DISTRICT OF COLUMBIA
DEPARTMENT OF INSURANCE,
SECURITIES AND BANKING
Thomas E. Hampton, Commissioner

FINAL REPORT

STATUS OF INSURANCE INDUSTRY PRACTICES AND PROCEDURES TO PROTECT THE PRIVACY OF CUSTOMER INFORMATION

in cooperation with

THE NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

May 2006

Table of Contents

Summary

This report presents the findings of a comprehensive survey (conducted through statutory examinations) of the privacy practices and procedures of over 100 of the largest insurance groups — representing approximately 800 insurance companies — operating in the United States.

The survey was performed by the Insurance Commissioner of the District of Columbia ("DC Insurance Commissioner"), in cooperation with the National Association of Insurance Commissioners ("NAIC"). The purpose of the survey was to ascertain to what extent insurance companies have put into place practices and procedures which protect customer information in accordance with the privacy provisions of the Gramm-Leach-Bliley Act and in conformity with the model privacy act and regulations adopted by NAIC.

The general results of the study are as follows:

- Overall, there is significant compliance with the provisions of the NAIC model regulations implementing the Gramm-Leach-Bliley Act ("GLB Act"). The safeguarding provisions of the GLB Act, however, appear to have generated a higher level of non-compliance.

- There is a greater level of non-compliance with the provisions of NAIC's 1982 model privacy act, which may warrant further vigilance by state insurance regulators.

- The examinations documented 384 findings, out of over 9000 possible findings.

- Of the 384 findings, 215 related to GLB Act provisions and 169 related to NAIC's 1982 model privacy act. [1]

- With respect to compliance with the NAIC model regulations implementing the GLB Act:

    - There were no findings related to GLB Act procedures for providing opt-out notifications and 2 finding on procedures for collecting opt-out elections.

    - Although there were 23 findings related to the GLB Act-mandated delivery of privacy notices, 14 of those findings related to the

[1] The number of findings for the GLB Act and the NAIC 1982 model is likely to underestimate the relative level of compliance with the provisions of those laws, since fewer than 10% of the questions that were part of the Questionnaire developed to determine compliance with these laws related directly to the NAIC 1982 model. In addition, only approximately 15 states have implemented the NAIC 1982 model, and therefore fewer insurers are subject to the model's provisions.

provision of the initial notice, and therefore do not represent recurring findings.

- The second most common findings overall in the survey (43 findings) were related to the GLB Act-related risk assessment process, with common findings within this category related to a failure to work toward a formalized risk assessment process.

- The examinations documented a number of findings (39 findings) related to the GLB Act-related requirements for information storage, transmission, and integrity.

- The most common findings overall (169 findings) were related to NAIC's 1982 model privacy act provisions, largely dealing with the customer's right to correct personal information.

- Of the 112 entities (representing approximately 700 insurance companies)[2] for which data has so far been collected:
  - 26 had no examination findings
  - 44 had one or two examination findings
  - 28 had three or four examination findings
  - 11 had five to nine examination findings
  - 3 had ten or more examination findings

  NOTE: There were 93 possible findings.

- Of those companies with initial findings, 44 have committed, by sworn affidavit to correct the findings.

Overall, the survey indicates that there is significant compliance with the GLB Act requirements incorporated in NAIC's "Privacy and Consumer Financial and Health Information" model regulation. That model was adopted in 2000 and has been implemented in almost every jurisdiction. There is a greater degree of non-compliance (or non-documented compliance) with the GLB Act-related provisions incorporated in NAIC's "Standards for Safeguarding Customer Information". Although the survey did not directly address the reason why there was greater non-compliance with these provisions, it seems reasonable to speculate that some non-compliance may be due to the fact that this model regulation was not adopted by NAIC until 2002 and as of June 2003 it had not been implemented by even a majority of states.

The survey found the greatest degree of non-conformity with the provisions of NAIC's "Insurance Information and Privacy Protection" model act, adopted in

[2] As discussed more fully in the Methodology section of this report, the number of entities includes both: (1) undivided insurance groups; and (2) sub-groups of certain insurance groups. Sub-groups of insurance groups were established where the insurance group maintained different privacy programs for different insurance companies in the group.

1982. This model incorporates standards greater than those required by the GLB Act and has been adopted by approximately 15 states.

Background

In November 1999, the United States Congress approved the Gramm-Leach-Bliley Act (Pub. Law 106-102, 113 Stat. 1443) ("Act"), in an effort to modernize the government's regulation of financial services institutions, including insurance companies. Title V of the Act imposes on insurers certain requirements to protect the non-public personal information of their customers; specifically, the Act requires insurers to provide an initial and annual notice to each of its customers setting forth the insurer's privacy policy and also requires insurers to provide customers with the opportunity to opt out of the disclosure of any non-public personal information.[3] The Act also imposes requirements on state insurance regulators; specifically, state insurance regulators are required to establish regulatory standards that ensure "the security and confidentially of customer records and information", "protect against any anticipated threats or hazards to the security or integrity of such records", and "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[4]

In response to the GLB Act, NAIC in September 2000 adopted the "Privacy of Consumer Financial and Health Information Regulation", to provide a model set of regulations that the states could adopt to implement the notice and disclosure provisions of the GLB Act. [5] The model regulation contains provisions requiring an insurer to provide notice to individuals about its privacy policies and practices; setting forth the circumstances under which an insurer may disclose non-public personal information to affiliates and third parties; and establishing a method for customers to prevent insurers from disclosing non-public personal information. In addition, in 2002, NAIC adopted "Standards for Safeguarding Customer Information Model Regulation" to provide to the states model standards for developing and implementing administrative, technical, and

---

[3] *See* 15 USC §§ 6801-6827.

[4] 15 USC § 6801.

[5] *See* NAIC Model Laws, Regulations and Guidelines, IV-672-1. As of November 2002, NAIC records indicated that: 36 states plus the District of Columbia have enacted regulations and/or laws based on NAIC's 2000 Model (of those 36 states, 22 states include the financial and health provisions of the model and 14 states plus the District of Columbia have financial but not health provisions of the model); 13 states have retained NAIC's 1982 Insurance Information and Privacy Protection Model Act (several of these states have incorporated some GLB privacy protections into their current laws); and 1 state had privacy regulations pending, but had not taken final action. 2003 NAIC Proc. 4th Qtr. 1087, 1095. At a June 2003 NAIC Privacy Issues Working Group meeting, NAIC staff reported that all states have taken action to implement the privacy protections set forth in the GLB Act, either through NAIC's 2000 Model or NAIC's 1982 Model, and that one state is working on finalizing its rules. 2003 NAIC Proc. 2nd Qtr. at 117.

physical safeguards to protect the security, confidentiality, and integrity of customer information, in accordance with the GLB Act.[6]

Neither of these model regulations was NAIC's first effort to address the issue of insurance customer privacy. In 1982, NAIC adopted the "Insurance Information and Privacy Protection Model Act". The purposes of that model act were, among others, to "establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions", "to establish a regulatory mechanism to enable natural persons to ascertain what information is being or has been collected about them in connection with insurance transactions and to have access to such information for the purpose of verifying or disputing its accuracy", and to "limit the disclosure of information collected in connection with insurance transactions."[7]

In 2002, members of NAIC began discussing how to ensure that insurance companies were in compliance with the privacy provisions of the Gramm-Leach-Bliley Act and the relevant provisions of NAIC's model laws and regulations. In response to these discussions, the DC Insurance Commissioner agreed to have his jurisdiction become the lead state for a NAIC-supported, multi-jurisdictional review of the privacy policies and procedures of insurance companies operating throughout the United States. [8] A multi-state uniform review was intended to forestall multiple, overlapping, and inconsistent examinations by numerous states of company compliance with essentially the same obligations to protect the privacy of customer information. To carry out this review, the DC Insurance Commissioner entered into an agreement with a lead consulting firm, PricewaterhouseCoopers LLP, to assist the Commissioner in conducting assessments of the privacy policies and procedures of approximately 130 insurance groups. The insurance groups were selected by the Insurance

---

[6] *See* NAIC Model Laws, Regulations and Guidelines, IV-673-1. At a June 2003 NAIC Privacy Issues Working Group, NAIC staff reported that 23 states had taken action to promulgate the Safeguarding Model Regulation. 2003 NAIC Proc. 2nd Qtr. at 117.

[7] *See* NAIC Model Laws, Regulations and Guidelines, IV-670-1. In 2003, NAIC reported that 16 states had adopted this model regulation. See 2003 NAIC Proc. 2nd Qtr. at 35. Other NAIC information indicates that 13 states have retained the provisions of the 1982 model. An April 2002 report of the United States General Accounting Office indicated that 14 states had adopted NAIC's 1982 Model, although some states had modified the model in light of the GLB Act requirements. See General Accounting Office, *Status of State Actions on Gramm-Leach-Bliley Act's Privacy Provisions* at 3 (2002).

[8] Other jurisdictions which agreed to participate in the review (so-called "participating states") were provided with copies of the individual reports and agreed not to perform a privacy exam on the reviewed companies for a period of three years, except under limited circumstances. Seventeen states and Puerto Rico signed formal agreements to participate in the project. The 17 states were: Alabama, Arkansas, California, Colorado, Hawaii, Idaho, Indiana, Kansas, Michigan, Nevada, New Hampshire, New Jersey, New York, Ohio, Oregon, Utah, and Vermont. Many other states indicated that they would be interested in the results of the examination and would refrain from performing their own examination of the same privacy issues, but declined to execute formal agreements. Only three states indicated that they would not participate in any manner in the survey.

Commissioner and an NAIC working group.[9] The DC Insurance Commissioner thereafter worked with the lead consultant, in consultation with NAIC and interested state regulators, to develop a Privacy Assessment Questionnaire, which was used as the main vehicle to perform a gap analysis of the companies' privacy policies and procedures vs. the privacy provisions of the Act and the NAIC model laws and regulations.[10]

The Questionnaire asked questions targeted at determining an insurer's practices related to specific substantive areas covered by the NAIC model law and regulations. Specifically, the following areas were addressed by the Questionnaire:

Substantive Area	Description of Substantive Area	Questions Addressing Substantive Area
Privacy of Consumer Financial and Health Information Model Regulation (NAIC 2000 Model)		
Delivery of privacy notices	Are notices delivered to customers and consumers as required by applicable laws and regulations?	Questions 1-7, 38
Content of privacy notices	Do notices contain all required disclosures?	Questions 8 -23
Policies and procedures for preventing unauthorized disclosures of information	Do policies and procedures protect against threats to the security and integrity of information and against unauthorized access to or use of nonpublic personal information?	Questions 31-32, 36-37, 39-40
Policies and procedures for obtaining authorization for disclosure of health information	Do policies and procedures provide customers and consumers the ability to restrict the sharing of information or direct the use of information?	Questions 33-35

[9] Because of consent issues raised by some of the companies related to the lead contractor assisting in the review, the DC Insurance Commissioner entered into an agreement with a second contractor, American Express Tax and Business Services, Inc., to perform certain of the reviews. Because of further consent issues raised by certain of the remaining insurance companies relating to the second contractor, the DC Insurance Commissioner entered into an agreement with a third (and final) contractor, Huff Thomas & Co. .

[10] Except for California licensees, state variations in these laws were not explicitly addressed in the Questionnaire.

Substantive Area	Description of Substantive Area	Questions Addressing Substantive Area
Policies and procedures for privacy complaints	Has the licensee developed a method for tracking, logging, and analyzing privacy complaints?	Question 41
Procedures for providing opt-out notifications	Do procedures provide customers and consumers opt-out notifications as permitted by applicable laws and regulations?	Questions 42-43, 45-48, 54-55
Procedures for collecting opt-out elections	Are opt-out notices and rights provided in accordance with applicable requirements?	Questions 44, 49-53
Standards for Safeguarding Customer Information Model Regulation (NAIC 2002 Model)		
Licensee's methodology in designing their information security policy	Does the policy address applicable laws and regulations?	Questions 56-58, 90
Content of information security policy	Do policy provisions explicitly address security and confidentiality of customer information, threats or hazards to the security and integrity of information, and unauthorized access to or use of information?	Questions 59-61
Information security awareness and training	Does the policy provide for awareness and training detailing acceptable activity and the consistent classification of sensitive customer information?	Questions 62, 87

Substantive Area	Description of Substantive Area	Questions Addressing Substantive Area
Risk assessment process	Does the policy provide for an initial and periodic risk assessment, which identifies internal/external threats/hazards to the safeguarding, confidentiality, and integrity of information?	Questions 63-69, 88
Access controls	Do policies and procedures provide for physical and logical controls, i.e., secured areas, password controls, access based on user job function, periodic re-evaluation, and the expeditious removal of terminated users?	Questions 70-71, 73, 79, 81, 82
Information storage	Do policies and procedures address internal and external backup, storage, and retrieval of information?	Questions 72, 74-76, 85
Information transmission	Do policies and procedures govern scenarios for the sending and receipt of information, i.e., authentication of sender/recipient and use of encryption?	Questions 77, 78
Information integrity	Do policies and procedures address the monitoring of and actions to be taken if an attack to systems or storage devices is identified?	Questions 77, 78, 80, 83, 84
Miscellaneous	Does the licensee have appropriate procedures related to business continuity, oversight of the information security program, and vendor selection and monitoring?	Questions 86, 89, 91-93

Substantive Area	Description of Substantive Area	Questions Addressing Substantive Area
Insurance Information and Privacy Protection Model Act (NAIC 1982 Model)		
Customer access to and ability to correct information	Do policies and procedures grant customers the appropriate rights related to access and correction of their information?	Questions 24-30

It should be noted that it was not the intent of the examination to determine whether individual companies were in violation of specific state or federal statutes. Rather the purpose was to identify and assess the practices and procedures implemented by companies to provide protection for the privacy of personal information, as generally required by law.

Methodology

Selection of Insurance Companies

A comprehensive list of major insurance groups was prepared. The list was comprised of property and casualty insurance groups with 2002 gross written premiums of approximately $250 million or more; life insurance groups with 2002 gross written premiums of approximately $200 million or more; and health insurance groups with 2002 gross written premiums of approximately $500 million or more. This initial list contained 129 insurance groups. After the initial list was compiled, 25 groups were exempted from examination for one of three reasons: (1) there was a prior, ongoing, or upcoming examination of the group that included (or would include) a comprehensive review of the group's privacy policy [22 groups]; (2) the group engaged primarily or solely in reinsurance [2 groups]; or (3) the state insurance regulator for the company's state of domicile requested that the group be exempted [1 group].

