CITIZENS, INC.

BANK SECRECY ACT/
ANTI-MONEY LAUNDERING POLICY AND PROGRAM

Updated: March 2, 2020

CITIZENS, INC. BANK SECRECY ACT/
ANTI-MONEY LAUNDERING POLICY AND PROGRAM

I. Introduction

The Bank Secrecy Act/Anti-Money Laundering Responsibilities of Insurance Companies

U.S. insurance companies have been designated as "financial institutions" subject to the Bank Secrecy Act and its implementing regulations (collectively, the "BSA") with respect to specific covered products, including life insurance and annuity products. The BSA requires financial institutions to maintain certain records and file reports to assist the U.S. government in criminal, regulatory and tax investigations and proceedings and in combating international terrorism. Insurance companies are required to develop and maintain written risk-based Anti-Money Laundering ("AML") programs ("BSA/AML programs") that are reasonably designed to ensure compliance with all applicable BSA requirements and to protect the company from being used to facilitate money laundering, drug trafficking, and the financing of terrorism.

The Crime of Money Laundering

In addition to the obligation to comply with regulatory requirements, insurance companies must be concerned with avoiding liability for the crime of money laundering. The money laundering criminal provisions reach activity broader than the process of "washing" criminal proceeds to conceal the source and ownership of the funds and cash transactions. Under the money laundering statutes, it can be a crime to engage in any transaction with knowledge that the funds involved in the transaction are the proceeds of criminal activity. Knowledge includes deliberately closing one's eyes to what would otherwise have been obvious to him or her and can include failing to inquire about or escalate situations where it is suspected that a person's funds may have an illegal source. While the government must establish that the proceeds actually were derived from one of a wide range of U.S. and foreign crimes, the government need not establish that a financial institution or its employees knew the particular type of illegal activity. Tax evasion and violations of foreign currency control requirements also can figure in money laundering schemes. In other words, an insurance company or its employee or independent agent could be considered to be engaged in money laundering if a customer were to make a payment with the proceeds of illegal activity, and the company, agent or employee were determined to have had knowledge of, deliberately ignored knowledge of, or to have failed to investigate suspicious activity or illegal source of funds.

Consequences of Non-Compliance

Violations of the money laundering criminal laws or the BSA can result in severe criminal or civil penalties for insurance companies and/or the employees involved. Violations also can result in regulatory enforcement actions against an insurance

company and/or its employees by the Department of the Treasury, Financial Crimes Enforcement Network ("FinCEN"), the Treasury Department bureau responsible for administering and enforcing the BSA. Involvement in money laundering, even unwittingly, could cause significant reputational harm to an insurance company. While not a defense to liability, an effective and fully implemented BSA/AML program may mitigate potential liability and is an insurance company's best protection against becoming involved in money laundering activity.

II. Citizens BSA/AML Policy and Program Commitment, Approval and Discipline

Compliance Commitment and Approval

It is the policy of Citizens, Inc. ("Citizens" or the "Company") to maintain a comprehensive risk-based BSA/AML program that includes strong governance and effective procedures and internal controls to comply fully with applicable BSA requirements and regulatory guidance, and to take measures reasonably designed to prevent and detect money laundering or other criminal activity. Under no circumstances will Citizens ever counsel a customer about avoiding BSA recordkeeping or reporting requirements or accommodate a client's request to circumvent them in any way. No business opportunity is worth the risk of engaging in money laundering.

To this end, Citizens' Board of Directors (the "Board") has approved this Bank Secrecy Act/Anti-Money Laundering Policy and Program ("AML Policy" or "Policy"), which outlines the Citizens, Inc. BSA/AML Program. The Board has appointed a BSA/AML Officer ("Citizens AML Officer" or "AML Officer") with responsibility for compliance with this Policy and coordination of the BSA/AML Program company-wide. The approval of the BSA/AML Policy and Program and appointment of Citizens' AML Officer is reflected in the minutes of the Board dated June 2, 2015. This Policy and Program replaces the previous Citizens, Inc., Anti-Money Laundering Policy adopted on June 6, 2006 and updated on January 4, 2010.

