Copies" which contains copies of all policies issued during the month.

12. The original, recorded Deed and Owner's Policy, if any, are mailed to the purchaser.

13. The original, recorded Mortgage and Loan Policy are overnighted to the address provided in the loan closing instructions. The tracking number of the overnight package is maintained in the file.

Note about ALTA Short Form Residential Loan Policies:

If the property is a One-to-Four Family Residence and the lender's closing instructions call for an ALTA Short Form Residential Loan Policy; the policy is typed, reviewed and signed immediately after settlement and sent to the lender with the closing package in accordance with the loan closing instructions.

MONTHLY PROCEDURE

The Office Manager monitors policy issuance via reports from the Company's settlement software and its underwriter to ensure compliance with these procedures.

5.2 – PREMIUM REMITTANCE AND POLICY REPORTING PROCEDURES

Green Label Title, LLC (“the Company”) shall report all title insurance premiums and policies to the underwriter(s) within the time frame required by the underwriter agency contract(s) and within the time frame required by any state statute or regulation.

DAILY PROCEDURES

1. Whenever a settlement is conducted in connection with a title insurance commitment issued by the Company, a check payable to the title insurance underwriter for their portion of the policy premium, endorsement premium(s), if any, and Closing Protection Letter fee, if any, is cut when the file is disbursed. The check is kept in the file and both are returned to the file processor.
2. The Office Manager enters the policy details in the underwriter’s Monthly Premium Report (“MPR”) system; ensures that the check amount matches the calculation by the underwriter’s system. The Office Manager places the check in a secure file labeled “Underwriter Remittance” which contains all checks made payable to the underwriter during the month.

MONTHLY PROCEDURES

1. During the first week of each month, the Company President prints a report of all title insurance settlements conducted the previous month along with the underwriter’s MPR system report for that month. The Company President compares the two reports to each other to make sure there are no discrepancies then compares the checks in the “Underwriter Remittance” file to the reports to make sure all files and checks are accounted for.
2. The Company President compares each check in the Underwriter Remittance file to the underwriter’s MPR system report to make sure each check amount matches the MPR system calculation. The Company President also sums up all of the checks to make sure the total sum matches the total on the MPR report. Any differences are researched and corrected.
3. Having confirmed all of the title insurance files from the previous month are included on the underwriter’s Monthly Premium Report and all of the checks are for the correct amounts, the bookkeeper prepares an overnight package with Monthly Premium Report and checks. The bookkeeper then gathers all of the policy from the Underwriter Policy Copies file; creates a list of the file numbers and policy numbers then places the copies in the overnight package as well.

4. The policy copies, Monthly Premium Report and checks are overnighted to the underwriter so that they receive it by the last day of the month.
5. The Company President places copies of the Monthly Premium Report, policy copy list and overnight air bill in a file containing the underwriter's name and year.
6. If the underwriter contacts the Company with any questions or additional documentation requests, the Company President addresses same within 48 hours.

QUARTERLY PROCEDURES

The Company President reviews a Policy Status Report and a Premium Variance Report from the underwriter to make sure if there are discrepancies that need to be reconciled. Files shown as not reported yet are researched to determine if they are canceled or still pending. Any file determined to have been canceled is then reported as such to the underwriter. Any discrepancies shown on the premium variance report are researched and rectified, if necessary.

BEST PRACTICE SIX (6) – ERRORS AND OMISSIONS AND FIDELITY COVERAGE

Definition: *Maintain appropriate levels of professional liability and fidelity coverage to ensure the financial capacity to stand behind the professional services provided.*

Green Label Title, LLC and Procedures: Green Label Title, LLC consistently maintains all levels of insurance as required by underwriters and lenders and that is comparable to the complexity, nature and scope of our operations. Coverage is held for professional liability and fidelity coverage (including employee theft) as well as any additional bond coverage that may be required by the state of New Jersey.

6.1 – E & O INSURANCE RENEWAL PROCEDURES

Green Label Title, LLC (“the Company”) shall maintain appropriate levels of Professional Liability/Errors & Omissions Insurance to ensure the Company has the financial capacity to stand behind its professional services and to ensure compliance with state regulations and underwriter agency contracts.

The Company has a current Professional Liability/Errors & Omissions Policy insured through Lloyd’s of London with an effective date of 10/12/2015 and an expiration date of 10/12/2016. The policy’s retro-active date is 10/12/2009. The policy limits are \$ 1,000,000 each claim and \$1,000,000 aggregate. The deductible amount is \$5,000. The policy specifically includes Title Agent, Closing Agent and Escrow Agent in the definition of “professional services.”

ANNUAL PROCEDURES

1. The Company President maintains a complete copy of the policy in a secure file in their office. Sixty days prior to the expiration date of the policy, the Company President reviews the applicable state regulations and underwriter agency agreement(s) to determine if any requirements have changed.
2. The Company President reviews the definition of “professional services” in the policy to determine if the policy provides adequate coverage for the Company’s current scope of operations. Any additional coverage deemed necessary is requested at the time of renewal.

6.2 – FIDELITY BOND RENEWAL PROCEDURES

Green Label Title, LLC (“the Company”) shall maintain a Fidelity Bond to provide coverage for employee dishonesty/crime in compliance with any state regulations and underwriter agency agreements. Currently, the state of New Jersey or its underwriters require licensed title agents (producers) to maintain a Fidelity Bond (employee dishonesty coverage) but the Company recognizes the importance of maintaining the coverage.

The Company has a current Fidelity Bond #ESB10995 through Lloyd's of London in the amount of \$500,000 with an effective date of 07/13/2015 and an expiration date of 07/13/2016. The deductible amount is \$15,000.

ANNUAL PROCEDURES

1. The Company President maintains a complete copy of the Fidelity Bond in a secure file in their office. Sixty days prior to the expiration date of each Bond, the Company President reviews the applicable state regulations and underwriter agency agreements to determine if any requirements have changed.
2. After reviewing the applicable state regulations, underwriter agency agreements and existing Bonds, the Company President completes renewal applications at least thirty days prior to the expiration of the current Bonds.

BEST PRACTICE SEVEN (7) – CONSUMER COMPLAINTS

Definition: *Adopt and maintain procedures for receiving and addressing consumer complaints so that any instances of poor service or non-compliance do not go undiscovered.*

Green Label Title, LLC Policies and Procedures: Green Label Title, LLC is very sensitive to any complaints that are made. Any and all complaints received by an employee are to be forwarded to our Company President for immediate resolution. This resolution will always include a follow up to not only the customer but also their loan officer to ensure that it is agreed that the issue has been resolved. In certain cases, the complaint is discussed with an employee regarding the circumstances causing the complaint and a review of Green Label Title, LLC policies and procedures. All activity is logged and placed in the corresponding transactional file.

7.1 – CONSUMER COMPLAINT INTAKE, RECORDATION AND RESPONSE PROCEDURES

Green Label Title, LLC (“the Company”) is dedicated to providing excellent client satisfaction and customer service. In an effort to ensure that complaints are addressed as efficiently and effectively as possible, the Company has a written Consumer Complaint Policy and procedures for the intake, recordation and response to client and customer complaints.

The Company has a written Consumer Complaint Policy that all employees must follow to ensure an effective and consistent way for dealing with client and customer complaints. The policy is made available to customers at settlement.

The written Consumer Complaint Policy is reviewed annually by all employees.

The definition of the term complaint is defined under the Complaint Resolution Policy as an expression of dissatisfaction or concern expressed by a client or customer regarding the services, operating procedures, staff, vendors, or complaint handling process.

1. Each complaint received is directed to the Company President who completes a Complaint Intake Form that includes:

- Date of complaint;
- Contact information of the consumer or person making the complaint;

- File number; name and/or policy number;
- Brief description of the complaint;
- Brief description of the resolution requested;
- Amount of fees associated with the transaction (if complaint is related to fees);
- Employee assigned to;
- Summary of Resolution;

2. The Company President also logs all complaints on the Company's Consumer Complaint Log which is used to identify open complaints.

3. The Company President assigns an employee to investigate and resolve each complaint within 24 hours of receipt.

4. The designated employee is provided with a copy of the Complaint Intake Form.

5. The designated employee locates the relevant file(s); reviews the relevant documentation; determines a proper resolution and carries out the action(s) necessary to resolve the complaint.

6. In the event that the employee is unable to resolve the complaint to the customer's satisfaction, the Company President will review the matter and re-assign it or assume the responsibility.

7. Upon resolution of the complaint (or inability to resolve), the employee completes the Summary of Resolution section of the Intake Form and returns it along with the supporting documentation, if any, to the Company President.

8. Complaint records are retained for a period of 5 years.

7.2 – COMPLAINT RECORDS PROCEDURES

Green Label Title, LLC ("the Company") is dedicated to providing excellent client satisfaction and customer service. In an effort to ensure that complaints are addressed as efficiently and effectively as possible, the Company records all complaints and tracks them. Lenders will be permitted to see complaint records related to their loans.

All complaints received by the Company are logged on the Company's Consumer Complaint Log which is used to track the status of each complaint.

The Log is maintained by the Company President .

7.3 – ANALYSIS AND SELF-ASSESSMENT PROCEDURES

Green Label Title, LLC ("the Company") is dedicated to providing excellent client satisfaction and customer service. In an effort to ensure that complaints are addressed as efficiently and effectively as possible, the Company reviews and analyzes the handling of complaints so adjustments to operations and procedures can be made as warranted.

The Company President and Company President review and analyze the Company's handling of consumer complaints in accordance with the Company's written consumer complaint policy on a semi-annual basis.

The purpose of the semi-annual review is to identify trends and types of risks (i.e. – legal, regulatory, reputation, financial, etc.) to determine if any changes need to be made to the Company's policies and procedures.

7.4 – CONSUMER COMPLAINT TRAINING PROCEDURES

Green Label Title, LLC (“the Company”) is dedicated to providing excellent client satisfaction and customer service. In an effort to ensure that complaints are addressed as efficiently and effectively as possible, all employees receive annual training on the Company's Consumer Complaint Policy.

New employee training: All employees hired by the Company will undergo specific training programs including:

- Consumer Complaint Policy
- Complaint Intake, Recordation and Response;
- Investigating and Resolution

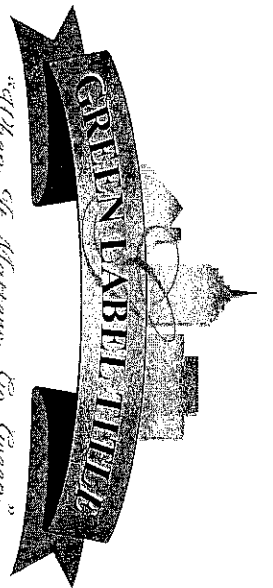
New employees are given a copy of all of the Company's policies and procedures, including a copy of the Company's Complaint Resolution Policy. An acknowledgment of receipt and comprehension of these procedures will be executed by the employee and maintained by the Company President.

All employees will be provided with updates to policies and procedures, including the Company's Complaint Resolution Policy, immediately after the updates are made to the policies and procedures. Employees will receive training, at least annually, on the Company's Complaint Resolution Policy and each employee will complete a training acknowledgment form every time an updated training session is completed. A Complaint Resolution Training Log of the trainings will be maintained by the Company President.