After the revised list was compiled, the companies were asked to complete a Privacy Program Questionnaire to determine whether all of the insurance companies within each insurance group used the same privacy program, or if there were multiple programs with the same group. If it was determined that more than one privacy program was used by the insurance companies within an insurance group, the insurance group was divided into sub-groups for the purposes of examination. (Each sub-group was comprised of the insurance companies within the insurance group that used the same privacy program.) Five insurance groups were divided into fourteen sub-groups through this process. In total, therefore, 112 insurance entities — comprised of 98 undivided insurance groups and 14 insurance sub-groups (created by the sub-division of five insurance groups) — became subject to examination under the current survey.

Study Protocol

Each examination of an insurer's privacy practices and procedures was performed as a limited scope market conduct examination pursuant to generally applicable procedures promulgated by NAIC. Each examination was "called" by the DC Insurance Commissioner, except where the insurance company was not licensed in the District of Columbia; in those cases, the examinations were called by a participating state where the company was licensed.[11]

A Privacy Status Review Questionnaire ("Questionnaire") was developed to begin assessing each insurer's privacy practices and procedures in comparison with the privacy practices and procedures embodied in the NAIC's three policy models: NAIC's "Privacy of Consumer Financial and Health Information Model Regulation" of 2000; NAIC's "Standards for Safeguarding Customer Information Model Regulation" of 2002; and NAIC's "Insurance Information and Privacy Protection Model Act" of 1982. (The first two models were designed to implement the Gramm-Leach-Bliley Act.) The Questionnaire also addressed the underlying factors that may increase the risk of non-compliance with these privacy laws.

The Questionnaire asked 93 specific questions. The questions required each insurer to make representations as to whether it was performing procedures established by the privacy laws, provide descriptions of any existing processes or procedures related to privacy compliance, and attach relevant documentation to support the existence of such processes or procedures.

The scope of the work did **not** include: (1) a review of the insurer's efforts with respect to remediation activities; (2) a detailed analysis of the effectiveness of the insurer's plans to correct privacy problems or to protect the business against the consequences associated with any privacy related occurrences, or (3) a determination of steps the insurer must take to become privacy compliant or maintain privacy compliance.

An objective, independent preliminary analysis summary of each insurer's answers to the Questionnaire was performed by the DC Insurance Commissioner and the Commissioner's consultant and provided to each group. A group's review of its analysis summary was followed by conferences with representatives of the insurer for further subject matter clarity.

Based on the responses to the Questionnaire, the information provided in the analysis work papers and the final analysis summary, a draft examination report was produced. The report contained an overview of the examination process and included a list of specific findings, where applicable. A finding consisted of an occurrence of a perceived gap between the companies privacy practices and

[11] The participating states that called exams on companies not licensed in the District of Columbia were Alabama, Arkansas, Indiana, New Jersey, and Oregon.

procedures and the guidelines outlined in one of the model acts or regulations of the NAIC. (Compliance with the Gramm-Leach-Bliley Act was not considered separately, since its provisions were incorporated through the NAIC's models.) The report recommended that the insurer consider addressing each finding.

The draft examination report was provided to the insurer and the insurer was allowed a 30-day period in which to make a written submission to the DC Insurance Commissioner containing comments or a rebuttal with respect to matters in the draft report. In addition, the insurer was provided the opportunity to provide an affidavit to the Department setting forth its sworn commitment to correct findings; if an affidavit in appropriate form and content was received by the Department, the final report was modified to remove the finding with respect to the gap that had been corrected.[12]

Supporting work for the group-specific public reports is protected under confidentiality. Areas of this report that regulators and lawmakers need elaborated should be directed to the DC Insurance Commissioner.

Findings

Based on the results of the Questionnaire, a total of 93 findings were possible for each company. The numbers of findings for each company are presented in the table below.

Number of Findings	Number of Companies
0	26
1	21
2	22
3	19
4	10
5	2
6	2
7	0
8	4
9	3
10+	3

In total, there were 384 findings. The breakdown of the findings as they relate to the NAIC models was as follows:

NAIC Model(s)	Number of Findings
2000/2002 Gramm-Leach-Bliley Models	215
1982 Privacy Model	169

[12] Unless otherwise noted, the information in this report refers to the pre-affidavit findings of the examinations.

NOTE: Forty-seven of the 2000/2002 findings were associated with only two companies.

The two substantive areas with the most findings were "customer access to and ability to correct information" (NAIC 1982 Model) and "risk assessment process" (NAIC 2002 Model). There were 169 findings related to customer access to and ability to correct information, with 60 companies having a finding that an element (or elements) of an individual's right to correct their personal information do not appear to be addressed in the procedures provided.[13] There were 43 findings related to the risk assessment process, with 11 findings from companies failing to formalize information security training. In addition, there were 39 findings related to the GLB Act-related requirements for information storage, transmission, and integrity.[14]

One substantive area had no findings. That area was "procedures for providing opt-out notifications". The area of "procedures for collecting opt-out elections" was found in only 1 group.

The following chart provides a complete overview of all of the findings from the examinations.

---

[13] Approximately 28% of companies reviewed that write business in NAIC 1982 Model states have notices that are missing elements outlined in sections 8 and 9 of the NAIC 1982 Model. The rights outlined in sections 8 and 9 relate to the customers' rights to access, correct, amend, and delete their personal information. Many companies did not feel that all the detailed elements related to these rights should be disclosed and that, if disclosed, the notices would be lengthy and somewhat confusing to customers.

[14] There were also 23 findings related to the insurer's delivery of privacy notices; however, 14 of the findings related to the company's failure with regard to the initial privacy notice which was to reach customers by July 1, 2001, and therefore do not represent a continuing finding.

FINDINGS[15]

FINDING	NUMBER OF COMPANIES
Privacy Notice And Customer Verification	
Delivery of Privacy Notices	
A – The company did not adequately define non-public information in its privacy notice. [Question 1]	1
A/B – The companies either did not disclose the end of the initial privacy notices mailing period or the mailing period provided caused a risk that the initial privacy notices did not reach customers by July 1, 2001 (e.g., mailed notices through June 29, 2001). [Question 2]	14
A – The companies did not provide documentation to support that it was certain who the clients are or the status of the client (customer and customer status). [Question 3]	2

[15] The letter preceding each finding represents the following:

A: The Company does not appear to provide a clear and/or full answer to the question and the narrative explaining the process or procedure and/or the documentation actually supplied in response to the question, absent other information, appears to show that: (1) The Company's process and procedures in this area are not reasonably designed to achieve compliance with the NAIC model; or (2) The Company's processes or procedures are potentially not in compliance with the NAIC model. Additional examination may show that the Company is in compliance with the NAIC models.

B: The Company appeared to answer the question fully and provided relevant documentation, but the narrative explaining the process or procedure and/or the documentation appears to show that: (1) The Company's process and procedures are not reasonably designed to achieve compliance with the NAIC model; or (2) The Company's processes or procedures are potentially not in compliance with the NAIC model. Additional examination may show that the company is in compliance with the NAIC model.

C: The narrative explaining the process or procedure and/or the documentation supplied in response to question when considered along with other questionnaire responses appear to indicate that the processes and procedures in this area may contribute a pervasive risk of potential noncompliance with the NAIC model.

FINDING	**NUMBER OF COMPANIES**
A – Although Section. 11 (E)(1) and (2) regarding retention or accessibility of notices for customers does not impose a duty on an insurer to maintain historical records, the company maintains records of customers who receive privacy notices for a 24-month period of time. A 24-month look-back may not be sufficient to support the Companies assertion that all and every consumer received appropriate notification. [Question 4]	2
A – No description or evidence of procedures that would ensure annual policies sent separately are mailed to all customers. [Question 5]	1
A – The company's response does not address the aspects of the question relating to "consumers". For instance, the company does not address whether consumers receive or should receive the notice, what criteria is used to identify consumers, or if this aspect of the question is not applicable, why it is. Additionally, while the company's response indicates there have been no substantive changes to their privacy policy, it does not address what they have defined to be a substantive change versus a non-substantive change to their privacy policy. [Question 6]	1
A – The company did not state whether or not it provides an electronic or hard copy of the privacy notice. [Question 7]	1
B – The company has explained that some agents do provide insurance products on their websites and "to the best of their knowledge" provide notices by mail accompanying new policies. It must be determined what, if any other methods of distribution exist when products are offered online. The company has noted that they require their agents to abide by all applicable laws. [Question 38]	1
INTENTIONALLY LEFT BLANK	

FINDING	**NUMBER OF COMPANIES**
Content of Privacy Notices	
B – The company did not provide sufficient information to reverse the examiners finding regarding the company's privacy notice being clear and conspicuous. [Question 8]	2
B – The company did not provide sufficient information to reverse the examiners finding regarding the company's information handling practices. [Question 9]	1
B – The companies did not address how they handle former customer personal information within the privacy notice. [Question 14]	3
A – The companies did not provide evidence of the methods used to ensure that the representations of company policy made in their privacy statements are being complied with on an ongoing basis. [Question 22]	4
Policies and procedures for preventing unauthorized disclosures of information	
A – The companies have not provided explanations and/or evidence of policies and procedures that ensure non-public personal financial information that is received from a non-affiliated financial institution is only used in compliance with the NAIC model regulation. [Question 31]	3
A – The companies have not provided explanations or documentation of their controls in place to limit sharing of account numbers or access codes with third parties. [Question 32]	3
A – The companies did not provide enough evidence to indicate that health information may not be shared outside the legal exceptions without an authorization. [Question 36]	4

FINDING	NUMBER OF COMPANIES
A – The companies have not provided explanations of the relevant policies and procedures that help ensure non-public personal financial information is not disclosed outside of the allowable exceptions without offering an opt-out. [Question 37]	2
A – The companies failed to provided enough evidence of policies that help ensure that non-public personal financial information obtained from non-affiliated financial parties is not used other than for the purpose for which it was received. [Question 40]	4
Policies and procedures for obtaining authorization for disclosure of health information	
B – The companies' authorization form stated that the authorization shall be valid for 36 months or how determinations are made whether an authorization was needed for sharing non-public health information. [Question 33]	2
B – Section 18.B. of the NAIC 2000 Model states that the authorization should remain valid for no more than 24 months. The companies' authorization forms stated that the authorization shall be valid for 36 months. [Question 35]	10
Policies and procedures for privacy complaints	
B – The company has explained that the privacy officer will handle any privacy-related complaints, but a formalized method in which complaints are logged, tracked, and analyzed does not exist. [Question 41]	1
Procedures for providing opt-out notifications	
NONE	

FINDING	NUMBER OF COMPANIES
Procedures for collecting opt-out elections	
B – The company failed to provide adequate explanations or include relevant policies supporting its controls to ensure that customers who have opted out do not have their information shared other than allowed under the exceptions pursuant to NAIC Model 672. [Question 52]	1
B – The company did not provide a description of the controls in place to prevent discrimination against customers that have opted out from being denied benefits based on their opt out preference. [Question 53]	1
Safeguarding of Customer Records	
Licensee's methodology in designing their information security policy	
B – The company does not currently have an information security policy in place. The company stated, "We are currently developing the company's information security policy based on company security practices and policies." The company has also provided its privacy policy and Internet, email, and VPN policies as examples of its security practices. [Question 56]	1
B – The companies provided Information Systems Security Manuals; however, the manuals did not reference the objectives outlined in the GLB Act. [Question 58]	4
A – Groups have been assigned the task of keeping the company abreast of changing technology, laws and regulations, etc. that may necessitate a change in the company's approach to its information security program. The company did not indicate how often the processing for adjustments to the information security program is performed (e.g., annually). [Question 90]	4

FINDING	NUMBER OF COMPANIES
Content of information security policy	
B – The companies' responses refer to restrictions for accessing customer data. There was no reference to information security standards, policies, or procedures or there was a failure to provide evidence to adequately reflect a positive response to all aspects of the question. In addition, one company also provided its Information Systems Security Manual; however, this manual does not sufficiently address the necessary security policies and procedures outlined in the GLB Act. [Question 59]	4
B – Assigned responsibilities of creating, maintaining, and implementing the security program are not described in sufficient detail. The company is currently in the search process for a Chief Information Security Officer. The company plans on reviewing all existing policies and procedures in light of the new administration and imaging systems being installed. [Question 61]	1
Information security awareness and training	
B – The companies are developing formalized information security training for their employees but currently evidence of training is inadequate. [Question 62]	3
B – The companies had not implemented formal information security training programs. [Question 87]	8
Risk assessment process	
A – The company's response provides no explanation of how the information security program was designed to be in compliance with regulatory guidance. [Question 63]	1
B – The companies are working toward formalizing risk assessment processes. [Question 64]	7

FINDING	NUMBER OF COMPANIES
B – The companies are working toward formalizing risk assessment processes. [Question 65]	5
B – The companies are working toward formalizing risk assessment processes. [Question 66]	9
A – The companies did not provide evidence that they are performing regular risk assessments for the determination of risk levels for sensitive information. [Question 67]	5
A – The companies are working toward formalizing risk assessment processes. [Question 68]	5
A – The companies did not indicate whether it monitors, evaluates, and adjusts risk assessments based upon changes in technology or sensitivity of customer information. [Question 69]	7
B – The companies did not have policies surrounding an independent security certification or internal audit or provide adequate responses. [Question 88]	4
Access controls	
B – The companies have stated that employees' level of access to customer information is not currently evaluated annually in order to ensure that each employee's level of access to customer information is necessary. Projects are currently underway to review the access level of associates. [Question 70]	4
B – The company's response to the examiners indicated that there were no procedures in place for periodic reviews of user access for active employees. [Question 71]	3

FINDING	**NUMBER OF COMPANIES**
B – Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 73]	3
A – Companies admitted that "live production" customer information is used in test environments. Polices that pertain to areas which use "live production" customer information in test environments were not provided. In addition, a business case use for the need to use "live production" customer information for testing was not provided. [Question 79]	4
B – Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 81]	3
B – Companies stated that employees who administer customer accounts have the ability to input and approve data; however, the system process will check and identify invalid data. Companies also failed to provide sufficient evidence to support their compliance positions. [Question 82]	5
Information storage	
B – Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 72]	1
A – Documentation was not provided which evidences that companies has implemented policies that require: o Authentication of users in order to access databases that contain customer information. o Access to customer information to be granted only to individuals that require that access to perform their job. o Customer information within databases to be encrypted and integrity checks to be performed with respect to the customer information. [Question 74]	3

FINDING	**NUMBER OF COMPANIES**
A – No documentation was provided as evidence of policies and procedures that ensure physical security controls such as access cards, security guards, surveillance cameras, and access logs are incorporated into the company's security policies and procedures. In addition, no evidence of policies and procedures was provided that ensure locking of file drawers and security cages which contain paper forms with customer information on them. [Question 75]	2
A – The company appears to have addressed all of the issues correctly; however, the company did not provide documentation that evidences only approved vendors can be used to store customer information. Procedures for retrieving stored information from remote storage facilities in a secure manner also were not provided. [Question 76]	2
B – The company's policy simply states that "adequate" controls should be in place to protect data centers against environmental hazards; however, there is no detailed explanation of the specific mechanisms or strategies that have been deployed for doing so. [Question 85]	2