Any significant changes to this Policy must be approved by the Board. This document will be reviewed annually and updated as necessary if there are any significant changes in BSA/AML laws, regulations or regulatory guidance, in Citizens' related procedures and internal controls or in Citizens' AML risk profile.

Discipline

Compliance with the BSA/AML requirements and this Policy is a shared responsibility, and directors, officers, and employees will be held strictly accountable for non-compliance. In addition to criminal or civil sanctions or regulatory enforcement actions, engaging in money laundering, BSA violations or violations of this Policy or related procedures and internal controls will result in disciplinary action, up to and including termination. While independent consultants ("ICs") are not subject to the BSA, they are subject to BSA/AML-related responsibilities imposed by Citizens. If an IC does not

comply with Citizens BSA/AML Program responsibilities, the IC may be subject to contract termination.

III. Citizens BSA/AML Policy and Program Compliance Organization, Responsibilities, and Governance

The Board

The Board, acting through Senior Management, has oversight responsibility for guiding Senior Management in the compliance with BSA/AML requirements and the implementation of this Policy. To meet this responsibility, the Audit Committee of the Board will receive periodic reports on compliance initiatives and issues, including any deficiencies, from the AML Officer. These reports will include the results of regulatory examinations and independent testing and report progress in remediating any issues identified in regulatory examinations and independent testing. The Board also will ensure that the BSA/AML compliance function operates independently, has adequate authority, and is adequately supported with funding, qualified personnel, and technology. The Board will clearly communicate the priority of BSA/AML compliance to Senior Management and oversee Senior Management's role in fostering and maintaining a strong BSA/AML compliance culture.

Senior Management

The responsibility for compliance with and the successful execution of this Policy rests with Senior Management. Senior Management will set the tone from the top about the importance of BSA/AML compliance and direct strict compliance with this Policy and the company's related procedures and internal controls. Discipline for infractions of this Policy and the Company's related procedures and internal controls will be applied consistently.

Employees

It is the responsibility of every employee to comply with this Policy and to protect Citizens from being used to facilitate money laundering, drug trafficking, terrorist financing, and other crimes. Employees must be alert to, and refer internally, reports of unusual and suspicious activity and violations of this Policy and related procedures and internal controls.

All referrals will be treated as confidential to the extent possible. Citizens will not tolerate retaliation against an employee who reports a suspected violation in good faith. Any employee found to have engaged in such retaliation will be subject to discipline, up to and including termination. Anonymous referrals of potentially unusual or suspicious activity may be made to Citizens' General Counsel by fax, mail, email or by interoffice mail. Additionally, anonymous referrals may be made to Citizens' Audit Committee of the Board by sending a sealed envelope addressed to the Audit Committee Chair directly to Citizens' General Counsel.

The Citizens AML Officer

Citizens' AML Officer is responsible for coordinating the implementation of this BSA/AML Policy and Program company-wide.

Citizens' AML Officer's duties include, but are not limited to, the following:

- Developing BSA/AML initiatives, with the guidance of the Legal Department, revising the BSA/AML Policy and Program as needed, and presenting the Policy and Program to the Board annually or as needed for approval.

- Assessing new BSA regulatory requirements and guidance and recommending how to implement necessary changes to the BSA/AML Policy and Program and related internal controls.

- Reviewing and approving the BSA/AML risk assessment, including the methodology and the risk assessment results.

- Reviewing and approving procedures and internal controls to implement this Policy and the BSA/AML Program.

- Ensuring compliance with BSA reporting requirements for cash transactions and cross-border mailing, shipment, and transportation of currency or other monetary instruments.

- Investigating potentially suspicious activity and filing Suspicious Activity Reports ("SARs") where required, and reviewing and approving back-end processes for identifying potential suspicious activity.

- Confirming that BSA quality assurance or compliance testing is conducted and that the frequency and scope of the testing are appropriate.

- Ensuring that the Customer Due Diligence processes include obtaining all relevant customer information and documentation for BSA/AML purposes.

- Ensuring that adequate training is developed and delivered to appropriate employees and ICs and facilitating communication with the Board, Senior Management, employees, and IC's about BSA/AML issues.