APPENDIX A

LICENSES



TITLE LICENSE LOG

<u>Date reviewed</u>	<u>Initials</u>	<u>Date reviewed</u>	<u>Initials</u>	<u>Date reviewed</u>	<u>Initials</u>
10/03/15	EA				



State of New Jersey

Department of Banking and Insurance
20 West State Street
Trenton, NJ 08625-0327

LICENSE NUMBER
1229764

THIS CERTIFIES THAT **GREEN LABEL TITLE, LLC**

AT BUSINESS ADDRESS 2517 HIGHWAY 35
BUILDING B SUITE 103
MANASQUAN, NJ 08736

This insurance license is valid and shall remain in effect unless revoked or suspended provided that the fee set forth in N.J.A.C. 17:27-2.12 is paid and renewal requirements set forth in N.J.A.C. 17:27-2.5, including continuing education requirements for resident individuals, are met by the license expiration date. A renewal notice will be mailed to the licensee mailing address approximately 30 days prior to the license expiration date.

IS DULY LICENSED WITH THE FOLLOWING LICENSE TYPE(S) AND AUTHORITIES

LICENSE TYPE	LINES OF AUTHORITY	EFFECTIVE DATE	EXPIRATION DATE
PRODUCER	TITLE INSURANCE	06/01/2015	05/31/2017

printed: 05/06/2015

K. S. Koyan
Commissioner of Banking and Insurance

The Department maintains an informative website at www.dobi.nj.gov. Please visit this web page for valuable information and forms necessary to maintain compliance with licensing requirements.

Department Contact Information

web site: www.dobi.nj.gov
phone: (609) 292-4337
fax: (609) 984-5263

The request for any change of license information must be sent to the Department within 30 days of the change.

Make any checks and/or money orders payable to: **STATE OF NEW JERSEY, GENERAL TREASURY**

Mailing Address: Department of Banking and Insurance
20 West State Street
P.O. Box 327
Trenton, NJ. 08625-0327



State of New Jersey

Department of Banking and Insurance
20 West State Street
Trenton, NJ 08625-0327

LICENSE NUMBER
0220162

THIS CERTIFIES THAT **STEVEN M. GREEN**

AT BUSINESS ADDRESS GREEN LABEL TITLE, LLC
2517 HIGHWAY 35 STE 103
MANASQUAN, NJ 08736-1918

This insurance license is valid and shall remain in effect unless revoked or suspended provided that the fee set forth in N.J.A.C. 11:17-2.12 is paid and renewal requirements set forth in N.J.A.C. 11:17-2.5, including continuing education requirements for resident individuals, are met by the license expiration date. A renewal notice will be mailed to the licensee mailing address approximately 30 days prior to the license expiration date.

IS DULY LICENSED WITH THE FOLLOWING LICENSE TYPE(S) AND AUTHORITIES

LICENSE TYPE	LINES OF AUTHORITY	EFFECTIVE DATE	EXPIRATION DATE
PRODUCER	TITLE INSURANCE	11/01/2014	10/31/2016

printed: 10/06/2014

R. S. K... ..
Commissioner of Banking and Insurance

The Department maintains an informative website at www.dobi.nj.gov. Please visit this web page for valuable information and forms necessary to maintain compliance with licensing requirements.

Department Contact Information

web site: www.dobi.nj.gov
phone: (609) 292-4337
fax: (609) 984-5263

The request for any change of license information must be sent to the Department within 30 days of the change.

Make any checks and/or money orders payable to: **STATE OF NEW JERSEY, GENERAL TREASURY**

Mailing Address: Department of Banking and Insurance
20 West State Street
P.O. Box 327
Trenton, NJ. 08625-0327



State of New Jersey

Department of Banking and Insurance

20 West State Street
Trenton, NJ 08625-0327

LICENSE NUMBER

9842544

This insurance license is valid and shall remain in effect unless revoked or suspended provided that the fee set forth in N.J.A.C. 11:17-2.12 is paid and renewal requirements set forth in N.J.A.C. 11:17-2.5, including continuing education requirements for resident individuals, are met by the license expiration date. A renewal notice will be mailed to the licensee mailing address approximately 30 days prior to the license expiration date.

THIS CERTIFIES THAT **ROBYN A. CAMPANILE**

AT BUSINESS ADDRESS GREEN LABEL TITLE LLC
2517 HIGHWAY 35
BLDG B SUITE 102
MANASQUAN, NJ 08735

IS DULY LICENSED WITH THE FOLLOWING LICENSE TYPE(S) AND AUTHORITIES

LICENSE TYPE	LINES OF AUTHORITY	EFFECTIVE DATE	EXPIRATION DATE
PRODUCER	TITLE INSURANCE	04/01/2014	03/31/2016

printed: 05/02/2014

R. S. K. A.
Commissioner of Banking and Insurance

The Department maintains an informative website at www.dobi.nj.gov. Please visit this web page for valuable information and forms necessary to maintain compliance with licensing requirements.



State of New Jersey
 Department of Banking and Insurance
 20 West State Street
 Trenton, NJ 08625-0327

LICENSE NUMBER
1016159

THIS CERTIFIES THAT **CHERYL L. DE NOIA**

AT BUSINESS ADDRESS GREEN LABEL TITLE LLC
 2517 ROUTE 35
 BUILDING B SUITE 102
 MANASQUAN, NJ 08736

This insurance license is valid and shall remain in effect unless revoked or suspended provided that the fee set forth in N.J.A.C. 11:17-2.12 is paid and renewal requirements set forth in N.J.A.C. 11:17-2.5, including continuing education requirements for resident individuals, are met by the license expiration date. A renewal notice will be mailed to the licensee mailing address approximately 30 days prior to the license expiration date.

IS DULY LICENSED WITH THE FOLLOWING LICENSE TYPE(S) AND AUTHORITIES

LICENSE TYPE	LINES OF AUTHORITY	EFFECTIVE DATE	EXPIRATION DATE
PRODUCER	TITLE INSURANCE	10/01/2015	09/30/2017

printed: 10/02/2015

K. S. Kohler
 Commissioner of Banking and Insurance

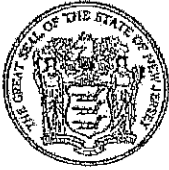
The Department maintains an informative website at www.dobi.nj.gov. Please visit this web page for valuable information and forms necessary to maintain compliance with licensing requirements.

Department Contact Information
 web site: www.dobi.nj.gov
 phone: (609) 292-4337
 fax: (609) 984-5263

The request for any change of license information must be sent to the Department within 30 days of the change.

Make any checks and/or money orders payable to: **STATE OF NEW JERSEY, GENERAL TREASURY**

Mailing Address: Department of Banking and Insurance
 20 West State Street
 P.O. Box 327
 Trenton, NJ. 08625-0327



State of New Jersey

Department of Banking and Insurance

20 West State Street
Trenton, NJ 08625-0327

LICENSE NUMBER
9826532

THIS CERTIFIES THAT **PHILIP J. GILBERT**

AT BUSINESS ADDRESS 1410 PAUL BLVD
MANAHAWKIN, NJ 08050-4135

This insurance license is valid and shall remain in effect unless revoked or suspended provided that the fee set forth in N.J.A.C. 11:17-2.12 is paid and renewal requirements set forth in N.J.A.C. 11:17-2.5, including continuing education requirements for resident individuals, are met by the license expiration date. A renewal notice will be mailed to the licensee mailing address approximately 30 days prior to the license expiration date.

IS DULY LICENSED WITH THE FOLLOWING LICENSE TYPE(S) AND AUTHORITIES

LICENSE TYPE	LINES OF AUTHORITY	EFFECTIVE DATE	EXPIRATION DATE
PRODUCER	TITLE INSURANCE	02/01/2014	01/31/2016

printed: 01/22/2014

K. S. Koyan
Commissioner of Banking and Insurance

The Department maintains an informative website at www.dobi.nj.gov. Please visit this web page for valuable information and forms necessary to maintain compliance with licensing requirements.

Department Contact Information

web site: www.dobi.nj.gov
phone: (609) 292-4337
fax: (609) 984-5263

The request for any change of license information must be sent to the Department within 30 days of the change.

Make any checks and/or money orders payable to: **STATE OF NEW JERSEY, GENERAL TREASURY**

Mailing Address: Department of Banking and Insurance
20 West State Street
P.O. Box 327
Trenton, NJ. 08625-0327



State of New Jersey
 Department of Banking and Insurance
 20 West State Street
 Trenton, NJ 08625-0327

LICENSE NUMBER
1294939

This insurance license is valid and shall remain in effect unless revoked or suspended provided that the fee set forth in N.J.A.C. 11:17-2.12 is paid and renewal requirements set forth in N.J.A.C. 11:17-2.5, including continuing education requirements for resident individuals, are met by the license expiration date. A renewal notice will be mailed to the licensee mailing address approximately 30 days prior to the license expiration date.

THIS CERTIFIES THAT **BARBARA J. KIZIS**

AT BUSINESS ADDRESS GREEN LABEL TITLE
 2517 ROUTE 35
 MANASQUAN, NJ 08736-1918

IS DULY LICENSED WITH THE FOLLOWING LICENSE TYPE(S) AND AUTHORITIES

LICENSE TYPE	LINES OF AUTHORITY	EFFECTIVE DATE	EXPIRATION DATE
PRODUCER	TITLE INSURANCE	10/01/2014	09/30/2016

printed: 09/30/2015

K. S. Kozlowski
 Commissioner of Banking and Insurance

The Department maintains an informative website at www.dobi.nj.gov. Please visit this web page for valuable information and forms necessary to maintain compliance with licensing requirements.

Department Contact Information
 web site: www.dobi.nj.gov
 phone: (609) 292-4337
 fax: (609) 984-5263

The request for any change of license information must be sent to the Department within 30 days of the change.

Make any checks and/or money orders payable to: **STATE OF NEW JERSEY, GENERAL TREASURY**

Mailing Address: Department of Banking and Insurance
 20 West State Street
 P.O. Box 327
 Trenton, NJ. 08625-0327



APPENDIX B

NOTAIRES

STATE OF NEW JERSEY NOTARY PUBLIC COMMISSION
THIS IS TO CERTIFY THAT
STEVEN MCGREEN
WHO RESIDES IN OCEAN COUNTY
IS COMMISSIONED A NOTARY PUBLIC
DECEMBER 8, 2012 TO DECEMBER 8, 2017
BY JUDITH A. WOODRUFF
SIGNATURE
2294544
STATE TREASURER
COMMISSION NUMBER

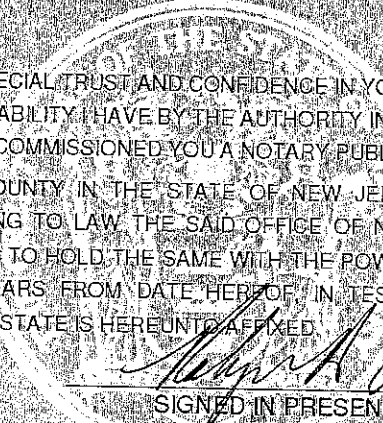
THIS DOCUMENT IS PRINTED ON WATERMARKED PAPER WITH A MULTI-COLORED BACKGROUND AND MULTIPLE SECURITY FEATURES TO ENSURE AUTHENTICITY

I.D. NO
2104709
FROM
SEPTEMBER 30, 2012
EXPIRES
SEPTEMBER 30, 2017
ROBYN A CAMPANILE

State Of New Jersey
Notary Public Commission

REPOSING SPECIAL TRUST AND CONFIDENCE IN YOUR INTEGRITY, PRUDENCE AND ABILITY, I HAVE BY THE AUTHORITY INVESTED IN ME BY LAW COMMISSIONED YOU A NOTARY PUBLIC OF

OCEAN COUNTY IN THE STATE OF NEW JERSEY TO EXECUTE AND PERFORM ACCORDING TO LAW THE SAID OFFICE OF NOTARY PUBLIC OF SAID STATE TO HAVE AND TO HOLD THE SAME WITH THE POWERS AND RIGHTS FOR A PERIOD OF FIVE YEARS FROM DATE HEREOF, IN TESTIMONY WHEREOF THE GREAT SEAL OF THE STATE IS HEREUNTO AFFIXED.