FINDING	**NUMBER OF COMPANIES**
Information transmission and integrity	
A – No documentation was provided as evidence of the following policies and procedures: o Policies requiring the listing of all file transmissions that are scheduled to occur on a regular basis, indicating the third party to whom the transmission is going, the purpose of the transmission, and the customer information contained within the transmission. o Policies designed to ensure data downloads or transmissions are appropriate, the business need is understood, the sensitivity of the information is communicated, and safeguards are in place. o Policies, procedures, or controls to protect the security and integrity of customer information that is being transmitted to third parties. o Controls to limit the employees who are authorized to perform or modify transmissions of customer information. o Controls that are in place to protect external transmissions of customer information from unauthorized access attempts (e.g. encryption, frame relay, other). [Question 77]	7
A – The company has indicated that they use the secure socket layer (SSL) 128-bit encryption technique to protect customer information during transmission; however, the company did not provide policies that indicate how or when encryption should be utilized to protect customer information during transmission. [Question 78]	4

FINDING	**NUMBER OF COMPANIES**
A/B – The company's policies surrounding changes to systems containing customer information are not described using appropriate detail required to answer this question or do not exist: o conducting a review of information security changes to systems containing customer information o evaluating the impact of information security changes to systems containing customer information o adjusting information security based on evaluation of the information security changes to systems containing customer information. [Question 80]	7
B – Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 83]	4
B – Currently no formal policies or procedures are in place to handle the occurrence of a network intrusion or the escalation of unusual activity. [Question 84]	7
Miscellaneous	
A – The companies either stated that a business continuity plan exists and that it addresses all of the necessary issues but failed to provide proof of existence or denied having a business continuity plan. [Question 86]	2
A – Contact information of the liaison between the board or management and the Corporate Information Security Group was not provided. [Question 89]	1
A – The companies did not provide documentation to support that they have included privacy language in joint marketing or service provider agreements. [Question 91]	5

FINDING	NUMBER OF COMPANIES
A – The companies did not provide sample language from a service provider contract used with a third party service provider. [Question 92]	5
B – The companies does not currently have a process to evaluate whether service providers have taken the appropriate steps to safeguard non-public personal information. [Question 93]	9
Customer access to and ability to correct information (1982 Model Law)	
Customer access to and ability to correct information	
B – The company stated that, when performing this review, it was determined two of the companies did not implement procedures to provide the Notice of Insurance Information Practices in Ohio, Wisconsin, and Minnesota. A shorter notice was used in these states, which did not include all the elements listed in the regulation. The company stated that they have taken the necessary steps to update their notices for these states. [Question 24]	1
B – Although the companies provide notice at the time of policy delivery when personal information is collected only from either the applicant or public records, an index evidencing the existence of this procedure was not provided to the examiners. [Question 25]	2
B – Although the companies have required their agents to distribute notices, copies of relevant policies that ensure notices are provided at the time of collection of personal information when personal information is collected from a source other than from the applicant or public records are not maintained. Agents are required by their contract to provide notices at the time of collection of personal information, and the company has noted that they will update their written instructions to agents reminding them of their contractual obligations. [Question 26]	5

FINDING	**NUMBER OF COMPANIES**
B – The company does not provide a notice prior to policy renewal when personal information is collected from a source other than from applicant or public records and a privacy notice has not been provided in the previous twenty-four months. [Question 27]	1
B – The companies' Notice of Insurance Information Practices is missing the following elements of Sections 8 and 9: Section 8 (1) The ability for individuals to see a copy of their personal information in person. (2) The requirement of provided personal information to include the source types of the information collected. Section 9 (1) The right of the individual to file a statement of why they disagree with the company's decision on their request for revision to their information and the need to keep such statement in the customer's file. (2) The need to send any revisions made to those parties that have been provided such information within the past 2 years and support organizations that have received such information in the past 7 years. (3) Within 30 days the recipient of a request must correct, amend, or delete the personal information or notify the individual of a refusal, the reasons for the refusal, and the individual's right to file a statement. (4) Upon a correction, amendment, or deletion the insurance institution, agent, or support organization must notify the individual in writing and furnish the correction to any entity described in Section 9.B.(1)–(3) of the NAIC 1982 Model. [Question 28]	47

FINDING	**NUMBER OF COMPANIES**
B – The company's policies and procedures did not address that the following activities needed to take place within 30 business days of receipt of a customer request: (1) Inform the individual of the nature and substance of the recorded information. (2) Permit the individual to see a copy of the recorded information in person or by mail. (3) Disclose the identity of the persons, agents, or institutions that accessed such personal information within the past two years. (4) Provide the individual a summary of the procedures by which he or she may request correction, amendment, or deletion of recorded personal information. In several cases the company only provided a copy of its privacy notice, providing no evidence that they have procedures in place to respond appropriately to customer requests to access information. [Question 29]	53
B – The following elements of an individual's right to correct his or her personal information do not appear to be addressed in the procedures provided: (1) Requirement for the request to be responded to within 30 days. (2) The need to provide the corrected information to any person specifically designated by the individual who may have received the information in the prior 2 years. (3) The 7- year timeframe in which parties who have received such information should be provided with the corrected information. (4) The need to file the individual's statement of disagreement with his or her personal information and provide it to those reviewing the information in the future. In several cases the company only provided a copy of its privacy notice, providing no evidence that they have procedures in place to respond appropriately to customer requests to correct, amend or delete information. [Question 30]	60

As noted above, after the initial findings were made, each insurer was afforded the opportunity to provide an affidavit to the Department setting forth its sworn commitment to correct the findings. If the insurer provided an affidavit and the Department found that the commitments in the affidavit would correct the gap, the final examination report was modified to remove the finding.

Overall, 184 of the original 384 findings were cleared through the affidavit process. Of these cleared findings, the majority — 104 of 184 — were related to gaps in the companies' practices and procedures vs. the guidelines outlined in the NAIC 1982 model. The findings which were cleared through affidavits are set forth in the chart below.

CLEARED FINDINGS

CLEARED FINDING	NUMBER OF CLEARED FINDINGS
Privacy Notice And Customer Verification	
Delivery of Privacy Notices	
CLEARED: The company either did not disclose the end of the initial privacy notices mailing period or the mailing period provided caused a risk that the initial privacy notices did not reach customers by July 1, 2001 (e.g., mailed notices through June 29, 2001). [Question #2]	4
CLEARED: The company's procedure only determines whether an individual client has had a relationship with another corporate group entity. The procedure does not determine who the clients are or the status of the client (customer and consumer status). [Question #3]	1
CLEARED: Although Section. 11 (E)(1) and (2) regarding retention or accessibility of notices for customers does not impose a duty on an insurer to maintain historical records, the company maintains records of customers who receive privacy notices for a 24-month period of time. A 24-month look-back may not be sufficient to support the Company's assertion that all and every consumer received appropriate notification. [Question #4]	2

CLEARED FINDING	**NUMBER OF CLEARED FINDINGS**
CLEARED: The company's response does not address the aspects of the question relating to "consumers". For instance, the company does not address whether consumers receive or should receive the notice, what criteria is used to identify consumers, or if this aspect of the question is not applicable, why it is. Additionally, while the company's response indicates there have been no substantive changes to their privacy policy, it does not address what they have defined to be a substantive change versus a non-substantive change to their privacy policy. [Question #6]	1
CLEARED: The company has explained that some agents do provide insurance products on their websites and "to the best of their knowledge" provide notices by mail accompanying new policies. It must be determined what, if any other methods of distribution exist when products are offered online. The company has noted that they require their agents to abide by all applicable laws. [Question 38]	1
Content of Privacy Notices	
CLEARED: The company does not address how it handles former customer personal information within the privacy notice. [Question 14]	1
CLEARED: Management's response has not addressed whether or not the company performs any security audit or compliance procedures to ensure that the representations of company policy made in the privacy statement are being complied with on an ongoing basis. [Question 22]	1
Policies and procedures for preventing unauthorized disclosures of information	
CLEARED: The companies did not provide evidence of a policy or failed to explain its position on non-discloser of private personal health information without a customer authorization. [Question 36]	2

CLEARED FINDING	**NUMBER OF CLEARED FINDINGS**
CLEARED: The group did not provide a description of its efforts to assure information obtained from third parties is not reused or re-disclosed. [Question 40]	2
Policies and procedures for obtaining authorization for disclosure of health information	
CLEARED: An explanation was not provided of how determinations are made whether an authorization was needed for sharing of non-public personal health information. [Question 33]	2
CLEARED: Section 18.B. of the NAIC 2000 Model states that the authorization should remain valid for no more than 24 months. The company's authorization form stated that the authorization shall be valid for 36 months. [Question 35]	4
Policies and procedures for privacy complaints	
CLEARED: The company has explained that the privacy officer will handle any privacy-related complaints, but a formalized method in which complaints are logged, tracked, and analyzed does not exist. [Question 41]	1
Procedures for collecting opt-out elections	
CLEARED: The company stated that it has implemented policies, procedures and other controls to ensure that customers who have opted out do not have their information shared other than allowed under the exceptions pursuant to NAIC Model 672. However, the company did not provide an explanation or include relevant policies supporting this practice. [Question 52]	1

CLEARED FINDING	NUMBER OF CLEARED FINDINGS
CLEARED: The company stated that it does not deny customers benefits based on their opt out preference. However, the company did not provide a description of the controls in place to prevent discrimination against customers that have opted out. [Question 53]	1
Safeguarding of Customer Records	
Licensee's methodology in designing their information security policy	
CLEARED: The company provided its Information Systems Security Manual; however, it does not reference the objectives outlined in the GLB Act. [Question 58]	2
CLEARED: Groups have been assigned the task of keeping The company abreast of changing technology, laws and regulations, etc. that may necessitate a change in the company's approach to its information security program. The company did not indicate how often the processing for adjustments to the information security program are performed (e.g., annually). [Question 90]	1
Content of information security policy	
CLEARED: The companies did not provide evidence of formal documentation to adequately reflect a positive response to all aspects of the question. [Question 59]	2
Information security awareness and training	
CLEARED: Formalized customer/consumer privacy training for all employees of the group does not currently exist except for new hires. [Question 62]	1
CLEARED: The companies may offer limited training, a formal security training program for all employees that have access to customer information is not established. [Question 87]	3

CLEARED FINDING	**NUMBER OF CLEARED FINDINGS**
Risk assessment process	
CLEARED: The company is working toward formalizing a risk assessment process. [Question 64]	5
CLEARED: The company is working toward formalizing a risk assessment process. [Question 65]	3
CLEARED: The companies' narratives and lack of supporting documentation could not support a positive response to this question; evidenced by a lack of assessing risk in terms of confidentiality and integrity of customer information. [Question 66]	6
CLEARED: The responses did not adequately address the existence of an ongoing assessment of vulnerability. [Question 68]	3
CLEARED: The company did not indicate whether it monitors, evaluates, and adjusts risk assessments based upon changes in technology or sensitivity of customer information. [Question 69]	5
CLEARED: The responses did not adequately address the question or the company failed to provide a response. [Question 88]	3
Access controls	
CLEARED: The company has stated that employees' level of access to customer information is not currently evaluated annually in order to ensure that each employee's level of access to customer information is necessary. A project is currently underway to review the access level of associates. [Question 70]	2
CLEARED: Based on responses provided, it appeared the companies were taking steps to ensure compliance in this access area. [Question 71]	2

CLEARED FINDING	**NUMBER OF CLEARED FINDINGS**
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 73]	3
CLEARED: The company admits that "live production" customer information is used in test environments. Polices that pertain to areas which use "live production" customer information in test environments were not provided. In addition, a business case use for the need to use "live production" customer information for testing was not provided. [Question 79]	3
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 81]	3
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 82]	3
Information storage	
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 72]	1
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 74]	1
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 75]	1

CLEARED FINDING	**NUMBER OF CLEARED FINDINGS**
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 76]	1
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 85]	1
Information transmission and integrity	
CLEARED: No documentation was provided as evidence of certain policies and procedures. (See Findings chart for full description.) [Question 77]	5
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 78]	2
CLEARED: The company's policies surrounding changes to systems containing customer information are not described using appropriate detail required to answer this question or do not exist. [Question 80]	3
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 83]	3
CLEARED: Currently no formal policies or procedures are in place to handle the occurrence of a network intrusion or the escalation of unusual activity. [Question 84]	4
INTENTIONALLY LEFT BLANK	

CLEARED FINDING	**NUMBER OF CLEARED FINDINGS**
Miscellaneous	
CLEARED: Currently no formal policies or procedures are in place to handle a disaster or identify the company's continuity should an unforeseen event occur. [Question 86]	1
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 91]	2
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 92]	2
CLEARED: Based on the information provided or its insufficiency, the examiners determined that a positive response could not be given. [Question 93]	3
Customer access to and ability to correct information (1982 Model Law)	
Customer access to and ability to correct information	
CLEARED: Although the company does provide the notice at the time of policy delivery when personal information is collected only from the applicant or public records, an index evidencing the existence of this procedure was not provided. [Question 25]	1
CLEARED: Although the company has required their agents to distribute notices, the company does not maintain copies of relevant policies that ensure notices are provided at the time of collection of personal information when personal information is collected from a source other than from the applicant or public records. Agents are required by their contract to provide notices at the time of collection of personal information, and the company has noted that they will update their written instructions to agents reminding them of their contractual obligations. [Question 26]	4

CLEARED FINDING	**NUMBER OF CLEARED FINDINGS**
CLEARED: The company does not provide a notice prior to policy renewal when personal information is collected from a source other than from applicant or public records and a privacy notice has not been provided in the previous twenty-four months. [Question 27]	1
CLEARED: The company's Notice of Insurance Information Practices is missing the elements of Sections 8 and 9. (See Findings chart for full description.) [Question 28]	21
CLEARED: The company's policies and procedures did not address that the activities needed to take place within 30 business days of receipt of a customer request. (See Findings chart for full description.) [Question 29]	25
CLEARED: Elements of an individual's right to correct his or her personal information do not appear to be addressed in the procedures provided. (See Findings chart for full description.) [Question 30]	28

Conclusion

Overall, the survey found significant alignment of companies privacy practices and procedures with the GLB Act provisions incorporated into NAIC's model regulations. There appears, however, to be a lesser level of alignment with the information safeguarding provisions of NAIC's 2002 Model. In addition, there appears to be significant misalignment with the provisions of the 1982 Model Act. Some of this apparent misalignment, however, may be due to state variations in requirements, which the survey did not generally track. Because of the importance of maintaining the privacy of customer information — and because of the measurable, though not high, level of misalignment of insurers privacy practices and procedures with the model rules — continued vigilance by state insurance regulators is warranted.