- Taking measures to integrate ICs in the Program, and providing communications to the ICs on their BSA/AML responsibilities.

- Ensuring that BSA/AML training is provided periodically to the Board and Senior Management.

- Consulting with the Internal Audit Department to review the proposed scope, method, and frequency for independent testing for consistency with regulatory expectations.

- In conjunction with Citizens' General Counsel, acting as the communication point for regulatory and law enforcement authorities on BSA/AML compliance issues.

- Monitoring and coordinating remedial actions in response to regulatory examinations and independent testing of the BSA/AML Program.

- Identifying and recommending appropriate technology to support BSA/AML compliance.

- Coordinating with the Human Resources Department on appropriate standards for BSA/AML-related discipline.

Citizens' AML Officer may delegate these responsibilities, as appropriate, and will be assisted in the execution of these responsibilities by the Legal Department. All references below to the AML Officer should be read to include any designees of the AML Officer.

Legal

The Legal Department will assist the AML Officer and provide support with implementation and ongoing compliance with this Policy. In addition, the Legal Department will be responsible for assisting with updating the AML Policy in accordance with any new regulations or regulatory guidance as well as providing advice in enhancing procedures and internal controls to comply with the new measures.

Citizens Internal Audit

Citizens' Internal Audit ("Internal Audit') is responsible for conducting periodic risk-based independent testing of the BSA/AML Program and related procedures and internal controls. Independent testing is a BSA requirement and ensures compliance with applicable BSA/AML laws, regulations, and regulatory guidance and the continued effectiveness of the Program. The AML Officer will review the proposed scope and methodology for independent testing for consistency with regulatory requirements. Internal Audit will report the results of its testing to the Audit Committee, the Board, the AML Officer, and Senior Management. In consultation with Citizens' AML Officer, Internal Audit also may engage qualified third party firms to conduct BSA/AML independent testing.

New Business

New Business personnel will implement reasonable risk-based procedures to identify and report internally potentially suspicious activity. These procedures will include, but

not be limited to, risk-based methods to verify the identity of any applicants and owners, maintain records of information used to verify identity, and check that the applicant and owner do not appear on the lists of designated persons and entities maintained by the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC") ("OFAC Lists"), and to detect and report potentially suspicious activity to the AML Officer.

Customer Solutions

Customer Solutions personnel will implement reasonable risk-based procedures to identify and report internally potentially suspicious activity and to obtain relevant customer information and conduct reasonable risk-based customer due diligence. The procedures will include, but not be limited to, identifying sources of funds; monitoring changes made to the owner, beneficiary and/or address of a policy; and monitoring loan, surrender, cancellation, non-forfeiture option, withdrawal request activity, changes made to methods of payment, unusual/suspicious payment activity, and loan repayment activity. Customer Solutions also will monitor policy changes and reinstatement requests and premium payments in association with change and reinstatement requests.

Claims

Claims personnel will implement reasonable risk-based procedures to identify potentially suspicious activity in the claims process. Claims procedures will include, but not be limited to, verifying identification of the beneficiary or beneficiaries or other payee(s), and checking that the beneficiar(ies) or other payee(s) do not appear on the OFAC Lists.

Accounting

Accounting personnel will implement reasonable risk-based procedures to identify potentially suspicious activity in the payment process and to ensure compliance with BSA reporting requirements for cash and monetary instruments, discussed below, and the Citizens payment policy. The procedures will include, but not be limited to, identifying sources of funds, and monitoring loan, surrender, cancellation, non-forfeiture option, withdrawal request activity, changes made to methods of payment, unusual/suspicious payment activity, and loan repayment activity.

Marketing

Marketing personnel will implement reasonable risk-based procedures to identify and report internally potentially suspicious activity identified in the course of executing their responsibilities for IC relationships. Marketing is responsible for conducting reasonable due diligence and OFAC screening on new ICs and periodic due diligence updates on existing ICs. Marketing also will advise the AML Officer if an IC is not executing his/her responsibilities under the BSA/AML Program.