Robyn A. Campanile
SIGNED IN PRESENCE OF COUNTY CLERK

In Witness Whereof, I have hereunto set my hand and affixed the Official seal

Andrew P. Sidamon-Eristoff
Andrew P. Sidamon-Eristoff
State Treasurer

STATE OF NEW JERSEY NOTARY PUBLIC COMMISSION
THIS IS TO CERTIFY THAT
ROBYN A. CAMPANILE
WHO RESIDES IN OCEAN COUNTY
IS COMMISSIONED A NOTARY PUBLIC
SEPTEMBER 30, 2012 TO SEPTEMBER 30, 2017
AND DATE
Robyn A. Campanile
SIGNATURE
2104709
I.D. NUMBER
STATE TREASURER
Andrew P. Sidamon-Eristoff

PLEASE DETACH HERE
Do not detach until validated
by county clerk.

I.D. NO.
2431270

State Of New Jersey
Notary Public Commission

FROM
MARCH 14, 2013
EXPIRES
MARCH 14, 2018

CHERYL L DENOIA

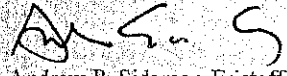
REPOSING SPECIAL TRUST AND CONFIDENCE IN YOUR INTEGRITY,
PRUDENCE AND ABILITY I HAVE BY THE AUTHORITY INVESTED IN ME BY
LAW COMMISSIONED YOU A NOTARY PUBLIC OF

OCEAN COUNTY IN THE STATE OF NEW JERSEY TO EXECUTE AND
PERFORM ACCORDING TO LAW THE SAID OFFICE OF NOTARY PUBLIC OF SAID
STATE TO HAVE AND TO HOLD THE SAME WITH THE POWERS AND RIGHTS FOR A
PERIOD OF FIVE YEARS FROM DATE HEREOF, IN TESTIMONY WHEREOF THE
GREAT SEAL OF THE STATE IS HEREUNTO AFFIXED.



SIGNED IN PRESENCE OF COUNTY CLERK

In Witness Whereof, I have hereunto set my hand and affixed the Official seal



Andrew P. Sidamon-Eristoff
State Treasurer

THIS DOCUMENT IS PRINTED ON WATER MARKED PAPER WITH A FULL COLORED BACKGROUND AND A SECURITY FEATURE PLEASE VERIFY AUTHENTICITY

I.D. NO:
2359076
FROM:
APRIL 25, 2012
EXPIRES:
APRIL 25, 2017
LINDA ANN DIMODICA

State Of New Jersey
Notary Public Commission

REPOSING SPECIAL TRUST AND CONFIDENCE IN YOUR INTEGRITY,
PRUDENCE AND ABILITY I HAVE BY THE AUTHORITY INVESTED IN ME BY
LAW COMMISSIONED YOU A NOTARY PUBLIC OF

MONMOUTH COUNTY IN THE STATE OF NEW JERSEY TO EXECUTE AND
PERFORM ACCORDING TO LAW THE SAID OFFICE OF NOTARY PUBLIC OF SAID
STATE TO HAVE AND TO HOLD THE SAME WITH THE POWERS AND RIGHTS FOR A
PERIOD OF FIVE YEARS FROM DATE HEREOF, IN TESTIMONY WHEREOF THE
GREAT SEAL OF THE STATE IS HEREUNTO AFFIXED.

Linda Ann Dimodica
SIGNED IN PRESENCE OF COUNTY CLERK

In Witness Whereof, I have hereunto set my hand and affixed the Official seal

Andrew P. Sidamon-Eisstoff
Andrew P. Sidamon-Eisstoff
State Treasurer

STATE OF NEW JERSEY NOTARY PUBLIC COMMISSION
THIS IS TO CERTIFY THAT
LINDA ANN DIMODICA
WHO RESIDES IN MONMOUTH COUNTY
IS COMMISSIONED A NOTARY PUBLIC
APRIL 25, 2012 TO APRIL 25, 2017

VALID DATES

SIGNATURE

Linda Ann Dimodica

2359076

PLEASE DETACH HERE

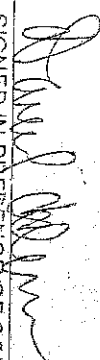
Do not detach until validate
by county clerk.

EXPIRES: AUGUST 8, 2014
AUGUST 8, 2019

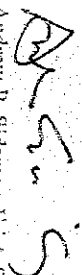
ANIEL V COLEMAN

REPOSING SPECIAL TRUST AND CONFIDENCE IN YOUR INTEGRITY,
PRUDENCE AND ABILITY I HAVE BY THE AUTHORITY INVESTED IN ME BY
LAW COMMISSIONED YOU A NOTARY PUBLIC OF

MONMOUTH COUNTY IN THE STATE OF NEW JERSEY TO EXECUTE AND
PERFORM ACCORDING TO LAW THE SAID OFFICE OF NOTARY PUBLIC OF SAID
STATE TO HAVE AND TO HOLD THE SAME WITH THE POWERS AND RIGHTS FOR A
PERIOD OF FIVE YEARS FROM DATE HEREOF, IN TESTIMONY WHEREOF THE
GREAT SEAL OF THE STATE IS HEREUNTO AFFIXED.


SIGNED IN PRESENCE OF COUNTY CLERK

In Witness Whereof, I have hereunto set my hand and affixed the Official seal


Andrew P. Sidamon-Hristoff
State Treasurer

THIS DOCUMENT IS PRINTED ON WATERMARKED PAPER WITH A MULTI-COLORED BACKGROUND AND MULTIPLE SECURITY FEATURES TO ENSURE AUTHENTICITY.

I.D. NO.
2191160
FROM:
JULY 24, 2011
EXPIRES:
JULY 24, 2016
PHILIP GILBERT

State Of New Jersey
Notary Public Commission

REPOSING SPECIAL TRUST AND CONFIDENCE IN YOUR INTEGRITY,
PRUDENCE AND ABILITY I HAVE BY THE AUTHORITY INVESTED IN ME BY
LAW COMMISSIONED YOU A NOTARY PUBLIC OF

OCEAN COUNTY IN THE STATE OF NEW JERSEY TO EXECUTE AND
PERFORM ACCORDING TO LAW THE SAID OFFICE OF NOTARY PUBLIC OF SAID
STATE TO HAVE AND TO HOLD THE SAME WITH THE POWERS AND RIGHTS FOR A
PERIOD OF FIVE YEARS FROM DATE HEREOF. IN TESTIMONY WHEREOF THE
GREAT SEAL OF THE STATE IS HEREUNTO AFFIXED.

Philip Gilbert

SIGNED IN PRESENCE OF COUNTY CLERK

In Witness Whereof, I have hereunto set my hand and affixed the Official seal

Andrew P. Sidamon-Eristoff
State Treasurer



STATE OF NEW JERSEY NOTARY PUBLIC COMMISSION
THIS IS TO CERTIFY THAT
PHILIP GILBERT
WHO RESIDES IN OCEAN
COUNTY IS COMMISSIONED A NOTARY PUBLIC
JULY 24, 2011 TO JULY 24, 2016

SIGNATURE
Philip Gilbert

PLEASE DETACH HERE
Do not detach until validated
by county clerk.



STATE OF NEW JERSEY NOTARY PUBLIC COMMISSION

THIS IS TO CERTIFY THAT

SCOTT MEAGLESON

WHO RESIDES IN MORRIS

IS COMMISSIONED AS A NOTARY PUBLIC

MAY 30, 2013 TO MAY 30, 2016



Scott Meagleson
SUPERVISOR

2434689

STATE ID NUMBER

ASIS

QUALIFIED

6/7/13

JOAN BRAMHALL MORRIS COUNTY CLERK

BY

A handwritten signature in black ink, appearing to be 'Joan Bramhall', written over a horizontal line.

Special Deputy Clerk

THIS DOCUMENT IS PRINTED ON WATERMARKED PAPER WITH A MULTICOLORED BACKGROUND AND MULTIPLE SECURITY FEATURES. PLEASE VERIFY AUTHENTICITY.

State of New Jersey
Notary Public Commission

ID NO:
2395694
FROM
APRIL 23, 2015
EXPIRES
APRIL 23, 2020
BARBARA KIZIS



REPOSING SPECIAL TRUST AND CONFIDENCE IN YOUR INTEGRITY, PRUDENCE AND ABILITY, I HAVE BY THE AUTHORITY INVESTED IN ME BY LAW COMMISSIONED YOU A NOTARY PUBLIC OF

MONMOUTH COUNTY IN THE STATE OF NEW JERSEY TO EXECUTE AND PERFORM ACCORDING TO LAW THE SAID OFFICE OF NOTARY PUBLIC OF SAID STATE TO HAVE AND TO HOLD THE SAME WITH THE POWERS AND RIGHTS FOR A PERIOD OF FIVE YEARS FROM DATE HEREOF IN TESTIMONY WHEREOF THE GREAT SEAL OF THE STATE IS HEREUNTO AFFIXED.

SIGNED IN PRESENCE OF COUNTY CLERK

In Witness Whereof, I have hereunto set my hand and affixed the Official seal

Andrew P. Stenison
Andrew P. Stenison-Eristoff
State Treasurer

APR 09 2015

SWORN IN OFFICE



APPENDIX C

E&O Insurance and Escrow Bond



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
10/5/2015

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Stewart Specialty Insurance Services 1980 Post Oak Blvd #R2C Houston TX 77056		CONTACT WILL ELIZONDO PHONE (A/C No. Ext): (866) 798-2827 FAX (A/C No.): (713) 985-1061 E-MAIL ADDRESS: welizond@stewart.com	
INSURED Green Label Title, LLC 2517 Highway 35 Building B, Suite 103 Manasquan NJ 08736		INSURER(S) AFFORDING COVERAGE INSURER A: UNDERWRITERS AT LLOYDS INSURER B: INSURER C: INSURER D: INSURER E: INSURER F:	

COVERAGES CERTIFICATE NUMBER: CL1210504911 REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
	GENERAL LIABILITY <input type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input type="checkbox"/> LOC						EACH OCCURRENCE \$ DAMAGE TO RENTED PREMISES (Ea occurrence) \$ MED EXP (Any one person) \$ PERSONAL & ADV INJURY \$ GENERAL AGGREGATE \$ PRODUCTS - COMP/OP AGG \$ \$
	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> HIRED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS						COMBINED SINGLE LIMIT (Ea accident) \$ BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
	UMBRELLA LIAB EXCESS LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> CLAIMS-MADE DED RETENTION \$						EACH OCCURRENCE \$ AGGREGATE \$ \$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below						<input type="checkbox"/> Y <input type="checkbox"/> N N/A WC STATUTORY LIMITS OTH-ER E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
A	PROFESSIONAL LIABILITY			STEO 1473-1504 RETRO DATE: 10/12/2009	10/12/2015	10/12/2016	\$1,000,000 PER CLAIM \$5,000 \$1,000,000 AGGREGATE RETENTION

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)
 The insurance afforded by this policy applies solely to wrongful acts in the insured's performance of professional services for others for a fee as title agent, abstractor and escrow/closing agent.