ATTACHMENTS

ATTACHMENT A: LIST OF INSURANCE GROUPS AND COMPANIES EXAMINED

ATTACHMENT B: THEMES

ATTACHMENT C: QUESTIONNAIRE

ATTACHMENT D: ACKNOWLEDGEMENT

ATTACHMENT A
LIST OF INSURANCE GROUPS AND COMPANIES EXAMINED

This section presents in alphabetical order the insurance groups included in this report. The effective date of the organizational structures used in the survey are as of January 1, 2003

21st Century Insurance
AAA Life Insurance Company
Aegon Insurance Group
AFLAC Group
AIG Personal Lines
AIG SunAmerica Insurance Group
Allianz Insurance Group
Allianz Fireman's Fund Group
Allmerica Financial Group
American Express Group
American Family Insurance Group
American Modern Insurance Group
American National Insurance Company
American United Life Insurance Company
Americo Life Group
Ameriprise Financial Services, Inc
Ameritas Acacia Companies
Amerus Group
Amica Mutual of America Group
Anthem Insurance Group
Beneficial Life Insurance Company
Berkshire Hathaway Insurance Group
Bristol West Group
Businessmen's Assurance Company of America
California Casualty Group
Ceres Group
Cincinnati Insurance Companies
Citigroup American Health and Life Insurance Company
Citigroup National Benefit Life
Citigroup Primerica
Citigroup Travelers Life and Annuity
Clarendon Insurance Group
CNA Insurance Companies
Combined Insurance Group
Combined Sterling Group
Conseco
Country Mutual Insurance Company
CUNA Mutual
Direct General Group
EMC
Erie Insurance Group
Fidelity Insurance Group
GE Financial Group
GMAC Insurance Group
Golden Rule
Government Employees Group
Great American Insurance Group
Great West Insurance Group
Hartford Insurance Group, The
Harleysville Insurance Companies
Health Care Service Corporation
Home State Insurance Group
Horace Mann Insurance Group
ING Group
Inviva Securities Group
Jefferson Pilot Financial Companies
John Hancock Financial Services
Kansas City Life Group
Kingsway America Group
Knights of Columbus
Lafayette Life Insurance Company
Liberty Mutual Insurance Group
Lincoln National Corporation
Manulife Financial
Mass Mutual Life Insurance Company

Merrill Lynch
Metropolitan Mortgage Group
Minnesota Mutual Companies
Modern Woodmen of America
Motorists Insurance Group
National Life Group
Nationwide Group
NJM Insurance Group
Northwestern Mutual
Ohio Casualty Insurance Company
Ohio National Financial Services
Old Mutual US Life
Pacific Life Group
Penn Mutual Group
Phoenix Life Group
Physicians Mutual Group
Progressive Insurance Group
Protective Life Insurance Group
Prudential of America Group
Royal & Sun Alliance USA
Safeco
Sammons Financial Group
Security Benefit Group
Selective Insurance Group
Sentry Insurance Group
Shelter Insurance Companies
Shenandoah Life Group
Standard Management Corporation
State Auto Insurance Companies
State Farm Group
State National Insurance Companies
Sun Life Financial Group
Swiss Reinsurance Group
Thrivent Financial for Lutherans
Torchmark Corporation
Travelers Group
Union Central Life Insurance Group
United Life Insurance Company
Unitrin, Inc.
Unum Provident Insurance Group
Western & Southern Group
Westfield Group
White Mountains Insurance Group
Winterthur General Casualty
Woodmen of the World Life Insurance Company
Zurich North America

Insurance *companies* included in this report

21st Century Casualty Company
21st Century Insurance Company
21st Century Insurance Company of Arizona
AAA Life Insurance Company
Academy Life Insurance Company
Addison Insurance Company
AGL Life Assurance Company
AIG Annuity Insurance Company
AIG Hawaii Insurance Company Inc.
AIG Life Insurance Company
AIG National Insurance Company Inc.
AIG SunAmerica Life Assurance
AIU Insurance Company
Alabama First Insurance Company
All Savers Insurance Company
Allegiance Life Insurance Company
Allianz Insurance Company
Allianz Life Insurance Company of North America
Allianz Life Insurance Company of New York
Allied Property & Casualty Insurance Company
Allmerica Financial Alliance Insurance Company
Allmerica Financial Benefit Insurance Company

Allmerica Financial Life Insurance and Annuity Company
Alpha Property & Casualty Insurance
Alta Health & Life Insurance Company
AMCO Insurance Company
Ameribest Life Insurance Company
America First Insurance Company
America First Lloyds Insurance Company
American Ambassador Casualty Company
American and Foreign Insurance Company
American Automobile Insurance Company
American Casualty Company of Reading, Pennsylvania
American Central Insurance Company
American Centurion Life Assurance Company
American Country Insurance Company
American Deposit Insurance Company
American Economy Insurance Company
American Empire Surplus Lines
American Employers Insurance Company
American Enterprise Life Insurance Company
American Equity Insurance Company
American Equity Specialty Company
American Family Assurance of Columbus
American Family Home Insurance Company
American Family Life Assurance of New York
American Family Life Insurance Company
American Family Mutual Insurance Company
American Fire & Casualty Company
American Guarantee & Liability Insurance
American Hardware Mutual Insurance Company
American Health and Life Insurance
American Home Assurance Company
American Income Life Insurance Company
American Indemnity Company
American Insurance Company
American Intern Insurance Company
American Intern Insurance Company of California
American Intern Insurance Company of Delaware
American Intern Insurance Company of New Jersey
American Intern Life Assurance Company of New York
American Intern Pacific Insurance Company
American Intern South Insurance Company
American Intern Specialty Insurance
American Investors Life Insurance Company
American Investors Life Insurance Company
American Life & Accident Insurance Company
American Life Insurance Company of New York
American Maturity Life Insurance Company
American Mayflower Life Insurance New York
American Merchants Casualty Company
American Modern Home Insurance Company
American Modern Life Insurance Company
American Modern Lloyds Insurance
American National Insurance Company
American National Life Insurance Texas
American Pacific Insurance Company, Inc.

American Partners Life Insurance Company
American Premier Insurance Company
American Select Insurance Company
American Service Insurance Company
American Skandia Life Assurance
American Southern Home Insurance
American Standard Insurance Company of WI
American Standard Lloyds
American States Insurance Company of Texas
American States Insurance Company
American States Life Insurance Company
American States Preferred Insurance
American United Life Insurance Company
American Western Home Insurance Company
American Zurich Insurance Company
Americo Financial Life & Annuity
Americom Life & Annuity Insurance
AmerUs Life Insurance Company
AmerUs Life Insurance Company
Amex Assurance Company
Amica Lloyd's of Texas
Amica Mutual Insurance Company
Annuity Investors Life Insurance Company
Anthem Health Plans of Virginia
Anthem Insurance Companies Inc
Anthem Life Insurance Company
Associated Indemnity Corporation
Associates Insurance Company
Associates Lloyds Insurance Company
Assurance Company of America
Atlanta Casualty Company
Atlanta Specialty Insurance Company
Atlantic Indemnity Company
Atlantic Insurance Company
Atlantic Security Insurance Company
Audubon Indemnity Company
Audubon Insurance Company
Auto Insurance Company of Hartford
Avomark Insurance Company
Bankers Life and Casualty Company
Bankers Life Insurance Company of Illinois
Bankers Life Insurance Company of New York
Bankers Life Insurance Company of New York
Bankers National Life Insurance Company
Beneficial Life Insurance Company
Berkshire Mutual Insurance Company
Birmingham Fire Insurance Company of Pennsylvania
Blue Ridge Indemnity Company
Blue Ridge Insurance Company
Bridgefield Casualty Insurance Company
Bridgefield Employers Insurance Company
Bristol West Casualty Insurance Company
Bristol West Insurance Company
Business Men's Assurance Company
C M Life Insurance Company
CalFarm Insurance Company
California Casualty & Fire Insurance Company
California Casualty Compensation Insurance Company
California Casualty General Insurance Company
California Casualty Indemnity Exchange
California Casualty Insurance Company
Camden Fire Insurance Assoc

Canada Life Assurance Company USB
Canada Life Insurance Company of America
Canada Life Insurance Company of New York
Central Reserve Life
Charter Indemnity Company
Charter Oak Fire Insurance Company
Cherokee National Life Insurance Company
Chicago Insurance Company
China America Insurance Company Ltd.
CIM Insurance Corporation
Cincinnati Casualty Company
Cincinnati Indemnity Company
Cincinnati Insurance Company
Cincinnati Life Insurance Company
Citizens Insurance Company of America
Citizens Insurance Company of Illinois
Citizens Insurance Company of the Midwest
Citizens Insurance Company of Ohio
Clarendon America Insurance Company
Clarendon National Insurance Company
Clarendon Select Insurance Company
Clarica Life Insurance Company-United States
CNA Group Life Assurance Company
Coast National Insurance Company
Colonial American Casualty & Surety
Colonial County Mutual Insurance Company
Colonial Life & Accident Insurance
Colonial Penn Life Insurance
Colorado Bankers Life Insurance Company
Colorado Casualty Insurance Company
Columbia Casualty Company
Columbine Life Insurance Company
Columbus Life Insurance Company
Combined Insurance Company of America
Combined Life Insurance Company of New York
Commerce and Industry Insurance Company
Commercial Guaranty Insurance Company
Connecticut Indemnity Company
Conseco Annuity Assurance Company
Conseco Health Insurance Company
Conseco Life Insurance Company of Texas
Conseco Life Insurance of New York
Conseco Life Insurance Company
Conseco Medical Insurance Company
Conseco Senior Health Insurance Company
Conseco Variable Insurance Company
Consolidated Insurance Company
Continental Assurance Company
Continental Casualty Company
Continental General Insurance Company
Continental Lloyd's Insurance Company
Continental National Indemnity Company
Cotton States Life Insurance Company
Cotton States Mutual Insurance Company
COUNTRY Casualty Insurance Company
COUNTRY Investors Life Assurance
COUNTRY Life Insurance Company
COUNTRY Mutual Insurance Company
COUNTRY Preferred Insurance Company
Coventry Insurance Company
CUNA Mutual Insurance Society
CUNA Mutual Life Insurance Company

Dairyland Insurance Company
Dairyland County Mutual Insurance Company of Texas
Dakota Fire Insurance Company
Depositors Insurance Company
Direct Insurance Company
Dixie National Life Insurance Company
Educators Life Insurance Company
EMC Property & Casualty Company
EMC Reinsurance Company
EMCASCO Insurance Company
Empire Fidelity Investments Life
Empire Fire & Marine Inc Company
Empire General Life Assurance
Empire Indemnity Insurance Company
Employers Fire Insurance Company
Employers Insurance Company of Wausau
Employers Mutual Casualty Company
Equitable Life Insurance Company of Iowa
Equity Insurance Company
Erie Family Life Insurance Company
Erie Insurance Company
Erie Insurance Company of New York
Erie Insurance Exchange
Erie Insurance Property & Casualty Company
Excelsior Insurance Company
Farm and City Insurance Company
Farmers Casualty Insurance Company
Farmington Casualty Company
Farmland Mutual Insurance Company
Federal Home Life Insurance Company
Fidelity & Guaranty Life of New York
Fidelity and Deposit Company of Maryland
Fidelity and Guaranty Life Insurance
Fidelity Investments Life Insurance
Financial Assurance Life Insurance
Financial Benefit Life Insurance Company
Financial Benefit Life Insurance Company
Financial Indemnity Company
Fire & Casualty Insurance Company of Connecticut
Fireman's Fund Count Mutual Insurance Company
Fireman's Fund Indemnity Corporation
Fireman's Fund Insurance Company of Georgia
Fireman's Fund Insurance Company of Hawaii
Fireman's Fund Insurance Company of Louisiana
Fireman's Fund Insurance Company of Missouri
Fireman's Fund Insurance Company of Nebraska
Fireman's Fund Insurance Company of Ohio
Fireman's Fund Insurance Company of Texas
Fireman's Fund Insurance Company of Wisconsin
Fireman's Fund Insurance Company
First Allmerica Financial Life Insurance Company
First Colony Life Insurance Company
First Fire & Casualty Insurance of Hawaii
First Floridian Auto & Home
First Great-West Life & Annuity Insurance Company
First Indemnity Insurance of Hawaii
First Insurance Company of Hawaii
First Liberty Insurance Corporation
First National Insurance Company of America
First Penn-Pacific Life Insurance Company

First SAFECO National Life of New York
First Security Benefit Life & Annuity, New York
First Security Insurance of Hawaii
First SunAmerican Life Insurance Company
First Trenton Indemnity Company
First United American Life Insurance
First Unum Life Insurance Company
First Variable Life Insurance Company
Flagship City Insurance Company
Fort Dearborn Life Insurance Company
G.U.I.C. Insurance Company
Galway Insurance Company
Garden State Life Insurance Company
GE Capital Life Assurance Company of New York
GEICO Casualty Company
GEICO General Insurance Company
GEICO Indemnity Company
GE Life & Annuity Assurance
General Casualty Company of Illinois
General Casualty Company of Wisconsin
General Electric Capital Assurance
General Insurance Company of America
Globe American Casualty Company
Globe Indemnity Company
Globe Life and Accident Insurance Company
GMAC Direct Insurance Company
GMAC Insurance Company Online
Golden American Life Insurance Company
Golden Eagle Insurance Corp
Golden Rule Insurance Company
Government Employees Insurance Company
Granite State Insurance Company
Great Amer Contemporary Insurance Company
Great American Alliance Insurance Company
Great American Assurance Company
Great American E&S Insurance Company
Great American Insurance Company
Great American Insurance Company, New York
Great American Life Assurance of Puerto Rico
Great American Life Insurance Company
Great American Lloyds Insurance Company
Great American Security Insurance Company
Great American Spirit Insurance Company
Great Southern Life Insurance Company
Great Texas County Mutual Insurance Company
Great-West Life & Annuity
Great-West Life Assurance Company, United States
Grocers Insurance Company
Guaranty National Insurance Company of Connecticut
Guaranty National Insurance Company
Gulf Group Lloyds
Gulf Insurance Company
Gulf Underwriters Insurance Company
Gulfco Life Insurance Company
Hamilton Mutual Insurance Company
Hanover American Insurance Company
Hanover Insurance Company
Harbor Specialty Insurance Company
Harleysville Mutual Insurance Company
Harleysville Preferred Insurance Company