Information Technology Department ("IT")

IT personnel will assist with the system support necessary for BSA and OFAC compliance, including programs to identify potentially suspicious activity, maintenance of customer due diligence information, and maintenance of OFAC software, for all locations, to be utilized to support the procedures of various departments within the Company to ensure accurate checking of names against the OFAC Lists.

Independent Consultants

Key to the success of Citizens outside the United States is its network of ICs. Citizens conducts risk-based due diligence on all ICs at the beginning of the relationship and periodically on a risk-based basis over the course of the relationship to ensure that they share Citizens business ethics and commitment to legal compliance. ICs are required by contract to comply with this Policy, and with all applicable laws, in their work for Citizens.

Citizens will communicate periodically with the ICs in writing about their BSA/AML responsibilities and require the ICs to attest to their commitment to fulfill their responsibilities. Citizens will convey that Citizens expects the ICs to exercise proper care and diligence in referring only customers who are engaged in legitimate business activities and who have legal sources of funds and to report potentially suspicious activity. If an IC knowingly refers customers whose sources of funds are found to have come from illegal activities or whose funds the IC deliberately ignores knowing the sources of or who the IC should have investigated further but did not, the IC's relationship will be terminated and commissions withheld.

IV. Citizens BSA/AML Policy and Program

Required Elements

Citizens BSA/AML Program contains all the required elements of a BSA/AML program for insurance companies under the BSA regulations.

- Development of risk-based policies, procedures, and internal controls to ensure compliance with BSA reporting and recordkeeping requirements, and integration of agents, associates and ICs into the BSA/AML program.

- Designation of a compliance officer to ensure effective implementation of the BSA/AML program, including ensuring ongoing training of appropriate persons, the integration of agents, associates and ICs into the program, and updating of the program as necessary.

- Ongoing education and training of appropriate company personnel, agents, associates and ICs on their program responsibilities.

- Periodic independent testing of the program.

- Obtaining all relevant customer information necessary for an effective program.

- Conducting risk assessments of covered products.

Compliance with Specific BSA Requirements

- *Compliance Organization and Governance* - As discussed above, Citizens has designated an AML Officer to ensure day-to-day compliance with the BSA, this Policy, and Citizens' related procedures and internal controls. Citizens has built a governance structure that ensures compliance will be sustained, compliance issues will be addressed promptly, and the BSA/AML Policy and Program will be adjusted, as needed, to address evolving risk.

- *Risk Assessment* - Citizens has developed and will maintain a risk assessment that is consistent with regulatory guidance. The risk assessment will consider Citizens' sales model, geographic markets, size, products, services, customers, ICs and day-to-day transactions. The fact that sales are made by ICs in many countries considered to pose high risks for money laundering and the need to have proper controls to address money laundering methods in those countries will be considered. The risk assessment will measure inherent risk, assess mitigating controls, and determine the residual risk. The risk assessment will be incorporated in the execution of the BSA/AML Program. Risk assessments must be updated annually and presented by the AML Officer to the Board**.**

- *Written Procedures and Internal Controls* – Citizens has implemented procedures and internal controls for compliance with each BSA requirement and the requirements of this Policy, which have been approved or developed by the AML Officer.

    - *Customer Due Diligence* - A key aspect of Citizens' business practices which protect it from becoming involved in money laundering or other criminal activity is our Customer Due Diligence ("CDD") process and procedures. In applying CDD practices to all customer relationships, Citizens complies with the BSA requirement that an insurance company must obtain all relevant customer information necessary for an effective BSA/AML program. In the insurance industry, CDD builds upon the underwriting process and covers both the owners of the policy and the insured, if different, and includes risk-based measures when beneficiaries are paid. While not explicitly required under the BSA, Citizens verifies the identity of the owners of all policies by viewing copies of a reliable identification document(s) or requiring the ICs to view the identification document(s) and requiring photocopies to be provided to Citizens with the application. If a new customer refuses or is unable to provide the required identification document(s), the policy will be denied. Citizens also conducts reasonable risk-based due diligence, including to ensure that payment will be made from a legitimate source of funds. Citizens also

confirms that there is a logical relationship or "insurable interest" between the owner of a policy and the insured, if different. Citizens also screens all owners, insureds, and beneficiaries through commercial services to identify material negative news and conducts OFAC screening of owners and insured parties, if different, and on beneficiaries prior to establishing a customer relationship or paying a claim.