CERTIFICATE HOLDER Green Label Title, LLC	CANCELLATION SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE Will Elizondo/SW <i>Will Elizondo</i>
---	---

Escrow Security Bond Certification

Stewart Title Guaranty Company

hereby certifies that

Green Label Title, LLC

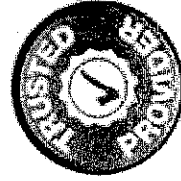
has been issued an Escrow Security Bond by underwriters at Lloyds of London[®]
through Stewart Specialty Insurance Services with a term from
July 13, 2015 to July 13, 2016

This bond may provide coverage of up to \$500,000 to protect
against loss of settlement funds due to acts such as:

- Cyber theft
- Employee theft
- Embezzlement
- Computer fraud
- Fictitious write-offs
- Diversion schemes
- Partner/principal theft
- Payable fraud
- Receivable fraud



Patrick Beall, Group President
Stewart Title Guaranty Company



stewart
Vetted and verified.



©2013 Stewart. Trademarks are the property of their respective owners. This information provides a brief description of typical coverage and is not meant to describe actual coverage under any escrow security bond. Coverages, discounts, and billing options are subject to state availability, individual qualification, and/or the insuring company's underwriting guidelines. Terms, conditions, limits, and exclusions may apply. Rates are subject to change.

ESCROW SECURITY BOND

Bond No.
ESB 10995

COURT COSTS AND ATTORNEYS FEES REDUCE AND MAY EXHAUST THE COVERAGE LIMITS AND ARE SUBJECT TO THE DEDUCTIBLE. SUBSECTIONS (2), (3) AND (4) OF INSURING AGREEMENT (G) ARE LIMITED TO LIABILITY FOR ONLY THOSE CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED DURING THE BOND PERIOD.

DECLARATIONS

Item 1. Name of Insured (herein called Insured): Green Label Title, LLC

Principal Address: 2517 Highway 35, B103
Manasquan, NJ 08736

Item 2. Bond Period: from 12:01 a.m. on 07/13/2015 and 12:01 a.m. on 07/13/2016 standard time at the Principal Address as to each of said dates.

IMPORTANT: UNLESS CANCELLED OR TERMINATED AT AN EARLIER DATE, THIS POLICY DEFINITELY EXPIRES ON THE DATE STATED ABOVE WITHOUT FURTHER NOTICE BY OR ON BEHALF OF THE UNDERWRITERS.

Item 3. Aggregate Limit of Liability and Deductible Amount

Subject to Sections 8 and 9 hereof, the Limit of Liability is \$ 500,000 in the aggregate (referred to in this bond hereinafter as the "Aggregate Limit of Liability") and Deductible Amount is \$ 15,000 each and every loss.

Item 4. Offices Covered--

The offices of the Insured covered under this Bond are:

- (a) all of its offices, established or to be established, which are located in the United States of America and Canada, and,
- (b) the office or offices of the Insured outside the United States of America or Canada and located as follows:

Item 5. The liability of the Underwriters is subject to the terms of the following riders attached hereto:

NMA 2918 08/10/2001, LMA 5090, NMA 1256, NMA 1477, LMA 5020, LMA 5021, BEJ&H DISCOVERY LIMITATION CLAUSE, NMA 358, LSW 1001, STEWART LPAY, SETTLEMENT 1, PCS1, SEC1, AGG1, SLC-3 (USA) NMA 2868 (24/08/2000), C250

Item 6. The Insured by the acceptance of this Bond gives notice to the Underwriters terminating or canceling prior Bond(s) or policy(ies) No.(s) such termination or cancellation to be effective as of the time this Bond becomes effective.

Item 7. Retroactive Date: 07/13/2015

Item 8. Notice pursuant to Sections 5, 9(c), and 12(a):

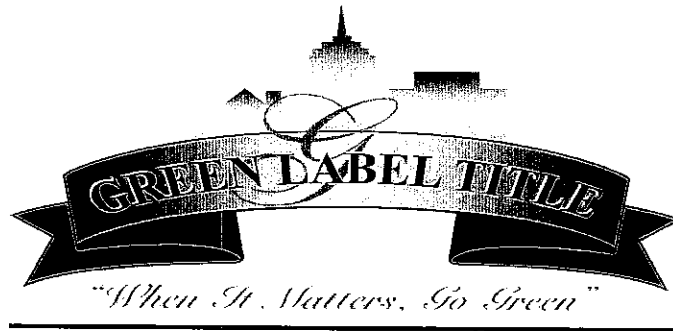
Stateside Underwriting Agency
265 Exchange Drive, Suite 101
Crystal Lake, IL 60014
P: 815-759-6800

=====



APRENDIX D

Information Technology to include NPI data security



ITEM 9 – INVENTORY

Green Label Tile, LLC is fully based in “Cloud” operations. Therefore our databases, relevant information and operational procedures are accessible from any location, anywhere at any time.

Green Label Title’s operation is not dependent upon a server, or standalone computers, so we are able to operate and conduct business from any location at any point from around the world. Our files are scanned into our cloud based system and we are able to access and recover from any location.

These “cloud based” systems are password protected and require login information in accordance with CFPB and REPA compliance standards.

There are several workstations and multi-functioning printers at the emergency location and every employee. Also have a multifunctioning offsite location

Handwritten initials "AT" inside a circle, positioned above a horizontal line.

Intials



General Information
Information Technology

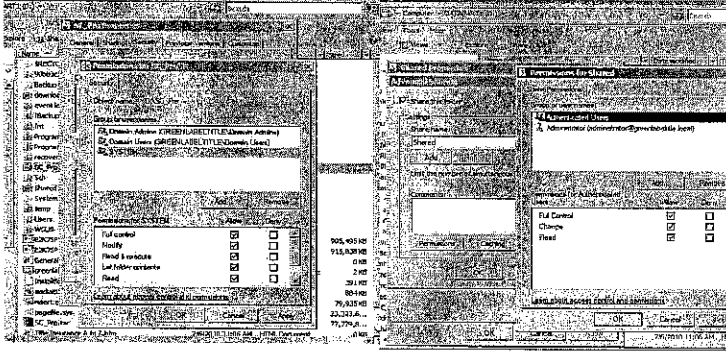
Agent Name: _____

Audit Date: _____

1. List all network drives and/or folders containing clients Non-public Personal Information (NPI).

Network Drives	Folders
D:\	SC_Pro
D:\	Shared

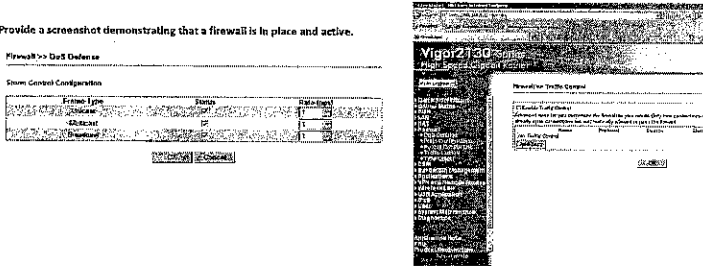
2. Provide screenshots from the network drive(s) and/or folders listed above showing all individual users (with in usegroups if applicable) with



3. If customer NPI is stored in any systems or applications other than the network drives and/or folders listed above provide a user access listing

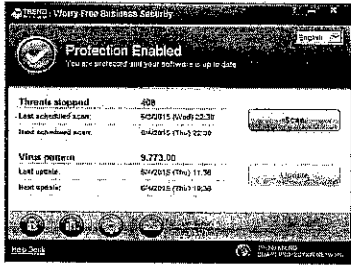
Employee / User Name	Access
Steph Chase Pro	Domain Admins & Domain Users

4. Provide a screenshot demonstrating that a firewall is in place and active.



5. Provide a name of your Anti-virus software being used and provide a screenshot showing that it has been updated within the last week. Then Micro Business Security

Denial of Service is on As you can see No ports are open for any incoming con



Completed by (please print): _____

Signature: _____

Position held within company (if completed by 3rd party provide name of company): _____ Cloudstar Nationwide Services

Date: _____

Channel	Channel 11, 2462MHz
Extension Channel	Channel 7, 2442MHz
Ix Power	100%
Enable Green AP	<input type="checkbox"/>
Enable IGMP Snooping	<input type="checkbox"/>

Isolate LAN: Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.
 Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

- SSID 1
- SSID 2
- SSID 3
- SSID 4

Wireless Security Configuration

Encryption WPA-PSK

WPA-PSK Configuration

Type Auto(WPA or WPA2)

WPA Algorithm TKIP

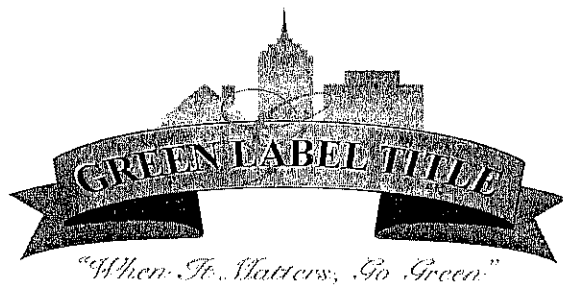
WPA Pre-Shared Key ●●●●●●●●

OK



APRENDIX E

Disaster Recovery Plan



Policy	Green Label Title ("the Company") has adopted the Business Continuity and Disaster Recovery procedures outlined herein as part of the Company's Information Security Program. These procedures are in place to assist the Company in a timely resumption of business activities should it experience an unexpected information system failure, including emergency or disaster situations.
Name of Procedure	Disaster Recovery Plan
Reference Number	3.8.1
Applicable Parties	All Employees and Contractors
Effective Date	10/03/2015
Supporting Documentation	List supporting documentation, if any Contact lists of vendors, employees and applicable parties

Procedures

1. Emergency Declaration

Who may declare an emergency?

President _ Steven Green
Office Manager - Robyn Campanile

When will an emergency be declared?

If a State of the Emergency has been issued, Governmental or State; if we are under terroristic attack or wartime declarations; in the event of disaster or an eminent emergency situation; or any circumstance deemed to be detrimental to the welfare of our employees

What is the time period that will elapse before an emergency is declared?