Harleysville Lake States Insurance Company
Harleysville Worcester Insurance Company
Harleysville Insurance Company
Harleysville Insurance Company of NY
Harleysville Pennland Insurance Company
Harleysville Insurance Company of NJ
Harleysville-Garden State Insurance Company
Harleysville Insurance Company of Ohio
Harleysville-Atlantic Insurance Company
Hart Life Insurance Company
Hartford Accident & Indemnity Company
Hartford Casualty Insurance Company
Hartford Fire Insurance Company
Hartford Insurance Company of Midwest
Hartford Insurance Company of Southeast
Hartford Insurance Company of Illinois
Hartford International Life Reassurance
Hartford Life & Accident Insurance
Hartford Life and Annuity Insurance
Hartford Life Insurance Company
Hartford Lloyds Insurance Company
Hartford Underwriters Insurance Company
Hawkeye-Security Insurance Company
Home State County Mutual Insurance Company
Homeland Central Insurance Company
Homeland Insurance Company of New York
Hoosier Insurance Company
Horace Mann Insurance Company
Horace Mann Life Insurance Company
Horace Mann Lloyds
Horace Mann Property & Casualty Insurance Company
IDS Life Insurance Company
IDS Life Insurance Company of NY
IDS Property Casualty Insurance Company
Illinois Annuity and Insurance Company
Illinois Annuity and Insurance Company
Illinois EMCASCO Insurance Company
Illinois National Insurance Company
Indiana Insurance Company
Indianapolis Life Insurance Company
Indianapolis Life Insurance Company
Infinity Insurance Company
Infinity National Insurance Company
Infinity Select Insurance Company
ING Insurance Company of America
ING Life Insurance Company of America
ING Life Insurance and Annuity
Insurance Company of the State of Pennsylvania
Insurance Corp of Hannover
Insurance Investors Life
Integon Casualty Insurance Company
Integon General Insurance Corporation
Integon Indemnity Corporation
Integon National Insurance Company
Integon Preferred Insurance Company
Integon Specialty Insurance Company
Integrity Life Insurance Company
Interstate Fire & Casualty Company
Interstate Indemnity Company
Investors Partner Life Insurance Company
Jefferson Insurance Company
Jefferson Pilot Financial Insurance Company

Jefferson-Pilot Life America Insurance Company
Jefferson-Pilot Life Insurance Company
John Hancock Life Insurance
John Hancock Variable Life
Kansas City Fire & Marine
Kansas City Life Insurance Company
Kemper Auto & Home Insurance Company
Keyport Life Insurance Company
Knights of Columbus
Lafayette Insurance Company
Lafayette Life Insurance Company
Landmark American Insurance Company
Landmark Insurance Company
Leader Insurance Company
Leader Preferred Insurance Company
Lexington Insurance Company
Liberty County Mutual Insurance Company
Liberty Insurance Company of America
Liberty Insurance Corporation
Liberty Insurance Underwriters
Liberty Life Assurance of Boston
Liberty Lloyds of Texas Insurance Company
Liberty Mutual Fire Insurance Company
Liberty Mutual Insurance Company
Liberty National Life Insurance Company
Liberty Northwest Insurance Corp
Liberty Personal Insurance Company
Liberty Surplus Insurance Corp
Life Insurance Company of Georgia
Life Insurance Company of Southwest
Life Investors Insurance Company of America
Lincoln General Insurance Company
Lincoln Life & Annuity of New York
Lincoln National Life Insurance Company
LM Insurance Corporation
Maine Bonding & Casualty Company
Mainland Insurance Company
Manufacturers Life Insurance (USA)
Maryland Casualty Company
Maryland Insurance Company
Maryland Lloyds
Massachusetts Bay Insurance Company
Massachusetts Homeland Insurance Company
Massachusetts Mutual Life Insurance
MassWest Insurance Company, Inc.
MEMBERS Life Insurance Company
Mendakota Insurance Company
Mendota Insurance Company
Merchants & Businessmen's Mutual
Meridian Citizens Mutual Insurance
Meridian Security Insurance Company
Merrill Lynch Life Insurance Company
MIC General Insurance Corporation
MIC Property & Casualty Insurance Corp
MICO Insurance Company
Mid-American Fire & Casualty Company
Mid-America Insurance Company
Mid-Continent Casualty Company
Mid-Continent Insurance Company (OK)
Middlesex Insurance Company
Midland National Life Insurance Company
Mid-Plains Insurance Company
Midway Insurance Company of Illinois
Midwestern Indemnity Company
Midwestern United Life Insurance Company

Milbank Insurance Company
Milwaukee Casualty Insurance Company
Milwaukee Insurance Company
Milwaukee Safeguard Insurance Company
MIMLIC Life Insurance Company
Minnesota Insurance Company
Minnesota Life Insurance Company
ML Life Insurance Company of New York
MML Bay State Life Insurance Company
Modern Life Insurance Company of Arizona
Modern Woodmen of America
Montgomery Indemnity Company
Montgomery Mutual Insurance Company
Montgomery Ward Insurance Company
Monticello Insurance Company
Monumental Life Insurance Company
Motorists Mutual Insurance Company
Motors Insurance Corporation
Mountain Laurel Assurance Company
Mutual Services Casualty Insurance Company
National Alliance Insurance Company
National Benefit Life Insurance Company
National Casualty Company
National Continental Insurance Company
National Farmers Union Life
National Fire Insurance Hartford
National General Assurance Company
National General Insurance Company
National Income Life Insurance
National Insurance Association
National Integrity Life Insurance Company
National Interstate Insurance Company
National Interstate Insurance Company, Hawaii
National Life Insurance Company
National Standard Insurance Company
National Surety Corporation
National Union Fire Insurance Company, Pennsylvania
National Union Fire Insurance of Louisiana
NationalCare Insurance Company
Nationwide Affinity Insurance Company of America
Nationwide Agribusiness Insurance Company
Nationwide Assurance Company
Nationwide General Insurance Company
Nationwide Indemnity Company
Nationwide Insurance Company of America
Nationwide Insurance Company of Florida
Nationwide Life & Annuity of America
Nationwide Life & Annuity Insurance
Nationwide Life Insurance Company
Nationwide Life Insurance Company of America
Nationwide Life Insurance Company of Delaware
Nationwide Lloyds
Nationwide Mutual Fire Insurance Company
Nationwide Mutual Insurance Company
Nationwide Property & Casualty Insurance Company
Netherlands Insurance Company
New Hampshire Indemnity Company
New Hampshire Insurance Company
New Jersey Indemnity Insurance Company
New Jersey Manufacturers Insurance
New Jersey Re-Insurance Company
New South Insurance Company
North American Company for Life and Health

North American Life & Health of New York
North Pacific Insurance Company
Northern Assurance Company of America
Northern Insurance Company of New York
Northfield Insurance Company
Northland Casualty Company
Northland Insurance Company
Northstar Life Insurance Company
Northwestern Long Term Care
Northwestern Mutual Life Insurance
Nutmeg Insurance Company
Nutmeg Life Insurance Company
Ohio Casualty Insurance Company
Ohio Casualty of New Jersey
Ohio Farmers Insurance Company
Ohio National Life Assurance Corporation
Ohio National Life Insurance Company
Ohio Security Insurance Company
Ohio State Life Insurance Company
Oklahoma Surety Company
Old American Insurance Company
Old Standard Life Insurance Company
Old West Annuity & Life Insurance Company
Omni Indemnity Company
Omni Insurance Company
Omnia Life Insurance Company
One Beacon America Insurance Company
OneBeacon Insurance Company
OneBeacon Lloyd's of Texas
OneBeacon Midwest Insurance Company
Oregon Automobile Insurance Company
Pacific Insurance Company, Ltd.
Pacific Life & Accident Insurance Company
Pacific Life & Annuity Company
Pacific Life Insurance Company
Parkway Insurance Company
Patriot General Insurance Company
Paul Revere Life Insurance Company
Peak Property & Casualty Insurance Corporation
Peerless Indemnity Insurance Company
Peerless Insurance Company
Penn Insurance and Annuity Company
Penn Mutual Life Insurance Company
Pennsylvania General Insurance Company
Pension Life Insurance of America
Peoples Benefit Life Insurance Company
PG Insurance Company of New York
PHL Variable Insurance Company
Phoenix Insurance Company
Phoenix Life and Annuity Company
Phoenix Life Insurance Company
Physicians Life Insurance Company
Physicians Mutual Insurance Company
Pioneer Life Insurance Company
Pioneer Mutual Life Insurance Company
Potomac Insurance Company of Illinois
Premier Insurance Company of Massachusetts
Primerica Life Insurance Company
Professional Insurance Company
Progressive American Insurance Company
Progressive Auto Pro Insurance Company
Progressive Bayside Insurance Company
Progressive Casualty Insurance Company
Progressive Classic Insurance Company

Progressive consumers Insurance Company
Progressive County Mutual Insurance Company
Progressive Express Insurance Company
Progressive Gulf Insurance Company
Progressive Halcyon Insurance Company
Progressive Hawaii Insurance Company
Progressive Home Insurance Company
Progressive Home Underwriters Insurance Company
Progressive Marathon Insurance Company
Progressive Max Insurance Company
Progressive Michigan Insurance Company
Progressive Mountain Insurance Company
Progressive Northeastern Insurance Company
Progressive Northern Insurance Company
Progressive Northwestern Insurance Company
Progressive Preferred Insurance Company
Progressive Premier Insurance Company of IL
Progressive Paloverde Insurance Company
Progressive Security Insurance Company
Progressive Southeastern Insurance Company
Progressive Specialty Insurance Company
Progressive Universal Insurance Company of IL
Progressive West Insurance Company
Property & Casualty Insurance Company of Hartford
Protective Life & Annuity Insurance
Protective Life Insurance Company
Protective Life Insurance Company of Ohio
Protective Life Insurance of Kentucky
Provident Life and Accident
Provident Life and Casualty
Pruco Life Insurance Company
Pruco Life Insurance Company of New Jersey
Prudential Healthcare of America
Prudential Insurance Company of America
Prudential Life Insurance Company of Arizona
Prudential Select Life of America
Prudential Uniformed Services
Reassure America Life Insurance Company
Red Oak Insurance Company
Redland Insurance Company
Regal Insurance Company
Regent Insurance Company
Reliable Life Insurance Company
ReliaStar Life Insurance Company of New York
ReliaStar Life Insurance Company
Republic Indemnity Company of California
Reserve National Insurance Company
Royal Indemnity Company
Royal Insurance Company of America
Royal Surplus Lines Insurance Company
SAFECO Insurance Company of America
SAFECO Insurance Company of Illinois
SAFECO Insurance Company of Oregon
SAFECO Life Insurance Company
Safeco Life Insurance Company of Indiana
SAFECO Lloyds Insurance Company
SAFECO National Insurance Company
SAFECO National Life Insurance Company
Safeguard Insurance Company
San Diego Insurance Company
Scottsdale Indemnity Company

Scottsdale Insurance Company
Scottsdale Surplus Lines Insurance
Securian Life Insurance Company
Security Benefit Life Insurance Company
Security Insurance Company of Hartford
Security Life of Denver Insurance Company
Security National Insurance Company
Security National Insurance Company
Security-Connecticut Life Insurance
Select Insurance Company
Selective Insurance Company of America
Selective Insurance Company of New York
Selective Insurance Company of South Carolina
Selective Insurance Company of the Southeast
Selective Way Insurance Company
Sentinel Insurance Company Ltd.
Sentry Casualty Company
Sentry Insurance a Mutual Company
Sentry Life Insurance Company
Sentry Life of New York
Sentry Lloyds of Texas
Sentry Select Insurance Company
Servus Life Insurance Company
Shield Insurance Company
Shelter General Insurance Company
Shelter Life Insurance Company
Shelter Mutual Insurance Company
Shenandoah Life Insurance Company
Southern Farm Bureau Life Insurance Company
Southern Farm Bureau Life Insurance Company
Southern United Fire Insurance Company
Southland Life Insurance Company
Southwestern Life Insurance Company
Specialty Risk Insurance Company
Standard Fire Insurance Company
Standard Life and Accident Insurance
Standard Life Insurance Company of Indiana
State and County Mutual Fire
State Auto Insurance Company of Ohio
State Auto Insurance Company of Wisconsin
State Auto National Insurance Company
State Auto Property & Casualty Insurance Company
State Automobile Mutual Insurance Company
State Farm Annuity and Life Insurance Company
State Farm County Mutual Insurance Company of Texas
State Farm Fire and Casualty Company
State Farm Florida Insurance Company
State Farm General Insurance Company
State Farm Indemnity Company
State Farm Life and Accident Assurance Company
State Farm Life Insurance Company
State Farm Lloyds
State Farm Mutual Automobile Insurance Company
State National Insurance Company, Inc
State National Spec Insurance Company
Steadfast Insurance Company
Sterling Life Insurance Company
Stonebridge Life Insurance Company
Sun Life Assurance Company of Canada (US)
Sun Life Assurance of Canada USB
Sun Life Insurance & Annuity of New York
SunAmerican Life Insurance Company

Sunset Life Insurance Company of America
Swiss Re Life & Health America
Teachers Insurance Company
Texas General Indemnity Company
Thrivent Financial Lutherans
TICO Insurance Company
Transamerica Assurance Company
Transamerica Financial Life
Transamerica Life Insurance & Annuity Company
Transamerica Life Insurance Company
Transamerica Occidental Life
Transcontinental Insurance Company
Transport Insurance Company
Transportation Insurance Company
Travelers Company Insurance Company
Travelers Casualty & Surety Company
Travelers Casualty & Surety Company of Illinois
Travelers Casualty & Surety of America
Travelers Casualty Company of Connecticut
Travelers Commercial Casualty Company
Travelers Commercial Insurance
Travelers Excess & Surplus Lines
Travelers Home and Marine
Travelers Indemnity Company of America
Travelers Indemnity Company of Connecticut
Travelers Indemnity Company of Illinois
Travelers Indemnity Company
Travelers Insurance Company (Life Department)
Travelers Life and Annuity
Travelers Lloyds Insurance Company
Travelers Lloyds of Texas Insurance
Travelers Personal Security
Travelers Property Casualty Insurance Company
Travelers Property Casualty Insurance Company of Illinois
Trinity Lloyd's Insurance Company
Trinity Universal Insurance Company
Trinity Universal Insurance Company of Kansas
Trumbull Insurance Company
Twin City Fire Insurance Company
Unified Life Insurance Company
Union Central Life Insurance Company
Union Fidelity Life Insurance Company
Union Insurance Company of Providence
Union National Life Insurance Company
Unisun Insurance Company
United American Insurance Company
United Casualty Insurance Company of America
United Fidelity Life Insurance Company
United Financial Casualty Company
United Fire & Casualty Company
United Fire & Indemnity Company
United Fire Lloyds (Texas only)
United Insurance Company of America
United Investors Life Insurance Company
United Life & Annuity Insurance Company
United Life Insurance Company
U.S. Security Insurance Company
United Teacher Associates Insurance
Unitrin Auto & Home Insurance Company
Unitrin County Mutual Insurance Company
Unitrin Direct Insurance Company

Unitrin Direct Property & Casualty Company
Unitrin Preferred Insurance Company
Universal Casualty Company
Unum Life Insurance Company of America
USG Annuity & Life Company
Valiant Insurance Company
Valley Forge Insurance Company
Valley Forge Life Insurance Company
Valley Insurance Company
Valley Property & Casualty Insurance
Variable Annuity Life Insurance Company
Veterans Life Insurance Company
Veterinary Pet Insurance Company
Viking County Mutual Insurance Company
Viking Insurance Company of Wisconsin
Vintage Insurance Company
Washington National Insurance Company
Wausau Business Insurance Company
Wausau General Insurance Company
Wausau Underwriters Insurance Company
West American Insurance Company
West Coast Life Insurance Company
Western and Southern Life Insurance
Western Heritage Insurance Company
Western Reserve Assurance of Ohio
Western Southern Life Assurance
Western States Insurance Company
Western United Life Assurance Company
Westfield Insurance Company
Westfield National Insurance Company
Windsor Insurance Company
Woodmen of the World Life Society
Worldwide Casualty Insurance Company
Worldwide Direct Auto Insurance Company
Worldwide Insurance Company
York Insurance Company of Maine
Zurich American Insurance Company of Illinois
Zurich American Insurance Company

Insurance groups exempted from examination

1) Allstate Insurance Group
2) Automobile Club of America
3) Balboa Life & Casualty Group
4) CBD Holdings Ltd.
5) Central Services Group
6) Chubb Group of Insurance Cos
7) Employers Re Group
8) Farmers Insurance Group
9) Guardian Life
10) Jackson National Group
11) Legal & General Insurance Group
12) Main Street America Group
13) Mercury General Group
14) Metropolitan Life & Affiliated
15) MONY Life Insurance Company
16) Munich American Reassurance Co
17) Mutual of Omaha Insurance Company
18).New York Life Group
19).PEMCO Insurance Companies
20) Presidential Life Corp
21) Principal Financial Group
22) St Paul Companies
23) TIAA Group
24) USAA Group
25) Vesta Insurance Group Inc.