- *Payment Policy* - Another important protection against money laundering is Citizens payment policy. Citizens only accepts premium payments in U.S. dollars, and will not accept cash, travelers checks or money orders (for international business) for premium payments. Citizens also has tightened its payment policy to require payment by check, credit card, wire transfer, or a foreign bank draft (much like a cashiers check) from an account in the name of the owner or another approved payee or payor, if such payment is made through an IC certified by Citizens and trained to engage in payment remitter services as set forth in a Consultant Payment Remitter Agreement executed by and between Citizens and the IC. Other checks must be made payable to the appropriate Citizens subsidiary insurance company and may not be drawn on non-bank financial institutions, such as unregistered or black market exchange houses. Citizens shall communicate this payment policy to its customers and ICs and will return payments inconsistent with this payment policy and, in appropriate cases, file SARs on suspicious payments.

- *Cash Transaction Reporting (Form 8300 Reporting)* - Under a BSA requirement and parallel requirement of the Internal Revenue Service ("IRS"), insurance companies must report receipts of cash in excess of $10,000 received on one business day (or in a series of related transactions received in the aggregate in an effort to evade the $10,000 threshold). Under some circumstances, cash can include not just currency, but certain monetary instruments, *e.g.,* money orders, travelers checks, cashier's checks, and bank drafts. This requirement is sometimes referred to as "Form 8300" reporting based on the number of the IRS form previously used for reporting. Structuring payments to avoid the filing of a Form 8300 is a crime. Under no circumstance may a Citizens' employee or an IC advise a payor on how to structure transactions to avoid the Form 8300 filing requirement. As it is Citizens policy generally not to accept payments with cash, travelers checks or money orders (for international business), the need to file Form 8300s will be minimized or eliminated. Nevertheless, to ensure compliance with this Policy, Citizens has established procedures and internal controls approved by the AML Officer for Marketing Services and the Accounting Department to review premium payments received to identify any instances of payments with reportable cash equivalent monetary instruments which may require the filing of a Form 8300. The AML Officer will also periodically review the IRS.gov web site and refer to the page: Guidance for the Insurance Industry on Filing

Form 8300, where the IRS originally updated the guidance on October 28, 2014 and indicated: "In summary, if an insurance company does not accept cash, but accepts cash equivalents; generally it is not necessary to file Form 8300 on payments for insurance policies and annuity contracts. An exception would be if the insurance company knew (not just suspected) that the monetary instrument(s) was used in an attempt to avoid the filing of Form 8300 by the insurance company." If reportable transactions are identified, the AML Officer will be responsible for timely filings in accordance with regulatory requirements and instructions.
Source: http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Guidance-for-the-Insurance-Industry-on-Filing-Form-8300

- *Reports of International Transportations of Currency or Monetary Instruments ("CMIRs")* - All U.S. persons (individuals or businesses), not just financial institutions under the BSA, must file CMIRs when currency (U.S. or the foreign equivalent) and certain money instruments (*e.g.*, travelers checks in any form and bearer negotiable instruments) in excess of $10,000 are physically transported into or out of the United States or sent out of or received in the United States. Citizens will monitor payments in any form received from ICs from outside the United States to identify any instances where travelers checks in any form and other checks in bearer form (endorsed to bearer or without restriction) with a face value in excess of $10,000 in the aggregate are received from the ICs in one or more mailings or shipments on the same day, and will file CMIRs (FinCEN Form 105) where required. Any required CMIRs will be filed by the AML Officer on a timely basis in accordance with regulatory instructions.

- *Suspicious Activity Reports* - A key element of this Policy and the BSA/AML Program is the timely identification of unusual and suspicious activity and the reporting of suspicious activity in accordance with the SAR requirements for insurance companies and FinCEN guidance.

