Office of the Internal Auditor

Confidentiality
Integrity
Ethics
Objectivity
Competency

CITIZENS
PROPERTY INSURANCE CORPORATION

AUDIT REPORT

Privacy

March 20, 2017

Report Number: 2017-AUD-01 Privacy

Table of Contents: **Page**

Executive Summary

Background

Privacy refers to the laws that deal with the regulation of personal information about individuals (including customers, vendors, employees and other parties), which can be collected, stored, used, shared and disposed of as part of a company's business processes. Data privacy protection requirements are mandated by various federal laws (GLBA, HIPPA, FCRA, Electronic Communications Privacy Act, etc.) and Florida Statutes and Administrative Rules.

Privacy is a high profile topic because of the potential impact on the company and the public. Ineffective processes and procedures related to the control of private information could result in greater reputational risk with the possibility of increased negative publicity, additional regulatory scrutiny and other legislative sanctions due to compromises of personal data. In addition, there is financial risk because of potential imposition of monetary sanctions by regulatory bodies and other costs such as compensation to the directly affected parties, litigation costs, and increased operating costs for notification and remediation. Citizens recognizes the importance of its privacy obligations and has the longstanding strategic objective to "Protect private information in Citizens' custody, as well as its access and use by internal and external parties."

To achieve this objective, Citizens has developed a privacy program that includes:

- Privacy Framework – In 2013, Citizens established a privacy framework to act as the foundation for the development of the company's privacy practices and policies. The framework incorporates the principles outlined the AICPA's Generally Accepted Privacy Principles (GAPP) in order to provide Citizens' management with guidance on privacy governance, risk and compliance.
- Privacy Policy – Based on the Privacy Framework, Citizens developed a Privacy Policy which establishes standards to ensure private information is collected, used retained, disclosed and disposed of in conformity with the principles set forth in Privacy Framework and with applicable laws and regulations. This policy, along with other corporate policies such as "Information Classification and Handling", "Information Security", "Vendor Management" and "Records Management and Records Request" policies, establish the requirements for identifying and controlling customer, employee and third-party private data.
- Privacy Officer – Citizens Privacy Officer reports to the Ethics and Compliance Officer and is the designated point of contact for all privacy matters. The Privacy Officer's duties include: overseeing privacy-related risks within the organization; developing, implementing, enforcing and monitoring Citizens' privacy policies; identifying which privacy laws, regulations and standards apply to Citizens; providing guidance to the business units on privacy matters.

Audit Objectives and Scope

The objective of this audit was to evaluate the design of the policies, practices and processes that Citizens has implemented to provide the appropriate level of control over customers', employees' and third-parties' private information. Through review of policies, interviews with management

and staff and examination of documentation we determined how Citizens manages the use of private information.

Audit Opinion

Our fact find work confirmed that the overall design of controls over private information of customers, employees and third parties is **Satisfactory**. We noted that processes are appropriately designed to support Citizens strategic privacy objective. These include: appropriate privacy related policies which are available to all employees on the internal portal; data classification criteria and standards; both new hire and annual mandatory refresher training covering privacy and data security; customer privacy notices available on the external website and provided to customers at policy inception and upon renewal; contracts with third parties that adequately outline their responsibilities prior to sharing private information; and physical and logical security practices over private data.

Our work, however, revealed a need to further develop regular monitoring and reporting on the continued strength of applied privacy compliance practices. Through implementing regular limited privacy assessments, the Privacy Officer could effectively opine and report on the condition of Citizens privacy compliance program on an enterprise level. This was discussed with management and a review/reporting program is being developed.

Several process improvement opportunities were identified during the review which were discussed with the management of the appropriate business units. Management will evaluate these process improvement suggestions and will take appropriate action as necessary.

We would like to thank management and staff for their cooperation and professional courtesy throughout the course of this audit.

Appendix 1

Definitions

Audit Ratings

Satisfactory:

The control environment is considered appropriate and maintaining risks within acceptable parameters. There may be no or very few minor issues, but their number and severity relative to the size and scope of the operation, entity, or process audited indicate minimal concern.

Needs Minor Improvement:

The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some minor areas of weakness in the control environment that need to be addressed. Once the identified weaknesses are addressed, the control environment will be considered satisfactory.

Needs Improvement:

The audit raises questions regarding the appropriateness of the control environment and its ability to maintain risks within acceptable parameters. The control environment will require meaningful enhancement before it can be considered as fully satisfactory. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some noteworthy areas of weakness.