Insurance groups that refused to participate

The following insurance groups refused to cooperate with the examination program: Auto-Owners Insurance Group; Pekin Insurance; and Grange Mutual Casualty Group. The DC Commissioner was therefore unable to render a report or opinion as to whether these companies are in compliance with the privacy requirements of the GLB Act or the NAIC model law and regulations.

ATTACHMENT B
THEMES

In addition to findings and observations, the consultants identified a number of themes related to insurers' information handling practices and procedures to ensure customers are granted the rights provided to them in the model laws and regulations. These themes are presented in the chart below. The themes are grouped by privacy elements and safeguarding elements, and categories of themes have been developed within these groups to differentiate between positive and negative themes, as well as items of interest that do not have either a positive or negative impact.

THEMES

THEME	IMPACT/RELEVANCE
Privacy Themes	
Privacy Notice Delivery Approximately 20% of companies automatically print the privacy notices along with the insurance policies and send the notices out with the policy. [NAIC 2000 Model]	This systemic control helps ensure that the customer receives the privacy notice in a timely manner because it reduces the potential for human error in delivering the privacy notice. This does, however, result in the customer not receiving the notice during the application process, which could be considered the initiation of the customer relationship.
Simplified and Short-form Notices Approximately 90% of companies do not provide customers with a simplified or short-form notice. Companies have the option of providing such a notice if they do not wish to reserve the right to disclose nonpublic personal financial information about customers except as authorized under sections 15 and 16 of the NAIC 2000 Model. Sections 15 and 16 relate to the companies' rights to share information with service providers or as necessary according to the law, without offering customers an opt-out. If this is the only sharing a company wishes to do, then they can simply state that ~~in~~ fact. [NAIC 2000 Model]	Even though many companies do not share outside of the exceptions outlined in sections 15 and 16, they choose to provide the more comprehensive long-form notice to their customers. In this notice, they more thoroughly describe how information is used and shared, providing examples of sharing relationships. The customer is therefore provided with a more informative notice than is required by the law.

THEME	IMPACT/RELEVANCE
Authorization Forms Approximately 90% of companies' sharing practices related to nonpublic personal health information are within the exceptions outlined in section 17 of the NAIC 2000 Model. However, many companies still have developed authorization forms and have policies related to when these authorization forms should be used. The exceptions outlined in section 17 state that no authorization is required to share nonpublic personal health information if such sharing is done within the context of certain insurance functions. Therefore, most companies do not require authorization forms for use in facilitating a request for a customer's nonpublic personal health information. [NAIC 2000 Model]	Many companies appear to be taking a conservative approach to restricting access to their customers' non-public personal health information.
Delivery of Notice of Insurance Information Practices All of the companies reviewed that write business in NAIC 1982 Model states provide the Notice of Insurance Information Practices at the time of collection of the personal information since the notice is embedded in the application form. The customer also signs these forms acknowledging that they have read the information, including the Notice of Insurance Information Practices. In addition to information on the collection and use of nonpublic personal information, these notices include disclosure on a customer's rights to access, correct, amend and delete such information. [NAIC 1982 Model]	This enables the customer to understand his or her privacy rights and rights to access and correct their personal information during the application process.

THEME	IMPACT/RELEVANCE
Content of Notice of Insurance Information Practices Approximately 50% of companies reviewed that write business in NAIC 1982 Model states have notices that are missing elements outlined in sections 8 and 9 of the NAIC 1982 Model. The rights outlined in sections 8 and 9 relate to the customers' rights to access, correct, amend and delete their personal information. Many companies did not feel that all the detailed elements related to these rights should be disclosed and that, if disclosed, the notices would be lengthy and somewhat confusing to customers. [NAIC 1982 Model]	There is an overall variation of practice in the extent of disclosure related to the customers' rights to access, correct, amend, and delete their personal information as outlined in sections 8 and 9 of the NAIC 1982 Model. Guidance may be necessary related to the extent of disclosure expected of companies to help ensure consistency in this area across the industry.
Policies and Procedures Related to Customers' Rights to Access, Correct, Amend, and Delete Their Personal Information While all companies insist that customers' rights to access, correct, amend and delete their information, as outlined in sections 8 and 9 of the NAIC 1982 Model are granted to them, approximately 60% of companies reviewed that write business in NAIC 1982 Model states did not have comprehensive internal policies and procedures related to these customer rights. [NAIC 1982 Model]	While there is no requirement in the NAIC 1982 Model for a company to have formally documented policies and procedures related to customers' rights to access, correct, amend and delete their personal information, without evidence of policies and procedures, or internal training, it is difficult to ensure that employees understand how to handle such customer requests. There is a risk that such customer rights would not be appropriately granted to them.

THEME	IMPACT/RELEVANCE
Differing Privacy Notices for Property & Casualty and Life & Annuity Approximately 90% of the groups that wrote both Property & Casualty and Life & Annuity business used different notices for the two lines of business. This is due to the fact that Life & Annuity lines of business have the additional requirement to comply with HIPAA regulations in addition to the GLB Act; while Property & Casualty lines of business need only comply with the GLB Act. [Item of interest]	In this way policyholders are provided with only the information that is relevant to their policy; however, if a policyholder has both types of policies, they may receive multiple notices which might be confusing to them.
Sharing with Third Parties Approximately 90% of companies do not appear to share information with third-parties outside of exceptions 14, 15 and 16 in the NAIC 2000 Model. These exceptions relate to the ability to share with service providers, joint marketers and as necessary according to the law. [Item of interest]	For this reason, most companies do not offer an opt-out to the customer to prevent sharing.
Online Delivery of Privacy Notices No companies accept applications for products over the Web. As a result, no companies required consumers to acknowledge receipt of the privacy notice electronically. The Model Law states that an acceptable method for delivering a notice when a customer conducts transactions electronically is to post the notice on the Web site and require the customer to acknowledge receipt of the notice prior to obtaining a particular insurance product or service. [Item of interest]	All the companies appear to prefer a traditional method of conducting business, among other reasons, due to the desire for hard copy documentation to be retained by both the company and the customer.

THEME	IMPACT/RELEVANCE
Safeguarding Themes	
Risk Assessment Process Approximately 10% of companies do not either: (1) complete risk assessments for customer information; (2) update the risk assessment regularly; or (3) have a formalized risk assessment process	This systemic control helps to ensure risks and threats to customer information are identified and mitigated. This includes: • Identification of all customer information within the organization. • Identification of the reasonably anticipated threats to that information. • Identification of the controls to mitigate the threats.
External Data Transmissions Less than 10% of companies transmit customer information out of their environment in an unprotected manner.	This systemic control helps ensure that the customer information stays protected at all times. This includes: • Policies requiring the listing of all file transmissions that are scheduled to occur on a regular basis, indicating the third party to whom the transmission is going, the purpose of the transmission, and the customer information contained within the transmission. • Policies designed to ensure data downloads or transmissions are appropriate, the business need is understood, the sensitivity of the information is communicated, and safeguards are in place. • Policies, procedures, or controls to protect the security and integrity of customer information that is being transmitted to third parties. • Controls to limit the employees who are authorized to perform or modify transmissions of customer information. • Controls that are in place to protect external transmissions of customer information from unauthorized access attempts (e.g., encryption, frame relay).

THEME	IMPACT/RELEVANCE
Protection of Customer Information Integrity Approximately 10% of companies use real customer information for system testing and do not control changes to systems containing customer information.	An insufficient number of policies have been developed and implemented surrounding "live production data". Documentation needs to be developed on areas where "live production" customer information can be used in a test environment along with a business case for the need to use "live production" customer information. In addition, customer information systems change processes do not have sufficient impact analysis and review.
Evaluating Service Providers Approximately 10% of companies are not using a controlled process to verify the security program and controls at service providers that are handling protected information on behalf of the company.	Companies do not currently have a process to evaluate whether service providers have taken the appropriate steps to safeguard non-public personal information nor do they have the contract language in place to support this evaluation.
Security Awareness and Response Approximately 10% of companies are not training their employees in general security principles, including what their responsibilities are to protect customer information as well as knowing how to respond when a breach of security occurs.	Companies have no formal policies or procedures to respond to a security breach or incident. In addition, lack of a formal security training program limits employee knowledge of their role in protection of customer information.
Remote Access Restrictions Approximately 20% of companies are not adequately controlling remote access to systems and information from employees and contractors who work outside of the company's offices and who require access to protected information.	The companies do not perform or did not provide documentation that they perform one or more of the following activities: • Review and monitor dial-up access granted to each user. • Restrict remote access to company-owned property. • Restrict access to time of day.

ATTACHMENT C

QUESTIONNAIRE

Please provide the name, title, and telephone number of the company contact person responsible for the answers to this set of questions using the file name "B1.Doc"

1) Does the company have a privacy notice that describes its information handling practices with respect to customer's nonpublic personal information? (Model 672 Section 5-7, Market Conduct Examination Standard - Standard 13)

Yes_____
No _____

Please provide copies of all privacy notices, including initial annual, short-form and simplified notices, if applicable, using file name "B1A.Doc"

2) Has the company sent a privacy notice to all existing customers as of July 1, 2001 and were the notices sent at a time and in a manner that would reasonably allow customers to have received the notices by this date? (Model 672 Sections 5&6, Market Conduct Examination Standard - Standard 13, Procedure G)

Yes_____
No _____

Please attach a brief explanation and any relevant documents using the file name "B1B.Doc"

3) Please explain how the company determined who all of their customers were, such as by performing an analysis defining customer and consumer status. (NAIC Model 672 Section 4 (F)&(I), Market Conduct Examination Standard - Standard 13, Procedure F)

Please attach a description/explanation and relevant documents using the file name "B1C.Doc"

4) What procedures has the company implemented to provide the initial privacy notice to customers and, if applicable, to consumers whose relationship began after July 1, 2001? (NAIC Model 672 Section 5 & NAIC Model 672 Section 6(B), Market Conduct Examination Standard - Standard 13, Procedure G)

Please attach an explanation and any relevant documents using the file name "B1D.Doc"

5) Please explain the procedure for providing privacy notices to customers on an annual basis? (e.g. at least once every 12 months or calendar year) (NAIC Model

672 Section 6(A), Market Conduct Examination Standard - Standard 13, Procedure G)

Please attach an explanation of the procedure and a copy of the annual privacy notice using the file name “B1E.Doc”

6) If applicable, please explain the procedure for providing revised notices to customers and, if applicable, to consumers. (Note this question applies only to substantive revisions to the privacy notice that will trigger a new mailing of the privacy notice) (NAIC Model 672 Section 9, NAIC Market Conduct Standard 13, Procedure F (4))

Please provide an explanation and attach a copy of any revised privacy notices using the file name “B1F.Doc”

7) Please explain how the notice was delivered in a manner that allows the customer to retain the notices or obtain them later in writing or, if the customer has agreed, electronically. (NAIC Model 672 Section 10(E), Market Conduct Examination Standard - Standard 13, Procedure K)

Please attach an explanation and/or any relevant documents using the file name “B1G.Doc”

8) What efforts did the company reasonably make to ensure that the format of all privacy notices meets the definition of “clear and conspicuous”? These efforts may include, but are not limited to:

- using everyday words
- using simple sentences; and
- avoiding technical language.

(NAIC Model 672 Section 4(B)(2), NAIC Market Conduct Standard 13, Procedure B).