As soon as management is made aware of the situations listed above; the time period is not to exceed 90 minutes from the time the situation or circumstance is discovered.

This should be a reasonable period of time, generally not a brief disruption in service. How often will the staff responsible be for declaration of the emergency review updates to determine if the situation necessitates declaration of an emergency.

What steps are taken during this monitoring period to continue business activities as possible?

Company procedures and operations are conducive to employees working from safe, remote locations; in the event that the disaster or disruption of business is known, employees are permitted to take home any required information, upon manager's inspection and approval, which may permit continued working procedures and business operations. When conditions are unknown; company has procedures in place (such as Cloud access) to enable business operations to continue from safe, remote locations

Procedures Continued

What is the company's overall estimated time frame for resumption of full business activity once an emergency has been declared?

Estimated down time should not exceed 60 minutes from the time disruption/emergency is first discovered.

2. Critical Processes

The following is a list of critical company processes, by order of importance, as determined by the appropriate management.

List processes and services your company performs by order of importance.

These processes and services may involve:

Issuing closing and payroll checks.

Closing transactions

Title searches;;

Policy issuance

Securing the office

Procedures
Continued

3. Critical Applications and Software

List Applications and Software your company uses in order of importance, such as:

The internet;
Email;
Telephones;
Voice mail;
Title and Closing Software; and
Fax, Mail, and Overnight Delivery Packages.

Include services that will be used to notify clients and staff of the emergency situation.

Notifications will be sent via e-mail, text and telephone calls

4. Backup Procedures

How is your company's network information backed up?

Network is located in the Cloud and is backed up continuously by Cloudtsar (E-mail and IT company) as well as Accutitle (software provider) on secure nonpublic servers

Where is this backup information stored?

Backup information is stored on secured Cloud location with above referenced providers

How will this information be accessed in the event of an emergency?

Our Cloud based system and technology allows us to access this information from any location, with approved login credentials (issued by management) Our office has continual, exclusive access and rights to the information from any location with secured internet access

Who has the authority to access these backups?

The owner and President, Steven M. Green

How frequently is your backup method tested and where are the results of these tests maintained?

Backups are tested on a monthly basis and maintained with our IT provider (Copy of the results is sent to us and maintained in a secure location).

5. Key Personnel

List the key personnel required to enact portions of the DR Plan. This section

Procedures
Continued

should include detailed information as to each staff member's role in the plan and the steps they will take. Include contact information for these key staff members, including home and cell phone information.

Steven Green - President
Steve@Greenlabeltitle.com
Cell - 732-674-4390 Home - 732-608-7098

Robyn Campanile - Office Manager
Robyn@Greenlabeltitle.com
Cell - 732-610-5648

Cheryl DeNoia - Assistant Manager
Cheryl@Greenlabeltitle.com
732-600-8416

For each key personnel team member, be sure to name at least one secondary person to fulfill this role in case an important person is unavailable.

Roles that may need to be filled during a disaster can include:

Who can declare a disaster;
IT Personnel;
Management responsible for communication with staff;
Staff responsible for client communications; and
Staff person responsible for media communications, if needed.

6. Personnel

7. Contact Information

This section must contain contact information for:

Clients (generally outlined in your client contract); and
Important vendors such as delivery services (Fed Ex, USPS, UPS, etc.)
Information technology suppliers (including those that will provide your office with hardware), office equipment, and any other vendor that would either assist in the emergency or that would need to be notified of the emergency (to temporarily halt service or re-direct delivery.);
All other third parties that would need to be notified of an emergency event.

Management has the proper contact information for vendors and suppliers, which are contained in privately locked files; it will be the managements responsibility to contact these vendors to advise them of situations arising from the above

8. Contingency Facilities

In the event your current operations location is unavailable, where will your staff, computer equipment, and IT Hardware be located to assist your company resume the available business functions.

Satellite office located at:
2069 Basswood Court, Toms River NJ 08755

Who are the individuals and their contact information that are responsible for readying this space?

Steven M Green - President

How much equipment is available and how many of your staff will this location house?

Location Houses 4 work stations, unlimited Wi-Fi access, and enough space to house 15-20 staff members, clients and customers at any given time

Include a map and directions to the facility as part of this plan. If attached to the plan, be sure to reference the attached map.

9. Inventory

Reference and attach a list of your office Information Technology inventory including:

Computers;
Phones;
Printers; and

The locations in which these items are used or stored.

List items kept only for Disaster Recovery purposes which are stored in an off-site location and specify where these items are kept. Include information as to how these items will arrive at the Contingency location if they are not already in that space.

Each item should include serial numbers, owner (if not owned by the company), and all other equipment specific information. Like the employee list, this needs to be updated frequently, annually at minimum.

10. Data Restoration

This section will contain detailed information regarding the backup restoration process for all processes within the company.

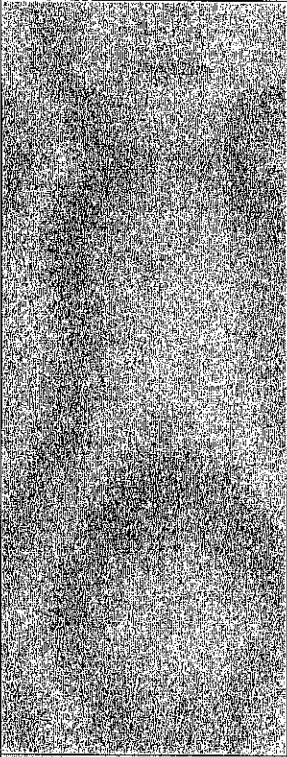
Using the processes, services, application and software information detailed above and create a step-by-step guide that will need to be followed in order to restore the critical operations for your office.

This section should include detailed information as to the expected resumption time frame for each critical business process. Remember the overall timeframe referenced above and ensure your individual time frames in this section meet the overall resumption expectations.

See appendix for offsite operations

11. Plan Testing

What is the scheduled frequency of the testing of your DR plan?

	<p>Testing is conducted Weekly or shorter on an as needed basis</p> <p>What types of testing has occurred?</p> <p>Said testing will occur on a quarterly basis but be supplemented by monthly use of equipment and operational procedure testing and use</p> <p>Our office conducts walk tough testing on a weekly basis; a checklist is comprised on any ongoing issues or issues that may become a problem</p> <p>What are the results of each DR test?</p> <p>Optimal</p> <p>Date and document changes made to DR plan based upon each test finding.</p> <p>How often have you tested the DR Plan with your staff Included should be results of previous testing and documentation as to how findings were corrected and changes implemented.</p> <p>Our plan is tested monthly and reviewed weekly at office meetings and staff assessment reviews.</p>
	<p>Approved by _____ (Title)</p>
	<p>Approval date _____</p>



"When It Matters, Go Green"

DISASTER RECOVERY PLAN

PURPOSE

This Disaster Recovery Plan (Tian") document is intended to provide information on the steps and procedures to be taken in the event of a manmade or naturally occurring emergency or disaster affecting the business operations of (Green Label Title, LLC, company). The Plan's purpose is to ensure the safety and wellbeing of our employees and the orderly continuation of the Company's business, including the ability to service the needs of our customers with minimal disruption and delay. This document outlines the processes and procedures that will be implemented in the event of an emergency or disaster.

Different types of emergencies and disasters require varying degrees of response, from damage to a critical server, to a short-term, single site incident affecting our Company, only; to large scale, regional disasters of a relatively long duration affecting not only the company but other businesses and governmental agencies in the area This Plan cannot foresee and address all possibilities but is intended to address those risks the Company's management team believes to be most likely to occur and of greatest risk to the Company's operations_

We provide all .employees with copies of this plan and any updates within 5 days of employment, and obtain signed acknowledgements of receipt for retention in their personnel files. We will practice the procedures outlined herein once a year and maintain a record of the date, participants and results of each training exercise.

EMERGENCY RESPONSE TEAM

In the event of a major, or eminent emergency situation our emergency response team will be responsible for properly activating, and administering the disaster plan in conjunction with the Emergency response Team Coordinator

Emergency Response Team Coordinator – **Steven M Green**

The Emergency response Team Coordinator is responsible for approving the Plan and updates to the Plan in the event of an emergency, he/She has the sole authority to invoke and execute the plan. The following person is the designated Emergency Response Team Plan Coordinator: 1

Steven m. Green
Address 2069
Basswood Court,
Toms River, NJ 08753
Phone 732-608-7098
Mobile Phone 732-674-4390
Steve@Greenlabeltitle.com
Greenpossible@gmail.com

in the event he/she is not available or is unable to respond to an emergency for any reason, the following Person shall act in his place:

Robyn Campanile
Address: 4 Alfred
Drive, Toms River NJ
Office -732-722-7323
Mobile 732-610-5648
Robyn@Greenlabeltitle.com

Information. Technology Steven M. Green, Cloudstar Consulting and R19

Due to the Company's reliance on technology to efficiently operate its business, the following person has been assigned responsibility for assuring the redundancy of the company's computer and telephone communications systems to prevent the loss of data and provide for the restart of the Company's electronic communications capabilities within the timeframes specified herein:

Cloudstar Consulting IT Manager
800-340-5780
support@mycloudstar.com

R19 – Phones
Ryan McShea
Hytec Telephone/ R-19
1900 Atlantic Ave
Manasquan NJ, 08734
Direct: 732-292-6796
Support: 732-528-0555

The IT coordinator will work directly with the Emergency Response Team Coordinator (or agency management) in planning the resumption of business services.

Business Continuity Planning Team Members

The members of this team are responsible for overseeing the deployment of this Plan within their area of responsibility.

Individual Contact information Area of Responsibility

Steven Green
732-674-4390
President

Robyn Campanile
732-610-5648
Office Manager

Cheryl DeNoia
732-600-8416
Assistant Office Manager

EVACUATION ROUTINE

In the event of a natural or man-made disaster that necessitates evacuating our building such as fire or bomb threat, the following procedures will be followed:

Declaration of Event and Order to Evacuate

The Emergency Response Team Coordinator or in his/her absence, the Alternate Emergency Response Team Coordinator will determine if an event has occurred that necessitates evacuation of the building. Once an event has been declared, the Emergency Response Team Coordinator will issue a warning and will then immediately contact the fire and/or police department.

Warning — A warning will be issued advising all occupants that there is an event requiring them to leave the building;

Exiting the Building

If instructions are given to evacuate the building, employees must use the stairs or fire escape to exit the building

Assembly Site:

2069 Basswood Court, Toms River, NJ

Reopening for Business

Once the event is determined to be over the Emergency Response Team Coordinator will make the decision whether to reopen for business and allow employees back to their workplaces.

Insurance Coverage:

The Emergency Response Team Coordinator will determine if any damage to the building or operations occurred that may be covered under any of the Company's insurance policies.

SHELTER IN BUILDING PLAN

In the event of a natural or man-made disaster that requires us to shelter the building, such as a tornado or terrorist threat external to the building

Following procedures will be followed:

Declaration of Event and Order to Move to the Shelter Location:

The Emergency Response Team Coordinator or, in his/her absence, the Alternate Emergency Response Team Coordinator will determine if an event has occurred that necessitates sheltering within the building. Once an event has been declared, the Emergency Response Team Coordinator will issue a warning and will contact the fire and/or police department if appropriate to do so.