Unsatisfactory:

The control environment is not considered appropriate, or the management of risks reviewed falls outside acceptable parameters, or both. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate pervasive, systemic, or individually serious weaknesses.

Appendix 2

Observation Classifications

Control Category	High	Medium	Low
Financial Controls (Reliability of financial reporting)	• Actual or potential financial statement misstatements > $10 million • Control issue that could have a pervasive impact on control effectiveness in business or financial processes at the business unit level • A control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in the financial reporting process	• Actual or potential financial statement misstatements > $5 million • Control issue that could have an important impact on control effectiveness in business or financial processes at the business unit level	• Actual or potential financial statement misstatements < $5 million • Control issue that does not impact on control effectiveness in business or financial processes at the business unit level
Operational Controls (Effectiveness and efficiency of operations)	• Actual or potential losses > $5 million • Achievement of principal business objectives in jeopardy • Customer service failure (e.g., excessive processing backlogs, unit pricing errors, call center non responsiveness for more than a day) impacting 10,000 policyholders or more or negatively impacting a number of key corporate accounts • Actual or potential prolonged IT service failure impacts one or more applications and/or one or more business units • Actual or potential negative publicity related to an operational control issue • An operational control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in operations • Any operational issue leading to death of an employee or customer	• Actual or potential losses > $2.5 million • Achievement of principal business objectives may be affected • Customer service failure (e.g., processing backlogs, unit pricing errors, call center non responsiveness) impacting 1,000 policyholders to 10,000 or negatively impacting a key corporate account • Actual or potential IT service failure impacts more than one application for a short period of time • Any operational issue leading to injury of an employee or customer	• Actual or potential losses < $2.5 million • Achievement of principal business objectives not in doubt • Customer service failure (e.g., processing backlogs, unit pricing errors, call center non responsiveness) impacting less than 1,000 policyholders • Actual or potential IT service failure impacts one application for a short period of time

Appendix 2

Control Category	High	Medium	Low
Compliance Controls (Compliance with applicable laws and regulations)	• Actual or potential for public censure, fines or enforcement action (including requirement to take corrective actions) by any regulatory body which could have a significant financial and/or reputational impact on the Group • Any risk of loss of license or regulatory approval to do business • Areas of non-compliance identified which could ultimately lead to the above outcomes • A control issue relating to any fraud committed by any member of senior management which could have an important compliance or regulatory impact	• Actual or potential for public censure, fines or enforcement action (including requirement to take corrective action) by any regulatory body • Areas of non- compliance identified which could ultimately lead to the above outcomes	• Actual or potential for non-public action (including routine fines) by any regulatory body • Areas of noncompliance identified which could ultimately lead the above outcome
Remediation timeline	• Such an issue would be expected to receive immediate attention from senior management, but must not exceed 60 days to remedy	• Such an issue would be expected to receive corrective action from senior management within 1 month, but must be completed within 90 days of final Audit Report date	• Such an issue does not warrant immediate attention but there should be an agreed program for resolution. This would be expected to complete within 3 months, but in every case must not exceed 120 days

Appendix 4

Distribution

Addressee(s)	Chuck Bowen, Counsel – Ethics and Compliance (Privacy Officer)
Copies	**Business Leaders:** Barry Gilway, President/CEO/Executive Director Dan Sumner, Chief Legal Officer & General Counsel Jay Adams, Chief – Claims Steve Bitar, Chief – Underwriting & Agency Services Kelly Booten, Chief System & Operations Jennifer Montero, Chief Financial Officer Violet Bloom, VP - Human Resources Christine Turner Ashburn, VP-Communications, Legislative & External Affairs Bruce Meeks, Inspector General Nancy Staff, Director – Ethics and Compliance **Audit Committee** Juan Cocuy, Citizens Audit Committee Chairman Bette Brown, Citizens Audit Committee Member Jim Henderson, Citizens Audit Committee Member **Following Audit Committee Distribution** The Honorable Rick Scott, Governor The Honorable Jeff Atwater, Chief Financial Officer The Honorable Pam Bondi, Attorney General The Honorable Adam Putnam, Commissioner of Agriculture The Honorable Joe Negron, President of the Senate The Honorable Richard Corcoran, Speaker of the House of Representatives The External Auditor

Audit Performed By

Auditor in Charge	Bill Atwood, Senior Internal Auditor
Under the Direction of	*Joe Martins* *Chief of Internal Audit*