Please attach an explanation and copies of the privacy notice in any formats in which it was delivered to customers and, if applicable, to consumers using the file name “B2A.Doc”

9) Are the privacy notices provided to customers and, if applicable, consumers an accurate representation of the company’s information handling practices? (Section 7 of NAIC Model 672, NAIC Market Conduct Standard 13, Procedure B)

Yes_____
No _____ B3A

10) Does the privacy notice address all of the required elements of a privacy notice as defined by Section 7 of the NAIC Model 672, including the identification

of the company and affiliates or subsidiaries, if applicable? (NAIC Market Conduct Standard 13, Procedure C)

Yes_____
No _____ B3B

11) Does the privacy notice include the categories of non-pub lie personal financial information that the company collects? (NAIC Model 672 Section 7(A)(1), NAIC Market Conduct Standard 13, Procedure C (2))

Yes_____
No _____ B3C

12) Does the privacy notice include the categories of non-public personal financial information that the company discloses, if applicable? (NAIC Model 672 Section 7(A)(2), NAIC Market Conduct Standard 13, Procedure C (3))

Yes_____
No _____
N/A _____ B3D

13) Does the privacy notice include the categories of affiliates and non-affiliated third parties to whom the company discloses non-public personal financial information, other than disclosures permitted under Section 15 and 16 of the NAIC model regulation, if applicable? (NAIC Model 672 Section 7(A)(3), NAIC Market Conduct Standard 13, Procedure C (4))

Yes_____
No _____
N/A _____ B3E

14) Does the privacy notice include the categories of non-public personal financial information about the company's former customers that the company discloses, and the categories of affiliates and non-affiliated third parties to whom the company discloses non-public personal financial information, other than disclosures permitted under Section 15 and 16 of the NAIC model regulation, if applicable? (NAIC Model 672 Section 7(A)(4), NAIC Market Conduct Standard 13 Procedure C (5))

Yes_____
No _____
N/A _____ B3F

15) If a company discloses non-public personal financial information to a non-affiliated third party under Section 14 of the NAIC model regulation, does the privacy notice include a separate description of the categories of information the company discloses and the categories of third parties with whom the company

has contracted? (NAIC Model 672 Section 7(A)(5), NAIC Market Conduct Standard 13 Procedure C (6))

Yes_____
No _____
N/A _____ B3G

16) Does the privacy notice include an explanation of the consumer' right to opt-out of the disclosure of non-public personal financial information to non-affiliated third parties, including the methods by which the consumer may exercise that right at any time, if applicable? (NAIC Model 672 Section 7(A)(6), NAIC Market Conduct Standard 13 Procedure C (7))

Yes_____
No _____
N/A _____ B3H

17) Does the privacy notice include any disclosures that the company may make under Section 603(d)(2)(A)(iii) of the Federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)). That is, notices regarding the ability to opt-out of disclosures of information among affiliates, other than transaction and experience information? (NAIC Model 672 Section 7(A)(7), NAIC Market Conduct Standard 13 Procedure C (8))

Yes_____
No _____ B3I

18) Does the privacy notice include the company's policies and practices with respect to protecting the confidentiality and security of non-public information? (NAIC Model 672 Section 7(A)(8), NAIC Market Conduct Standard 13 Procedure C (9))

Yes_____
No _____ B3J

19) Does the privacy notice include, if a company only discloses non-public personal financial information as authorized under Section 15 and 16 of the NAIC model regulation, a statement that at a minimum should indicate the company makes disclosures to other affiliated and non-affiliated third parties, as applicable, as permitted by state laws regarding privacy? (NAIC Model 672 Section 7(B), NAIC Market Conduct Standard 13 Procedure C (10))

Yes_____
No _____
N/A _____ B3K

20) Does the company use a simplified privacy notice? (NAIC Model 672 Section 7(C)(5), NAIC Market Conduct Standard 13 Procedure D)

Yes_____
No _____ B3L

If yes, please provide an explanation of the process the company used to determine that a simplified privacy notice was appropriate using the file name "B3M.Doc" (NAIC Model 672 Section 7(C)(5)).

21) Does the company use a short form privacy notice? (NAIC Model 672 Section 7(D), NAIC Market Conduct Standard 13 Procedure E)

Yes_____
No _____ B3N

Please provide an explanation regarding the process for providing a short form privacy notice to consumers. The explanation should include the description of how consumers may obtain a privacy notice and how the company determined that the notice met the requirements of "Clear and Conspicuous" using the file name "B3O.Doc". (NAIC Model 672 Section 7(D)).

22) What procedures has the company performed to verify the accuracy and content of the privacy notice? (NAIC Model 672 Section 5(A) and Section 6(A), NAIC Market Conduct Standard 13 Procedure B)

Yes_____
No _____
N/A _____

Please attach a description of the process and/or relevant sample documents using the file name "B3P.Doc"

23) Do the licensee's privacy notices include all necessary disclosures as determined by their review of information handling practices? (NAIC Model 672 Section 7, NAIC Market Conduct Standard 13 Procedure B)

Yes_____
No _____
N/A _____

Please provide copies of the privacy notice(s) delivered to customers and, if applicable, to consumers using the file name "B3Q.Doc"

Note: Questions 24-30 relate to compliance with the privacy aspects of the NAIC 1982 Insurance Information and Privacy Protection Act. Companies that are not licensed in any state that has this law in effect should respond with an N/A.

24) Does the licensee provide a Notice of Insurance Information Practices to applicants or policyholders in those states that have adopted the Insurance Information and Privacy Protection Model Act? (NAIC Insurance Information and Privacy Protection Model Act, Section 4, NAIC Market Conduct Standard 10)

Yes_____
No _____
N/A ____

Please provide copies of the privacy notice(s) delivered to applicants and policyholders using the file name "B3R.Doc"

25) Does the licensee provide the notice at the time of policy delivery when personal information is collected only from the applicant or public records? (NAIC insurance Information and Privacy Protection Model Act, Section 4(A)(1)(a), NAIC Market Conduct Standard 10)

Yes_____
No _____
N/A ____

Please provide copies of any relevant policies and the index evidencing the existence of relevant procedures using the file name "B3S.Doc"

26) Does the licensee provide the notice at the time the collection of personal information is initiated when personal information is collected from a source other than from the applicant or public records? (NAIC Insurance Information and Privacy Protection Model Act, Section 4(A)(1)(b), NAIC Market Conduct Standard 10)

Yes_____
No _____
N/A _____

Please provide copies of any relevant policies and the index evidencing the existence of relevant procedures using the file name "B3T.Doc"

27) Does the licensee provide a notice prior to policy renewal when personal information is collected from a source other than from the applicant or public records and a privacy notice has not been provided in the previous twenty-four months? (NAIC Insurance Information and Privacy Protection Model Act, Section 4(A)(2), NAIC Market Conduct Standard 10)

Yes_____
No _____
N/A _____

Provide copies of any relevant policies and the index evidencing the existence of relevant procedures using the file name “B3U.Doc”

28) Does the licensee’s Notice of Insurance Information Practices contain all of the required disclosures required by the Insurance Information and Privacy Protection Model Act? (NAIC Insurance information and Privacy Protection Model Act, Section 4(B), NAIC Market Conduct Standard 10)

Yes_____
No _____
N/A _____

Please provide copies of the privacy notice(s) delivered to applicants and policyholders using the file name “B3V.Doc”

29) Does the licensee provide access to recorded personal information? (NAIC Insurance Information and Privacy Protection Model Act, Section 8, NAIC Market Conduct Standard 11)

Yes_____
No _____
N/A _____

Please provide copies of any relevant policies that explain the individual’s access rights, how the individual may exercise these rights, and how the licensee responds to such requests, as well as the index evidencing the existence of relevant procedures, using the file name “B3W.Doc”

30) Does the licensee allow individuals to request that recorded personal information be corrected, amended, or deleted? (NAIC Insurance Information and Privacy Protection Model Act, Section 9, NAIC Market Conduct Standard 11)

Yes_____
No _____
N/A _____

Please provide copies of any relevant policies that explain the individual’s rights to request that personal information be corrected, amended, or deleted, how the individual may exercise these rights, and how the licensee responds to such requests, as well as the index evidencing the existence of relevant procedures, using the file name “B3X.Doc”

Policies and Procedures

31) Does the company use and disclose nonpublic personal financial information that it receives from a nonaffiliated financial institution in compliance with the NAIC model regulation? (NAIC Market Conduct Standard 15, Procedure B)

Yes_____
No _____

Please provide copies of any relevant policies and the index evidencing the existence of relevant procedures using the file name "C1A.Doc"

32) Does the company restrict the sharing of an account number, access number, or access code for a consumer's policy, brokerage account, or transaction account with any non-affiliated third party for use in telemarketing, direct mail marketing, or other marketing (i.e. electronic mail) to the consumer? (NAIC Model 672 Section 13, NAIC Market Conduct Standard 15, Procedure D)

Yes_____
No _____

Please attach an explanation and/or relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "C1B.Doc"

33) Does the company share nonpublic personal health information with affiliates or non-affiliated third parties for purposes that require an authorization? (NAIC Model 672 Sections 17 & 18, NAIC Market Conduct Standard 16)

Yes_____
No _____

Please provide an explanation of how the company determined whether an authorization was needed for sharing of health information and any relevant sample documents using the file name "C2A.Doc"

34) Has the licensee secured authorizations from its customers and consumers before disclosing their non-public personal health information to affiliates or non-affiliated third parties, except to the extent such disclosure is permitted under Section 1 7B of the NAIC Model Regulation? (NAIC Model 672 Section 17(B), NAIC Market Conduct Standard 16, Procedure A)

Yes_____
No _____

Please provide an explanation of the process for securing authorization using the file name "C2B.Doc". If no authorization is required based upon due diligence activities, note accordingly.

35) Does the licensee's authorization form include "all" of the elements required by Article V of the NAIC Model Regulation #672? The elements may include, but not necessarily be limited to, the following: (NAIC Model 672 Section 18, NAIC Market Conduct Standard 16, Procedure B)

- The identity of the consumer or customer who is subject of non-public personal health information.
- A general description of the types of non-public personal health information to be disclosed.
- A general description of the parties to whom the licensee discloses non-public personal health information.
- A general description of the purpose of the disclosure of the non-public personal health information.
- A general explanation of how the non-public personal health information will be used.
- The signature of the consumer or customer who is subject of the non-public personal health information or the individual who is legally empowered to grant disclosure authority and the date signed.
- A notice of the length of time for which the authorization is valid.
- A notice that the consumer or customer may revoke the authorization at any time, and an explanation of the procedure for making a revocation.

Yes_____
No _____
N/A _____

Please attach a sample copy of the authorization using the file name "C2C.Doc"

36) Did the licensee have policies and procedures in place so that non-public personal health information will not be disclosed unless a customer or consumer has authorized the disclosures? (NAIC Model 672 Section 17, NAIC Market Conduct Standard 16, Procedure A)

Yes_____
No _____

Please attach an explanation and/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "C2D.Doc"

37) How does the licensee ensure that non-public personal financial information is not disclosed outside the allowable exceptions without offering an opt-out? (NA1C Model 672 Section 11 (A)(1), NAIC Market Conduct Standard 14, Procedure A)

Yes_____
No _____

Please attach an explanation and/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "C3A.Doc"

38) For financial products or services offered via a website, are users required to acknowledge receipt of a privacy notice electronically prior to completing a purchase of a financial product or service? (NAIC Model 672 Section 10(B)(1)(c), NAIC Market Conduct Standard 13, Procedure J&K).

Note: If a licensee offers financial products and services through a website, but chooses to provide privacy notices in a paper format, please mark N/A and state this in the explanation.

Yes_____
No _____

Please provide an explanation describing how privacy notices are delivered in relation to products and services offered on web sites and please provide a URL link to pages in which a privacy notice must be acknowledged using the file name "C4A.Doc"

39) Has the licensee included privacy language in joint marketing or service provider agreements that prohibits the non-affiliated third party from disclosing or using the non-public personal information received from the company other than to carry out the purposes for which the information was disclosed to the third party, including use under an exception in sections 15 or 16 of NAIC Model 672? (NAIC Model 672 Section 14 (A)(1)(b), NAIC Market Conduct Standard 15 Procedure (A)(2) & Procedure C)

Yes_____
No _____

Please attach an explanation and a sample of the privacy language using the file name "C5A.Doc"

40) Has the licensee undertaken reasonable efforts to ensure that information obtained from non-affiliated third parties is not reused or re-disclosed for a purpose other than that which is allowed pursuant to NAIC Model 672? (NAIC Model 672 Section 14, NAIC Market Conduct Standard 15, Procedure B)

Yes_____
No _____

Please attach an explanation and/or any relevant policies using the file name "C6A.Doc"

41) Has the licensee developed a method for tracking, logging and analyzing privacy complaints? (NAIC Market Conduct Standard 12, Procedure E)

Yes_____
No _____

Please provide a description of the method, as well as copies of any privacy related complaints and an explanation of the resolution of such complaints, using the file name "C7A.Doc"

Customer Option Preferences

This section is applicable only to licensees who offer their customers or consumers an opportunity to opt-out of sharing with either third parties or affiliates. Licensees who do not offer an opt-out should answer only the first two questions of this section.

42) Does the licensee offer customers the opportunity to opt out of having certain information shared with non-affiliated third parties? (NAIC Model 672 Section 8(A), NAIC Market Conduct Standard 14, Procedure B)

Yes_____
No _____ D1A

43) Does the licensee offer customers the opportunity to restrict the sharing among its affiliated companies of information that is subject to the Fair Credit Reporting Act (FCRA)? (NAIC Model 672 Section 7(A)(7), NAIC Market Conduct Standard 13, Procedure C (8))

Yes_____
No _____
N/A _____ D1B

44) How does the licensee ensure that customers that have chosen to opt-out of such sharing have their information removed from customer lists prior to sharing? (Note: this question may be skipped if the licensee does not offer an opt-out for sharing of information with third parties).
(NAIC Market Conduct Standard C 14, Procedure A)

Please provide an explanation and/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "D2A.Doc"

45) What was the process for delivering the opt-out notice and did it take into consideration whether opt-out notices, if required, were delivered to customers

and, if applicable, consumers along with the initial and annual notice? (NAIC Model 672, Section 8(B), NAIC Market Conduct Standard 14, Procedure A)

Please provide a description of the process and any/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "D2B.Doc"

46) Are opt-out notices delivered in a form that makes them reasonably easy for customers and, if applicable, consumers to retain them? (NAIC Model 672, Section 8(B)&(C))

Please attach an explanation and/or any relevant documents, including opt-out notices, using the file name "D2C.Doc"

47) What was the process used for ensuring the delivery of opt-out notices (if separate from Privacy Notices)? (NAIC Model 672 Section 8) (Note: If opt-out notices were delivered with privacy notices please note that as your response.)