Warning. A warning will be issued advising all occupants that there is an event requiring them to seek shelter;

Shelter Location 2514 Highway 34, B103, Manasquan, NJ 08736

Note: If the event is an earthquake, all employees are to immediately seek shelter under the nearest sturdy table or desk. If one is not nearby, crouch in the nearest corner using your arms to cover your head and face. Doorways should only be used for shelter if they are known well to be in a supporting wall. Do not shelter **near a** window or other potential sources of broken glass.

Reopening for Business

Once the event is determined to be over the Emergency Response Team Coordinator will make the decision whether to reopen for business and allow employees back to their workplaces.

Insurance Coverage:

The Emergency Response Team Coordinator will determine if any damage to the building or operations occurred that may be covered under any of the Company's insurance policies.

VITAL RECORDS PRESERVATION PLAN

This section of the Disaster Recovery Plan is designed for the protection and preservation of all vital information and critical data (including Green Label Title), both in electronic and hard copy forms. This would include any important papers and / Or files, as well as any vital information that is saved electronically. This operation will be coordinated with the Emergency Response Team Coordinator (or agency management) and the IT Coordinator.

1

Company data is backed up on a daily basis to a remote server located with Cloudstar or

1

Vital Paper Files and Documents

Company data is locked up daily by Steven Green and a copy of the backed up data is maintained at the company's offsite location

Employees are required to backup all critical data stored on their personal computers every 1 day

Physical files are maintained in our office in a locked file room, or locked file cabinet, or at a secure off-site facility

Vital paper documents and files are scanned on a daily basis. Copies of the scanned documents are maintained on our remote server located a Planet Shred or with our daily backed up data

Once a disaster is eminent and the Plan has been activated, the following procedures will be initiated:

Phone/communications calls are laced to employees and vendors advising of the situation

Protection protocols are initiated

Management ensures communication a disaster relief protocols are followed

Electronic Data Processing

The Emergency Response Team (ERT) will be informed of the existing situation and immediately begin the gathering, securing and transferring process (to either our off-site storage area, or the emergency operations location)

When possible, computer hardware will be secured and prepared (by the Qualified people) for movement to 2069 Basswood Court, Toms River, NJ 08755

If our computer hardware has been destroyed or become otherwise unusable, our IT Coordinator will immediately begin the process offering our system from

the backup at 2069 Basswood Court, Toms River, NJ 08755

if possible, all important paper files will be included in the transfer to (2069 Basswood Court, Toms River, NJ 08755. This includes copies of our insurance policies, banking information and a copy of our disaster recovery.

TELEPHONE NUMBERS FOR EMPLOYEES, VENDORS AND CONTRACTORS

In the event there is a disaster (or that a disaster strike is eminent) below is the list of employee, vendor, and emergency personnel contact numbers. This will allow our Emergency Response Team Coordinator (or agency management) to properly and efficiently complete their respective responsibilities.

Emergency Contacts

Employee Steven Green

732-674-4390

Local Police (732) 223-1000

Fire and Rescue 732-223-1599

Ambulance and Fire and

Sheriff – 732-223-1000

Poison Control

Utilities) Vendor JCP&L

(732) 223-1000

Title insurance Underwriter

Westcor Land Title

732.576.1870

First American

609-528-6860

Fidelity National

732-545-1003

Stewart Title

800-858-6842

Computer Equipment

www.mycloudstar.com

1-800-340-5780 Option 1

Telephone Equipment

Ryan McShea

Hytec Telephone/ R-19

1900 Atlantic Ave

Manasquan NJ, 08734

Direct: 732-292-6796

Support: 732-528-0555

Fax: 732-528-4853

www.r-19.com

www.hytectelephone.com

Office Equipment

Shore Business Solutions

732-780-1333

Security and Alarm Services

ADT

877-473-9434



APRENDIX F

Consumer Complaint Policy

Consumer Complaint Policy

Purpose

Green Label Title (“the Company”) endeavors to be responsive to clients and customers and to quickly and fairly address any concerns or complaints the client and customer may have. The Company recognizes a client and customer’s right to make a complaint about the conduct of the Company’s operations, services, staff, or third-party vendors, where that client and customer’s interests appear to have been adversely affected.

The purpose of the Complaint Resolution Policy is to protect the client and customer’s rights, including the right to comment and complain; provide an efficient and fair process for resolving client and customer complaints; and to monitor complaints in an effort to improve the quality of operations and services the Company provides. This policy will provide the Company an opportunity to provide service and satisfaction to dissatisfied clients and clients and customers; ensure a consistent method of management; monitoring, and reporting of complaints; and identify areas that need improvement.

Definitions

Complaint: An expression of dissatisfaction or concern regarding the services, operating procedures, staff, vendors, or complaint handling process made by a client and client and customer.

Complainant: The person making the complaint.

Client and customer: The person or entity receiving advice, a service, or otherwise engaged in a business relationship with the Company.

Complaint Log: Electronic or paper records of all incoming complaints, including information on the complainant and resolution of complaint.

Complaint Process

Clients and customers should initially direct their concerns to Steven M Green, Steve@Greenlabeltitle.com, and 732-722-7373. The complaint should be made in writing, including means of electronic communication such as email, or via the Company’s website; www.Greenlabeltitle.com

Response to complaints

A Consumer Complaint Intake Form will be opened for each complaint and all complaints will be logged into the Company’s complaint log. The Office Manager or Assistant Office manager will attempt to resolve the complaint within the first contact, when possible, and will respond to the client and client and customer’s concerns within 1-2 business day of the initial complaint. At the time of the first contact, the Office Manager or Assistant Office Manager will inform the client and customer if more time will be needed to research the complaint.

Unresolved Complaints

If the complaint is still unresolved after communication with the Office Manager or Assistant Office Manager, or if the initial complaint is not addressed in a timely manner, the complainant may contact the Company’s President. The President will then contact the client and customer and endeavor to resolve the complaint within 1 business days after being contacted.

Complaint Log Review

The Company’s complaint log will be regularly reviewed to identify areas of the Company’s operations and services that may require improvement. The Company President will research reoccurring complaint matters and recommend process and procedure changes, when appropriate. These changes will be noted on the Complaint Resolution Log, and any necessary Company Policy and Procedure updates will be made within 2 business days thereafter.

- COMPLAINT RESOLUTION LOG AVAILABLE UPON REQUEST

COMPLAINT SHEET

DATE: _____ 2015

FILE NO: GL- _____

NAME OF PARTY: _____

CONTACT INFO: _____

ISSUE: _____

RESOLUTION: _____

EMPLOYEE: _____

MANAGEMENT ACKNOWLEDGEMENT: _____

Entered into Log: _____



APENDIX G

Privacy Policy (s)

Green Label Title's Privacy Policy

Effective January 29, 2015

Green Label Title respects the privacy and security of your non-public personal information (NPI) and is dedicated to ensuring financial protection for our policyholders and others with whom we do business with by providing quality products and exceptional service.

In order to provide quality products and services, we may require access to certain NPI which is personally identifiable data such as information provided by a customer on a form or application, information about a customer's transactions, or any other information about a customer which is otherwise unavailable to the general public. While access to NPI may be critical, the protection of that information is equally important.

NPI includes first name or first initial and last name coupled with any of the following: Social Security Number, driver's license number, state-issued ID number, credit card number, debit card number, or other financial account numbers.

Green Label Title works hard to protect the security and confidentiality of your personal information. In accordance with the provisions of federal law, Green Label Title maintains policies and procedures regarding the collection and disclosure of information considered to be NPI.

This privacy statement applies to personal information we obtain anytime you interact with Green Label Title.

What Information We Collect, and Why. Green Label Title obtains nonpublic personal information about our consumers from information:

- we receive from you orally or in writing on transaction forms and applications
- we secure from our files or from our affiliates or others
- we receive from others involved in your transaction, such as the real estate agent or lender
- we may receive from a consumer reporting agency

We routinely ask for your name, address, telephone number, e-mail address, financial information (which may include mortgage payoff information and sometimes debit/credit card information), and any other identifying data (such as driver's license, state-issued ID, your social security number or date of birth) to facilitate the processing of our services and the management of our customers' transactions and business.

Green Label Title does not collect any NPI from our website. Please do not send personal information to Green Label Title via an unsecured email message. We recommend that you send personal information to Green Label Title via postal mail, courier, phone or fax.

Your provision of any NPI constitutes your agreement to this privacy policy, which may be amended from time to time. Do not provide any NPI (or allow others to do so on your behalf) if you (or your principal, if you are acting as an agent) do not agree with all of the terms including this privacy statement and any applicable supplemental privacy statement.

Disclosing Personal Information to Others. Green Label Title strictly limits disclosure of NPI; however, we may share the necessary personal or transaction details only to the extent necessary with

- (a) financial and non-financial entities (such as our agents, lenders, and underwriters) that perform a part of the transaction that you have requested,
- (b) our employees, agents, independent contractors, data processors, auditors, bankers, insurers, lawyers, consultants, and other service providers, and
- (c) government agencies in compliance with law or with a subpoena.

Green Label Title requires that employees having access to NPI take special precautions to protect the confidentiality of NPI. Access to NPI is limited to those who have a need for that information in order to perform their job responsibilities.

We shall not sell or rent the information we collect to third parties so that they can use it to directly contact you for their own promotional purposes. We will not provide your e-mail address, postal address, or telephone number to our business partners or other unaffiliated third parties for the purpose of allowing them to offer you products and services directly.

Security. Green Label Title employs technology, expert services, and operational procedures designed to protect the integrity and confidentiality of our communications and data processing and storage. These practices (including encryption, firewalls, physical access controls, and other appropriate techniques) meet or exceed the regulatory requirements and examination guidelines established by the relevant US federal, state financial services supervisory agencies and trade organizations.

Access to personal information is restricted to employees and service providers who need to have access to that information as described in this privacy statement. Our service providers are required to observe standards for the security, collection, use and sharing of personal information, and to comply with applicable law. Documents containing NPI are required to be stored in secured areas or in computer applications having password protections. Documents containing NPI must be destroyed by placing them in the secured shredding boxes provided by Green Label Title's shredding services vendor.

Preventing Identity Theft. Green Label Title recognizes the importance of protecting your personal information and is therefore committed to its protection. Please be advised that Green Label Title will never initiate requests for personal information or request such information from you by fax or email. Please do not send personal information to Green Label Title via unsecured email message. We recommend that you send personal information to Green Label Title via postal mail, courier, phone or fax.

Do not be misled by emails that appear to be from us and ask for personal information. If you receive a suspicious email requesting your personal information, please forward the email immediately to us.

Settlement is a private meeting. Settlement is not considered a public meeting. Audio and video recording is prohibited. Our compliance officer has responsibility for monitoring compliance with our Privacy Policy.

Green Label Title's Website Privacy Policy

Log Files. As true of most Websites, we gather certain information automatically and store it in log files. This information includes internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system and date/time stamp data.

We use this information, which does not identify individual users, to analyze trends, to administer the site, to track users' movements around the site and to gather demographic information about our user base as a whole.