  (a) The SAR Requirement - The BSA requires insurance companies to file SARs with FinCEN electronically to report attempted or completed transactions by, at or through the company, involving at least $5,000 in the aggregate (or in smaller amounts when deemed appropriate), if the company knows, suspects or has reason to suspect that the transaction:

    - Involves money laundering;

    - Is designed to evade any BSA requirements, including by structuring transactions to evade BSA reporting or recordkeeping requirements;

- Is unusual, *i.e.*, has no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to engage, and the company knows of no reasonable explanation for the transaction after examining the available facts; or

- Involves the use of the insurance company to facilitate criminal activity.

An insurance company is responsible for reporting suspicious transactions conducted through its ICs and brokers. SARs generally must be filed within 30 calendar days after detection of the facts that constitute the basis for filing. In addition to filing a SAR, if a matter requires immediate attention, a company must contact an appropriate law enforcement agency.

(b) Citizens' SAR Procedures and Internal Controls - Citizens has implemented procedures and internal controls for identifying, investigating and tracking potentially suspicious activity and filing SARs to ensure that SARs are timely filed and accurate, and that they provide required information to law enforcement.

Employees are trained to refer internally attempted or completed transactions that may require the filing of a SAR. ICs also are trained to report potentially suspicious activity to the AML Officer. In addition, the AML Officer has approved procedures to identify suspicious activity by periodic (at established intervals) back-end monitoring and reviews of certain reports and records to identify suspicious activity on a regular basis that meet certain criteria at established thresholds.

The criteria and scope for back-end monitoring will be assessed for effectiveness and adjusted, if necessary, at least annually. Any adjustments to the criteria must be approved by the Citizens AML Officer.

In appropriate cases, *e.g.*, in the case of ongoing illegal activity, in addition to filing SARs, the AML Officer in coordination with the Legal Department will reach out to appropriate law enforcement authorities.

(c) The SAR Decision - The decision to file or not to file a SAR will be discussed by the AML Officer, as appropriate, with the Legal Department and other appropriate officers. The decision to file or not to file a SAR, however, ultimately rests with the AML Officer. The reasons for filing (or not filing) will be recorded.

(d) SAR Recordkeeping, Confidentiality and Disclosure - Records of SARs and the supporting documentation for SARs will be maintained by the AML Officer. The supporting documentation will be identified as such at the time of the filing of the SAR.

FinCEN's regulations require that SARs, and any information that would reveal that a SAR has been filed or that a SAR exists, must be kept strictly confidential, subject to a few limited exceptions. Therefore, Citizens has established safeguards to ensure the confidentiality of SARs and SAR information, including decisions not to file SARs. The underlying facts, transactions, and records upon which a SAR is based, however, may be shared, so long as the information or documents do not disclose the existence (or nonexistence) of a SAR. The Legal Department will ensure that no SAR or SAR information that could reveal the existence of a SAR is provided to third parties in litigation consistent with BSA regulations and FinCEN guidance.

SAR and SAR information may be shared with appropriate law enforcement and state regulators in accordance with the regulations and FinCEN guidance.

In coordination with the Legal Department, the AML Officer will handle all requests for SARs and supporting documentation from law enforcement authorities and will require that such requests be in writing. Only a copy of the SAR and information identified as supporting documentation will be provided. Any additional information or documentation about the subject or the subject's transaction will be provided only if pursuant to legal process.

Employees and ICs are trained that it is prohibited to advise or "tip off" any person that a transaction is being referred internally or is being reported or may be reported to the government as suspicious. Any such "tipping off" will constitute a serious violation of this Policy and will subject to discipline, up to and including termination. It may also be referred to government authorities for investigation as a possible criminal offense.

(e) Escalation Procedures - If suspicious activity is identified, the AML Officer will recommend that the insurance policy not be approved, or the proposed transaction not be allowed. If the company officer disagrees with the AML Officer's recommendation, the matter will be referred to the Audit Committee of the Board for review and determination. Records will be made of each step in the decision-making process.

Legal and regulatory requirements and insurance contracts may impact the ability to terminate a policy after a certain period of time even if a SAR is required to be filed or it is suspected that payment is from an illegal source. In such cases, the SAR will be filed with an explanation why the relationship cannot be terminated.

The AML Officer may recommend an IC be terminated, suspended or otherwise disciplined because of failure to execute his or her BSA/AML responsibilities. If the company officer disagrees with the AML Officer's recommendation, the matter will be referred to the Audit Committee of the Board for review and determination. Records will be made of each step in the decision-making process.

(f) Recordkeeping - Citizens will maintain records required by the BSA for financial institutions generally and records of customer information (customer identification, due diligence, underwriting, and payments) and IC due diligence for at least five years after the termination of a customer or IC relationship. Citizens also will retain all records relating to the BSA/AML Program for at least five years, including: risk assessments and risk assessment methodologies; records of compliance with BSA requirements (Form 8300, CMIR, and SAR requirements); records of quality assurance and independent testing and remedial measures; training and communications; BSA/AML-related disciplinary actions involving employees or ICs; BSA/AML law enforcement and regulatory requests, including requests for SAR supporting information and responses; and regulatory examinations and responses to examinations or government criticism.

- *Training* - All employees, including employees who deal with customers or process customer payments, *e.g.,* new business, customer service, policy owner service, claims processing, and accounting, or those who support the BSA/AML function, *e.g.,* legal, compliance, internal audit, management, and ICs, will receive BSA/AML training upon being hired and at least annually thereafter. New employees must be trained before assuming any BSA/AML responsibilities.

  All training will emphasize the priority of BSA compliance for Citizens and include red flags for suspicious activity. A list of some of these red flags is attached as Exhibit A. Training also will emphasize the Board and Senior Management's expectations for BSA/AML compliance and the consequences of non-compliance with BSA/AML requirements and Citizens related procedures and internal controls.

  Training will be developed or approved by the Citizens AML Officer, and annual training will contain a testing component. Records of who was trained, the dates

of training, the contents of training, and the delivery method will be maintained. The Citizens AML Officer is responsible for ensuring that the Citizens Board and Senior Management receive periodic updates and training.

- *Information Sharing 314(b)*

The Company, under the protection of the safe harbor from liability, may voluntarily receive, or otherwise share information with any other financial institution or association of financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that the financial institution or association suspects may involve possible terrorist activity or money laundering. The following rules apply:

- Notice Requirement. The financial institution that intends to share information is to submit to FinCEN a "Notice for Purposes of Subsection 314(b) of the USA Patriot Act Each notice provided is effective for the one-year period beginning on the date of the notice. In order to continue to engage in the sharing of information after the end of the one-year period, the financial institution must submit a new notice. The AML Officer is responsible for completing and submitting the notice to FinCEN for the Company on an annual basis.

- Verification Requirement. Prior to sharing information, it is the responsibility of the AML Officer to take reasonable steps to verify that the financial institution with which the Company intends to share information has submitted to FinCEN their notice. Verification may be obtained by confirming that the other financial institution appears on a list that FinCEN will periodically make available to the Company that have filed a notice with it, or by contacting FinCEN directly to ensure the notice has been filed.

- Use of Information. It is against Company procedures for information received from another financial institution be used for any purpose other than:

    - Identifying and, where appropriate, reporting on money laundering or terrorist activities

    - Determining whether to establish or maintain an account, or to engage in a transaction; or

    - Assisting a financial institution in complying with the regulation.

- Safe Harbor Liability. If the Company shares information with another financial institution it is protected from liability for such sharing, or for any failure to provide notice of such sharing, to an individual, entity, or organization that is identified in such sharing.

- Information Sharing Between Financial Institution and the Federal Government. If, as a result of information shared by the Company, and the Company knows, suspects, or has reason to suspect that an individual, entity, or organization is involved in, or may be involved in terrorist activity or money laundering, and the Company is subject to a suspicious activity reporting, the AML Officer is to file a Suspicious Activity Report. In situations involving violations requiring immediate attention, such as when a reportable violation involves terrorist activity or is ongoing, the AML Officer is to immediately notify, by telephone, an appropriate law enforcement authority and Senior Management in addition to filing a Suspicious Activity Report.

- Confidentiality - 314(b) requests are subject to the same confidentiality requirements as SARs. The Company shall not share 314(b) sharing information with affiliates or holding company (unless the request specifically states otherwise).