Cookies. A cookie is a small text file that is stored on a user's computer for record-keeping purposes. We DO NOT use cookies on this site.

Links to Other Sites. This Website contains links to other sites that are not owned or controlled by us. Please be aware that we are not responsible for the privacy practices of such other sites.

We encourage you to be aware when you leave our site and to read the privacy policies of each and every Website that collects personal information.

This Website privacy policy applies only to information collected by this Website.

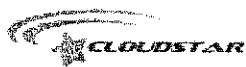
Will Green Label Title sell data gathered to anyone? No, Green Label Title does not and never will sell any data to anyone.

Who monitors our privacy policy? Green Label Title's policies are closely monitored by Green Label Title's management team. Green Label Title is committed to inform users directly if there is any change in Green Label Title's privacy policy.

Changes to our privacy policy. Green Label Title reserves the right to amend this policy at any time. Unless stated otherwise, any changes performed to this document will become effective as of the date a revised version is posted on our website.

If you have questions about information security, privacy, or usage of NPI at Green Label Title that were not answered here, please contact us at the following address:

Green Label Title
2517 Highway 35, Building B, Suite 103
Manaaquan, New Jersey 08736
732.722.7373
<http://www.greenlabeltitle.com>
Info@greenlabeltitle.com



Search

[Home](#) [Services](#) [Technology](#) [Resources](#) [Company](#) [News](#) [Contact](#)Cloudstar Relocates to Secure Banking-Grade Facility
1/5/15 Jacksonville, Florida

Privacy Policy

What information do we collect?

We collect information from you when you subscribe to our newsletter.

Any data we request that is not required will be specified as voluntary or optional.

When ordering or registering on our site, as appropriate, you may be asked to enter your: name, e-mail address, mailing address or phone number. You may, however, visit our site anonymously. Please see section entitled "Non-Public Personal Information" below if you are currently a client of Cloudstar.

Like most websites, we use cookies to enhance your experience, gather general visitor information, and track visits to our website. Please refer to the 'do we use cookies?' section below for information about cookies and how we use them.

What do we use your information for?

Any of the information we collect from you may be used in one of the following ways:

- To personalize your experience
(your information helps us to better respond to your individual needs)

How do we protect your information?

We implement a variety of security measures to maintain the safety of your personal information when you submit a request.

These security measures include: password protected directories and databases to safeguard your information, SSL (Secure Sockets Layered) technology to ensure that your information is fully encrypted and sent across the Internet securely or PCI Scanning to actively protect our servers from hackers and other vulnerabilities.

We offer the use of a secure server. All supplied sensitive/credit information is transmitted via Secure Socket Layer (SSL) technology and then encrypted into our Database to be only accessed by those authorized with special access rights to our systems, and are required to keep the information confidential.

After a transaction, your private information (credit cards, social security numbers, financials, etc.) will not be stored on our servers.

Do we use cookies?

Yes (Cookies are small files that a site or its service provider transfers to your computers hard drive through your Web browser (if you allow) that enables the sites or service providers systems to recognize your browser and capture and remember certain information.

Do we disclose any information to outside parties?

We do not sell, trade, or otherwise transfer to outside parties your personally identifiable information. This does not include trusted third parties who assist us in operating our website, conducting our business, or servicing you, so long as those parties agree to keep this information confidential. We may also release your information when we believe release is appropriate to comply with the law, enforce our site policies, or protect ours or others' rights, property, or safety. However, non-personally identifiable visitor information may be provided to other parties for marketing, advertising, or other uses.

Third party links

Occasionally, at our discretion, we may include or offer third party products or services on our website. These third party sites have separate and independent privacy policies. We therefore have no responsibility or liability for the content and activities of these linked sites. Nonetheless, we seek to protect the integrity of our site and welcome any feedback about these sites.

California Online Privacy Protection Act Compliance

Because we value your privacy we have taken the necessary precautions to be in compliance with the California Online Privacy Protection Act. We therefore will not distribute your personal information to outside parties without your consent.

Non-Public Personal Information

Cusomters of certain Cloudstar products and services may require the storage, trasmission, or backup of non-public personal information though servers, networks and systems hosted by Cloudsta either directory, or through our compliant vendor partners. Cloudstar agrees to never disclose, or cause to be disclosed, any non-public personal information. Non-public personal information is stored at various compliant data centers located throughout the country. All Cloudstar Datacenters have meet SSAE-16, SOC1, SOC2, and PCI-DSS compliance standards and employ the usage of various physical and logical security controls including by not limited to: data encryption, N+1 redundancy, fault tollerant storage solutions, redundant power, redundant cooling, redundant network systems, employee background checks, biometric access, security awareness training and other industry standard security controls.

Childrens Online Privacy Protection Act Compliance

We are in compliance with the requirements of COPPA (Childrens Online Privacy Protection Act), we do not collect any information from anyone under 13 years of age. Our website, products and services are all directed to people who are at least 13 years old or older.

CAN-SPAM Compliance

We have taken the necessary steps to ensure that we are compliant with the CAN-SPAM Act of 2003 by never sending out misleading information.

Online Privacy Policy Only

This online privacy policy applies only to information collected through our website and not to information collected offline.

Your Consent

By using our site, you consent to our privacy policy. By doing business with Cloudstar, you consent to our privacy policy.

Changes to our Privacy Policy

If we decide to change our privacy policy, we will post those changes on this page, send an email notifying you of any changes, and/or update the Privacy Policy modification date below. Policy changes will apply only to information collected after the date of the change.

This policy was last modified on 1/1/15

Contacting Us

If there are any questions regarding this privacy policy you may contact us using the information below.

Cloudstar is a DBA of the Keystone Management Group, LLC Family of Companies

www.mycloudstar.com

4800 Spring Park Road #16

Jacksonville, Florida 32207

support@mycloudstar.com

800-340-5780

Privacy Policy Customer Pledge

We pledge to you, our customer, that we have made a dedicated effort to bring our privacy policy in line with the following important privacy laws and initiatives:

Federal Trade Commission

California Online Privacy Protection Act

Childrens Online Privacy Protection Act

Privacy Alliance

Controlling the Assault of Non-Solicited Pornography and Marketing Act



About us

Business, compliance, and technology solutions for the Real Estate, Land Title,

Newsletter

Stay informed on our latest news!

E-mail *

Contact us

Cloudstar Headquarters

4800 Spring Park Road

Insurance & Financial Industries.

© 2015 Keystone Management Group, LLC
All rights reserved

Subscribe



Jacksonville, FL32207USA

800.340.5780
info@mycloudstar.com

Privacy Policy



Effective as of 07/23/2014

This Privacy Policy covers and describes how Segin Software, LLC ("Company", "We", "Us", or "Our") collects, uses and disclosure of information we collect through our website www.rynoh.com ("RynohLive" "we" or "our") and our service RynohLive. The use of information collected through our service shall be limited to the purpose of providing the service for which the Client has engaged Segin Software, LLC.

Segin Software, LLC has been awarded TRUSTe's Privacy Seal signifying that this privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's Program Requirements and the TRUSTed Cloud Program Requirements including transparency, accountability and choice regarding the collection and use of your personal information. TRUSTe's mission, as an independent third party, is to accelerate online trust among consumers and organizations globally through its leading privacy trustmark and innovative trust solutions. If you have questions or complaints regarding our privacy policy or practices, please contact us at support@rynoh.com. If you are not satisfied with our response you can [contact TRUSTe here](#).

The TRUSTe program covers our collection, use and disclosure of information we collect through our website, www.rynoh.com and our Platform. The use of information collected through our service shall be limited to the purpose of providing the service for which the Client has engaged Segin Software, LLC.

Use of and access to the RynohLive Sites is expressly conditioned on your acceptance of the following terms and conditions. If you do not agree with any part of the following terms and conditions, you may not use or access the RynohLive Site.

Company Policy

The privacy of your non-public personal information is important to us. We use safeguards to protect your privacy and confidentiality. We may update this privacy policy to reflect changes to our information practices. If we make any change in how we use your personal information we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on this Site prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

Security

We use good-faith efforts to maintain physical and electronic procedures to safeguard your non-public and personal information. However, while we strive to protect your personal information, we do not ensure or warrant the security of any information you transmit to us. This is done at your own risk. When you enter sensitive information on our site such as log-in information, credit card information and bank account information, we encrypt the transmission of that information using Secure Socket Layer (SSL) technology.

Information Collection

If you only browse through the RynohLive website and read the information contained on the web pages, we may automatically gather information about your visit. This information does not identify you personally. We may automatically gather the Internet domain or IP address from which you access the RynohLive site. We may also gather the date and time you access the site and the specific pages you visit.

We may collect non-public personal information from you such as names, street addresses, email addresses, credit card number, bank account information, and phone numbers when you voluntarily provide this identifiable information to us through the RynohLive site, such as when signing up as a user or accessing account-specific or other profile information. We may collect information about your transactions that we secure from our files and from our affiliates. We limit use of such information to the purposes for which the information was provided, except as described below. However, we reserve the right to use such information for marketing/product development research and other similar purposes and/or to contact you regarding additional services or products.

If you send an electronic mail (email) message that includes personally identifiable information, for example, in an email message containing an inquiry, we will use that information to respond to your inquiry. Remember that email is not necessarily secure against interception or other disclosure. If your communication is very sensitive or includes information such as your bank account charge card or social security number, you should not send it in an email.

You may choose to stop receiving our newsletter or marketing emails by following the unsubscribe instructions included in these emails or you can contact us at sales@rynoh.com.

We may use "cookies" to improve our service to you. Cookies may help us recall a previous visit. The cookies we use do not collect personally identifiable information and we do not use them to determine your identity. If you are not comfortable with this use, you may configure your browser to be notified when cookies are to be received and to provide you with the option of refusing cookies. However, refusing cookies may limit your ability to use of this site.

Our tracking utility company uses cookies to assist us with marketing data and site performance issues. The use of cookies by our tracking utility company is not covered by our privacy policy. We do not have access or control over these cookies.

Our third party advertising partner employs a software technology called clear GIFs (a.k.a. web beacons/web bugs), that help us better manage content on our site by informing us what content is effective. Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies, and are used to track the online movements of web users. In contrast to cookies, which are stored on a user's computer hard drive, clear GIFs are embedded invisibly on web pages and are about the size of the period at the end of this sentence. We do not tie the information gathered by clear GIFs to our clients' personally identifiable information.

We partner with a third party ad network to either display advertising on our website or to manage our advertising on other sites. Our ad network partner uses cookies and web beacons to collect non-personally identifiable information about your activities on this and other websites to provide you targeted advertising based upon your interests. If you wish to not have this information used for the purpose of serving you targeted ads, you may opt-out by clicking [here](#). Please note this does not opt you out of being served advertising. You will continue to receive generic ads.

Our website includes Social Media Features, such as the Facebook Like button and Widgets, such as the Share this button or interactive mini-programs that run on our site. These Features may collect your IP address, which page you are visiting on our site, and may set a cookie to enable the Feature to function properly. Social Media Features and Widgets are either hosted by a third party or hosted directly on our site. Your interactions with these Features are governed by the privacy policy of the company providing it.

Employees

Our employees and agents may view information that you provide us in order to perform their jobs and service your account. We do not authorize access to non-public personal information about you to those individuals who do not need to know that information in order to provide products or services to you or as otherwise provided herein.

Sharing

We may disclose any information that we collect about you to our affiliates or non-affiliated third parties as permitted by law. We also may disclose information about our clients or former clients and others to the following types of non-affiliated companies that perform marketing services on our behalf or with whom we have joint marketing agreements:

- Financial service providers such as companies engaged in banking, consumer finance, securities and insurance.
- Non-financial companies such as envelope stuffers and other fulfillment service providers. These companies are authorized to use your personal information only as necessary to provide these services to us.

- We may also release your information to others when we believe, in good faith, that such release is reasonably necessary to (i) comply with law, such as to comply with a subpoena (ii) enforce or apply the terms of any of our user agreements, or (iii) protect the rights, property or RynohLive users or others. We may also sell, transfer and disclose your information part of a business divestiture, sale, merger, or acquisition of all or a part of our business. You will be notified via email and/or a prominent notice on our website of any change in ownership or uses of your personal information, as well as any choices you may have regarding your personal information.
- If you do not want us to share your personal information with these companies, contact us at support@rynoh.com.

We will share your personal information with third parties only in the ways that are described in this privacy policy. We do not sell your personal information to third parties.

User Access and Choice

If your personally identifiable information changes, or if you no longer desire our service, you may correct, update, amend, delete/remove, by making the change on our member information page or by emailing support@rynoh.com or by contacting us by telephone or postal mail at the contact information listed below.

We will retain your information for as long as your account is active or as needed to provide you services. We will retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Links to Other Websites

The RynohLive site may contain links to websites that are provided and maintained exclusively by third parties. Websites provided and maintained by third parties are not subject to this privacy policy. Please review the privacy policies on those websites to understand their personal information handling practices. We make no representations concerning the privacy policies of these third-party websites.

Client Testimonials

We post client testimonials on our website which may contain personally identifiable information. We do obtain the client's consent via email prior to posting the testimonial to post their name along with their testimonial. To request removal of your personal information from Testimonials please contact us at sales@rynoh.com.

Contact Information

You can contact us by writing, calling, or emailing:

Segin Software, LLC
397 Little Neck Rd.
3300 South Building, #306
Virginia Beach, VA 23452

(877) 467-9664

support@rynoh.com

Information Related to Data Collected through RynohLive

Segin Software, LLC collects information under the direction of its Clients, and has no direct relationship with the individuals whose personal data it processes.

Choice

We collect information for our clients. If you are a customer of one of our Clients and would no longer like to be contacted by one of our Clients that use our service, please contact the client that you interact with directly.

Service Provider, Sub-Processors/Onward Transfer

Segin Software, LLC may transfer personal information to companies that help us provide our service. Transfers to subsequent third parties are covered by the provisions in this Policy regarding notice and choice and the service agreements with our Clients.

Access to Data Controlled by our Clients

Segin Software, LLC has no direct relationship with the individuals whose personal data it processes. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct his query to Segin Software, LLC's Client (the data controller). If the Client requests Segin Software, LLC to remove the data, we will respond to their request within 30 business days.

Data Retention

Segin Software, LLC will retain personal data we process on behalf of our Clients for as long as needed to provide services to our Client. Segin Software, LLC will retain and use this personal information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Steve Green

From: John W. Cody <johnw@planetshred.net>
Sent: Tuesday, February 03, 2015 12:13 PM
To: Steve Green
Cc: Kevin Judge
Subject: PLANET SHRED RECORDS MANAGEMENT/Privacy Policy

Follow Up Flag: Flag for follow up
Flag Status: Flagged

All Members & Employees of **Planet Shred Records Management LLC** ("Company") have signed Confidentiality Agreements stating, among other things, that they shall not disclose to any third-party the business names of any Client of the Company nor the name of any employee of such Client. At no time will any stored records of Client be shared with any person or entity other than the Client, unless ordered by subpoena of a lawful authority. The Company may comply with any such subpoena or similar order related to the stored records, provided that the Company notifies Client promptly upon receipt thereof, unless such notice is prohibited by law.

The Company shall exercise the same degree of care in safeguarding Stored Material entrusted to it by Client which a reasonable and careful company would exercise with respect to similar records of its own.

John Cody, Sr.
Sales Director
Planet Shred Records Management
Tel: 732.722.7777
johnw@planetshred.net
www.planetshred.net



Note: Records Storage Services provided by Planet Shred Records Management, LLC; Document Destruction Services provided by Planet Shred, LLC.

This email, including any attachments, is legally privileged and confidential under applicable law, and is intended only for the use of the individual or entity named above. If you are not the intended recipient of this message, you are hereby notified that any use, distribution, copying or disclosure of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by reply email or by phone (732) 722-7777 and then delete this email.

 **Please consider the environment before printing this email**




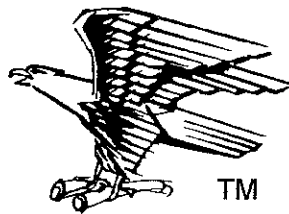
APPENDIX H

ALTA Self Certification

ALTA Best Practices Framework: Certification Package

Version 2.0
Published July 19, 2013


AMERICAN
LAND TITLE
ASSOCIATION





ALTA Best Practices Framework

The ALTA Best Practices Framework has been developed to assist lenders in satisfying their responsibility to manage third party vendors. The ALTA Best Practices Framework is comprised of the following documentation needed by a company electing to implement such a program.

- ALTA Best Practices Framework: Title Insurance and Settlement Company Best Practices
- ALTA Best Practices Framework: Assessment Procedures
- ALTA Best Practices Framework: Certification Package (Package includes 3 Parts)

Version History and Notes

Date	Version	Notes
7/19/2013	2.0	Publication of the ALTA Best Practices Framework: Certification Package, along with other documents in the ALTA Best Practices Framework, as approved by the ALTA Board on July 19, 2013. This is the first publication of the ALTA Best Practices Framework: Certification Package.

Certification Package Overview

The Certification Package is comprised of a Cover Page and 3 Parts. These documents should be prepared and either posted or delivered in the following order:

- Certification Package
 - Certification Package Cover Page
 - Agency Letter (Part 1)
 - Best Practices Certificate (Part 2)
 - Declarations Page (Part 3)

This certification package is issued in accordance with the ALTA Best Practices Framework, which includes the ALTA Title Insurance and Settlement Company Best Practices, Assessment Procedures, and Certification Package. The Framework is published and available at <http://www.ALTA.org/bestpractices>.



ALTA Best Practices Framework: Certification Package
Cover Page

American Land Title Association

Certification Package
ALTA Best Practices Framework

Agency: Green Label Title, LLC

This Certification Package contains this cover page and three parts, as follows:

- Part 1: Agency Letter
- Part 2: Best Practices Certificate
- Part 3: Declarations Page

ALTA Best Practices Framework: Certification Package
Agency Letter (Part 1)

**[Instructions: Print on Company letterhead and update references to "Company" to actual
Green Label Title, LLC**

Date: **[09/29/2015**

Subject: ALTA Best Practices Framework Dated July 19, 2013.


We are providing this letter in connection with the ALTA Best Practices Framework ("Framework") dated July 19, 2013. We intend that it be considered by any consumer, mortgage originator or mortgage servicer doing business with our company during the 24-month period following the date of this letter.

"Company" has implemented the ALTA Title Insurance and Settlement Company Best Practices ("Best Practices") dated July 19, 2013, listed in the attached ALTA Best Practices Certificate. As of the date of this letter, we comply with the Best Practices in all material respects.

We represent that, during the 24 month period commencing on the date of this letter, we will remain in material compliance with each of the Best Practices.

Attached to this letter, please find (i) an ALTA Best Practices Certificate issued to us pursuant to the Framework, and (ii) a copy of the current Declarations Page for our errors and omissions or professional liability insurance.

Sincerely,



"Company" **GREEN LABEL TITLE** President

ALTA Best Practices Framework: Certification Package
Certificate (Part 2)

Certificate

Issued to:

Green Label Title, LLC. "the Company"

Green Label Title performed the assessment procedures enumerated in the ALTA Best Practices Framework: Assessment Procedures dated July 19, 2013 ("Procedures"). These Procedures were agreed to by the Company to assist it in evaluating compliance with the ALTA Title Insurance and Settlement Company Best Practices, dated July 19, 2013 ("Best Practices"), as of 10/03/2015.

Procedures executed related to the following ALTA Best Practices:

- 1. Licensing
- 2. Escrow Accounting Procedures
- 4. Settlement Procedures
- 5. Title Policy Production & Delivery
- 6. Professional Liability Insurance Coverage
- 7. Consumer Complaints

- 3. Privacy and Information Security

Our performance of such Procedures rendered a resulting grade of:

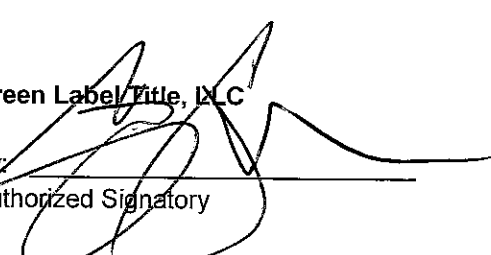
PASS

The scope of our engagement was limited to performance of the Procedures. We neither express an opinion regarding (i) the sufficiency of the Procedures for any particular purpose, nor (ii) compliance with the Best Practices.

This certificate is intended solely for the use of the Company. It is not intended to be relied upon by anyone other than the Company itself. Use of or reference to this certificate other than by the Company is at the user's sole responsibility and risk.

Green Label Title, LLC

By: _____
Authorized Signatory





ALTA Best Practices Framework: Certification Package
Declarations Page (Part 3)

**[Copy of Errors and Omissions or
Professional Liability Declaration Page attached]**



APPENDIX I

ALTA License/Membership Certification



APPENDIX I

ALTA License/Membership Certification

Certificate of License
2015

This certificate license grants authority to

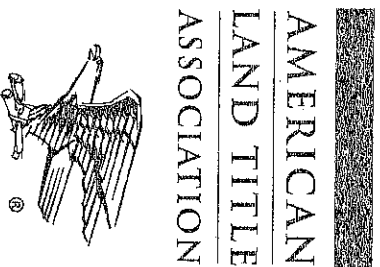
Green Label Title, LLC

To use ALTA's Policy Forms for the purpose of
writing title insurance policies during 2015.

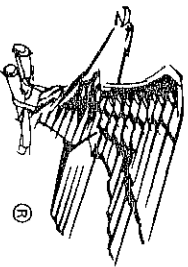


Michelle L. Korsmo, C.E.O.

ALTA ID# 1125812



AMERICAN
LAND TITLE
ASSOCIATION



CERTIFICATE
of
Membership

THIS CERTIFIES THAT

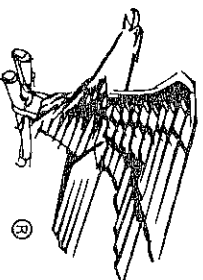
Green Label Title, LLC

ALTA ID: 1125812

Is a member in good standing of the
American Land Title Association for

2015

Diane Evans NTP, President



Michelle L. Korsmo, C.E.O.