➢ *Testing of the Program*

- *Independent Testing* - Citizens Internal Audit will maintain a risk-based BSA/AML audit program and annually test compliance with, and the effectiveness of, the BSA/AML Policy and Program and Citizens' related procedures and internal controls to comply with BSA requirements and prevent and detect money laundering.

- *Compliance Testing* **-** The AML Officer will develop risk-based compliance audits or quality assurance testing to ensure compliance with the recordkeeping and reporting requirements of the BSA and related procedures and internal controls.

V. Cooperation with Law Enforcement and Regulatory Authorities

The AML Policy and BSA/AML Program require law enforcement and regulatory cooperation. It is Citizens' policy to cooperate fully with federal, state, and local law enforcement authorities in investigations, prosecutions, and forfeiture actions involving money laundering, terrorist financing or other illegal activity. Citizens will respond timely and fully to lawful requests for information about its officers, employees, ICs, or customers.

Citizens also will cooperate with FinCEN and the IRS, to which FinCEN has delegated the authority to examine insurance companies for BSA compliance, and with state regulatory authorities. Citizens will respond promptly to any issues raised in examinations and will make records and appropriate employees readily available to facilitate the examination process. Citizens will take appropriate remedial actions in response to any regulatory issues identified.

VI. Questions and Guidance

If there are any questions regarding this document or compliance with BSA/AML requirements or Citizens related procedures and internal controls, the questions should be addressed to the AML Officer at Compliance@citizensinc.com or (512) 837-7100.

Exhibit A

Suspicious Activity – "Red Flags"

- Policy owner or customer exhibits unusual concern about the insurance company's compliance with Government reporting requirements or its AML policies, particularly with respect to his or her identity, type of business and assets.
- Policy owner or customer is reluctant or refuses to reveal information concerning business activities, or furnishes unusual or suspect identification or business documents.
- Policy owner or customer wishes to engage in transactions that lack a business or apparent investment purpose, or are inconsistent with stated business or investment objectives.
- Policy owner or customer provides false, misleading or substantially incorrect information concerning the source of funds.
- Policy owner or customer refuses to identify or fails to indicate a legitimate source of funds.
- Policy owner or customer exhibits a lack of concern regarding, commissions, surrender charges, withdrawal charges, or other transaction costs.
- Policy owner or customer appears to be acting as an agent for an undisclosed principal, but is evasive about providing, or declines or is reluctant, without legitimate commercial reasons, to provide information regarding the undisclosed principal.
- Policy owner or customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- New business in any way involves individual, entities, or countries on the Office of Foreign Assets Control (OFAC) list.
- Policy owner's or customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- Policy owner's or customer's account shows numerous currency or cashier's check transactions aggregating to significant sums.
- Policy owner or customer requests wire transfers to unrelated third parties.
- Policy owner's or customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- Policy owner or customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- Policy owner or customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.
- Policy owner or customer attempts to borrow the maximum cash value of a single premium policy soon after purchase.
- Policy owner or customer requests an early cancellation of the policy and refund of the premium soon after the purchase.

- Policy owner or customer refuses to provide information required to underwrite the application and it appears the customer applied for the purpose of obtaining a refund.
- Policy owner or customer applied for insurance coverage and it appears the customer or sales consultant likely knew the insurance would be declined for the purpose of obtaining a refund.
- Policy owner or customer requests a withdrawal of advance premiums.
- Policy owner or customer requests an early withdrawal of annuity funds.
- An application for insurance is received from a politically exposed person (PEP), or an existing policy owner becomes classified as a PEP. A PEP is a senior foreign government or foreign political figure, immediate family member or close associate.
- Policy owner or customer attempts to pay premiums with cash or cash equivalents like Traveler's Checks or Money Orders even though these payment types are prohibited for international clients.
- An unrelated third party payment (TPP) is utilized to pay premiums without the proper TPP documentation and oversight by a consultant certified as a Payment Remitter.
- Policy owner or customer arranges excessive numbers or excessively high values of reimbursements due to over payments of premium and requests a refund for the excess payment(s).
- Policy owner, customer or an unrelated third party submits payment(s) without a clear explanation of how the payment(s) should be applied, especially when no premiums are due, and requests a refund of the payment(s).