Please provide a description of the process and any relevant documents using the file name "D2D.Doc"

48) What is the process used by the licensee for customer's and, if applicable, consumers to report their opt-out elections and does the opt-out format contain items that include, but are not necessarily limited to, the following:

- Check-off boxes in a prominent position on the relevant forms with the opt-out notice? (NAIC Model 672 Section 8(A)(2)(b)(i))
- A reply form together with the opt-out notice? (NAIC Model 672 Section 8(A)(2)(b)(ii))
- An electronic means to opt-out, such as a form that can be sent via electronic mail or a process at the licensee's web site, if the consumer agrees to the electronic delivery of information? (NAIC Model 672 Section 8(A)(2)(b)(iii))
- A toll-free number that consumers may call to opt-out? (NAIC Model 672 Section 8(A)(2)(b)(iv))

Please provide an explanation and/or any relevant documents, including copies of all opt-out forms, using the file name "D3A.Doc"

49) What is the process used by the licensee for recording opt-out elections for joint policyholders in company systems and:

- Does the licensee's privacy notice address how opt-out elections for joint policies will be handled? (NA1C Model 672 Section 8(D)(1))
- Does an opt-out election by a joint customer apply to all associated accounts or are joint customers allowed to opt out separately? (NAIC Model 672 Section 8(D)(2))

- Does the licensee permit each joint customer to opt-out on behalf of other joint customers? (NAIC Model 672 Section 8(D)(3))

Please provide a description of the treatment of joint customers and/or any relevant documents using the file name "D3B.Doc"

50) What is the process used by the licensee for recording opt-out elections in the company's systems and does the process reasonably ensure that all opt-out elections will be recorded on a timely basis? (NAIC Model 672 Section 8(E))

Please provide an explanation and/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "D3C.Doc"

51) Are marketing lists or other customer lists that are shared outside of the allowable exceptions updated on a regular basis to ensure that opt-out elections are implemented within a reasonable period of time? (NAIC Model 672 Section 8(E))

Yes_____
No _____

Please attach an explanation and/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "D3D.Doc"

52) Has the licensee implemented policies, procedures and other controls to ensure that customers who have opted out do not have their information shared other than allowed under the exceptions pursuant to NAIC Model 672? (NAIC Market Conduct Standard 15, Procedure C)

Yes_____
No _____

Please attach an explanation and/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "D3E.Doc"

53) Are any policy benefits, pricing discounts, or other options denied to customers who have chosen to opt out? (NAIC Model 672 Section 23(A), NAIC Market Conduct Standard 12, Procedure D)

Yes_____
No _____

Please provide a description of the controls in place to prevent discrimination against customers that have opted out and/or any relevant documents using the file name "D3F.Doc"

54) Does the licensee's opt-out notice accurately explain the consumer's right to opt-out, including the methods by which the consumer may exercise that right at any time, in accordance with applicable law and the company's policies and procedures and does the notice contain a statement that the licensee discloses or reserves the right to disclose non-public personal financial information about its consumer to a non-affiliated third party? (NAIC Model 672 Section 8(A)(l)(a), NAIC Market Conduct Standard 14, Procedure F)

Yes_____
No _____

Please attach an explanation and/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "D3G.Doc"

55) Does the notice contain a statement that the consumer has the right to opt-out of that disclosure and a reasonable means by which the consumer may exercise the right to opt-out? (NAIC Model 672 Section 8(A)(1)(b), NAIC Market Conduct Standard 14, Procedure F)

Yes_____
No _____

Please attach an explanation and/or relevant documents, including a copy of the company's opt-out notice, using the file name "D3H.Doc"

Safeguarding of Customer Records

Please provide the name, title, and telephone number of the company contact person responsible for the answers to this set of questions using the file name "F1.Doc"

56) Please describe the applicable components of the company's information security policy, which may include but not necessarily be limited to a definition of scope, objectives, risk assessment, and roles and responsibilities relating to administrative, technical and physical safeguards. (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation 3, 4, 6, 7, Market Conduct Examination Standard 17, Procedure A)

Please provide a narrative description, as well as relevant documentation that supports the existence of pertinent policy components, using the filename "F1A.doc"

57) Please describe how the company's information security policy addresses the following, which may include, but not necessarily be limited to: (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer

Information Model Regulation —4; Market Conduct Examination Standard 17, Procedure C)

- Policies to ensure the security and confidentiality of customer records and information.
- Policies to protect against any anticipated threats or hazards to the security or integrity of such records.
- Policies to protect against unauthorized access to or use of such records or information, which could result in substantial harm or inconvenience to any customer.

Please provide a narrative description, as well as copies of relevant policies, using the file name "F1B.Doc"

58) Please describe how the company's information security program was designed to meet the objectives of the Gramm-Leach-Bliley Act Standards for Safeguarding of Customer Information. (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 1, 2, 3, 4, 5, 6, 7, 8, 9; Market Conduct Examination Standard 17)

Please provide a narrative description, as well as any relevant program documentation, which may include policies and an index evidencing the existence of relevant procedures, using the file name "F1C .Doc".

59) Please describe to what level of detail the company's information security program contains formal documentation of the following, which may include, but not necessarily limited to:

- Information security standards. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3,4; Market Conduct Examination Standard 17, Procedure A)
- Policies and procedures. (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer information Model Regulation — 3, 4; Market Conduct Examination Standard 17, Procedures A and C)
- Established baselines for security over operating systems and databases. (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 7, 9; Market Conduct Examination Standard 17, Procedures A and C)

Please provide a narrative description, as well as relevant documentation that supports the existence of the standards, procedures, and baselines, using the filename "F1D.Doc"

60) Please describe to what level the company's information security program addresses the IT organizational structure. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4; Market Conduct Examination Standard 17, Procedure A)

Please provide a narrative description, as well as relevant organization charts showing where the responsibility for information security resides in relation to the IT department and other control and administration departments within the company, using the file name "F1E.Doc"

61) Please describe how specific responsibility was assigned- for creating; implementing and maintaining the program. (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 5, 8, 9; Market Conduct Examination Standard 17, Procedure A and C)

Please provide a narrative description, as well as relevant job description materials evidencing who is responsible for program implementation within the company, using the file name "F1F.Doc"

62) Please describe how the program addresses information security awareness and training. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 7; Market Conduct Examination Standard 17, Procedure A)

Please provide a narrative description, as well as relevant sample materials, policies, or training guide indices evidencing the existence of such, using the file name "F1G.Doc"

63) Please describe how the company's information security program was designed to be in accordance with regulatory guidance, which may include but not necessarily be limited to applicable federal, state, local, and other laws. (Gramm-Leach-Bliley Act Section 501(a) & (b), NAIC Market Conduct Examination Standard 17, Procedure A)

Please provide a narrative description using the file name "F1H.Doc"

64) Please describe the company's risk assessment process and whether that process provides for the identification of systems involved in the creation, processing and storing of customer information, and whether it identifies and assesses the reasonably foreseeable internal and external and natural disaster threats that may threaten the security and integrity of customer information that could result in unauthorized disclosure, misuse, alteration or destruction of customer information and related systems by considering the following items, which may include, but not necessarily limited to: (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 6; Market Conduct Examination Standard 17, Procedure C)

- Whether the assessment addresses all potential external network access points e.g. Internet and dial-up).
- Whether the assessment addresses the inventory of systems containing customer information, including the platforms on which these systems reside.

- Whether the assessment addresses all extranet access points or all other methods of transmitting data outside the company (e.g. via vendors and business partners).
- Whether the assessment addresses unauthorized activity or viewing of sensitive information on internal systems.
- Whether the assessment addresses physical access points to system hardware?
- Whether the assessment addresses storage points for hard copy documentation?

Please provide a narrative description, including an explanation of risk assessment activities that have been undertaken, as well as a copy of the risk assessment, using the file name "F2A.Doc"

65) Please describe how the company addressed the likelihood and potential damage of the threats noted in the risk assessment and how the company identified the likelihood of occurrence and potential threat based on the sensitivity of customer information. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 6; Market Conduct Examination Standard 17, Procedure C)

Please provide a narrative description, as well as a summary of general vulnerability assessment results if different from the risk assessment, using the file name "F2B.Doc"

66) Please describe how the company assesses risk in terms of confidentiality and integrity of customer information systems and non-public customer information whether it is being stored, processed or transmitted. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 6; Market Conduct Examination Standard 17, Procedures B and C)

Please provide a narrative description using the file name "F2C.Doc"

67) Please describe how the company has considered the sensitivity and classification of information in assessing the risk of customer data (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 7; Market Conduct Examination Standard 17, Procedure B)

Please provide a narrative description, as well as any relevant policies, using the file name "F2D.Doc"

68) Please describe how the company's assessment of data classification strategies, policies or procedures and related controls for sensitive information has been formally conducted and documented, and how the company assessed the sufficiency of existing policies, procedures, customer information systems and other arrangements intended to control the risks identified by executing

vulnerability tests of the following, which may include, but not necessarily limited to:

(Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 6, 7; Market Conduct Examination Standard 17, Procedures B and C)

- Internal/external network access points.
- Logical access to information systems included in internal audit reviews.
- Physical access secured server rooms.

Please provide a narrative description, as well as a summary of results documented or reports issued using the file name "F2E.Doc"

69) Please describe how the company monitors, evaluates and adjusts risk assessments based on changes in technology or the sensitivity of the information. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 7, 9; Market Conduct Examination Standard 17, Procedure B)

Please provide a narrative description, including any planned risk assessment activities that will take place over the next 12 to 24 months to re-assess risk areas and levels of risk, using the file name "F2F.Doc"

70) Please describe how the company's policies and procedures address access controls on systems maintaining customer information and how it addresses the following, which may include, but not necessarily be limited to:

- Formal procedures to ensure only authorized individuals are granted access to data as needed. (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation —3, 4; Market Conduct Examination Standard 17, Procedures A and C)
- Formal procedures to ensure data is periodically re-evaluated or certified to ensure the appropriate levels of access are consistent with policies and procedures. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 7, 9; Market Conduct Examination Standard 17, Procedures A and C)

Please provide a narrative description and attach any relevant reports or other materials that show access controls over customer information exist and are periodically reviewed and maintained, as well as any relevant policies and the index evidencing the existence of relevant procedures, using the file name "F3A.Doc"

71) Please describe how user access rights to customer information are determined and granted to ensure the following, which may include but not necessarily be limited to: (Gramm-Leach-Bliley Act Section 501(a) & (b),

Standards for Safeguarding Customer Information Model Regulation — 3; Market Conduct Examination Standard 17, Procedure B)

- Access for new users is properly established on an individual or group basis.
- Access is restricted to only relevant customer information based upon valid authentication criteria (e.g. date of birth, mothers maiden name).
- User access rights are periodically reviewed to ensure each user's access is commensurate with the user's job functions.
- Termination and job change procedures are enforced.
- Inactive user accounts are identified and removed.

Please provide a narrative description and attach any relevant reports or other materials that show access controls over customer information exist and are periodically reviewed and maintained, as well as any relevant policies and the index evidencing the existence of relevant procedures, using the file name "F3B.Doc"

72) Please describe how the company's security policies and procedures address password controls at the network, operating systems, application and database levels and whether they include each of the following, which may include but not necessarily be limited to: (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3; Market Conduct Examination Standard 17, Procedure B)

- Use of unique ID's and passwords.
- Use of minimum password length.
- Use of alphanumeric/case sensitive.
- User lockout after a number of unsuccessful login attempts.
- User lockout after a period of inactivity.
- Procedures for setting up new passwords.
- Procedures if users forget passwords.
- Use of a standard frequency for forced change of passwords.
- Use of encryption for stored passwords.

Please provide a narrative description and attach any relevant reports or other materials that show password controls exist and are maintained at each level, as well as any relevant policies and the index evidencing the existence of procedures, using the file name "F3C.Doc"

73) Please describe how the company's security policies and procedures address dial-up access and whether they include each of the following, which may include but not necessarily be limited to: (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4, 7(A), 9; Market Conduct Examination Standard 12, Procedure A and Standard 17, Procedure A)

- Granting dial-up access.

- Authorizing dial-up access for particular employees.
- Reviewing and monitoring dial-up access.
- Reviewing violations logs or unsuccessful dial-up access attempts.
- Restricting dial-up access (e.g., time or day, single login).

Please provide a narrative description and attach any relevant reports or other materials that show dial-up access controls exist and are periodically reviewed and maintained, as well as any relevant policies and the index evidencing the existence of relevant procedures, using the file name "F3D.Doc"

74) Please describe how database controls exist to authenticate users, achieve data confidentiality (i.e. through encryption), and maintain data integrity for databases supporting customer related applications. (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4; Market Conduct Examination Standard 17)

Please provide a narrative description and attach any relevant reports or other materials that show database controls that maintain confidentiality and integrity exist and are periodically reviewed, as well as any relevant policies, using the file name "F3E.Doc"

75) Please describe how physical security controls were incorporated in the information security policies and procedures and whether they include each of the following, which may include but not necessarily be limited to: (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4; Market Conduct Examination Standard 12, Procedure A and Standard 17, Procedures A and C)

- Policies to restrict access at locations, such as buildings, computer facilities, record storage facilities and mail rooms.
- Policies requiring the use of card keys, security guards, surveillance cameras and access logs.
- Policies requiring the locking of file drawers and security cages for paper forms containing customer information.

Please provide a narrative description and attach any relevant reports or other materials that show physical security controls exist, as well as any relevant policies and the index evidencing the existence of relevant procedures, using the file name "F3F.Doc"

76) Please describe the controls that exist over external storage vendors used for archiving customer information and whether a list of approved vendors used to store records is maintained and contains the following, which may include but not necessarily be limited to: (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4, 8 (A, B); Market Conduct Examination Standard 12, Procedure A and Standard 17, Procedures A and C)

- Procedures for retrieving internal and external stored information.
- Procedures for storing customer information, data, paper and forms.
- Procedures for granting access to new employees and removing terminated employee access.

Please provide a narrative description and attach any relevant reports or other materials that show the existence of off-site storage vendors or company managed storage locations, as well as any relevant policies governing access review and maintenance and the index evidencing the existence of relevant procedures, using the file name "F3G.Doc"

77) Please describe whether the company's external transmission policies and procedures that address customer information contain each of the following, which may include but not necessarily be limited to: (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 6; Market Conduct Examination Standards 17)

- Policies requiring the listing of all file transmissions that are scheduled to occur on a regular basis, indicating the third party to whom the transmission is going, the purpose of the transmission and the customer information contained within the transmission.
- Policies governing one-off or ad-hoc file transmissions.
- Policies governing who is authorized to perform or modify file transmissions.
- Policies governing who is authorized to perform one-off or ad-hoc downloads.
- Policies designed to ensure data downloads or transmissions- are appropriate, the business need is understood, the sensitivity of the information is communicated and safeguards are in place.
- Policies governing the type of security used to protect against unauthorized access (e.g. encryption, frame relay, other).

Please provide a narrative description and attach any relevant reports or other materials that show an inventory of external data transmissions, data communications, and network diagrams showing public vs. private networks, encryption methods used, as well as any relevant policies and the index evidencing the existence of relevant procedures, using the file name "F3H.Doc"

78) Please describe the forms and use of data encryption products and algorithms employed by the company (e.g. SSL 128 Secure Data). (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4; Market Conduct Examination Standard 17)

Please provide a narrative description, as well as any relevant reports or other materials that list forms and use of data encryption products/algorithms in use, using the file name "F3I.Doc"

79) Please describe whether "live production" customer information is used in a test environment and whether a business case has been developed for the need to use "live production" customer information. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4 (A, B, C), 6 (A, B, C); Market Conduct Examination Standard 17, Procedure A)

Please provide your narrative description, as well as evidence of the existence of a business case that provides for the use of "live production" customer information in the test environment, using the file name "F3J.Doc"

80) Please describe whether formal policies and procedures exist to assess the impact of information security changes to systems containing customer information. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4 (A, B, C), 9; Market Conduct Examination Standard 12, Procedure A)

Please provide a narrative description, as well as any relevant policies pertaining to the assessment of the impact of information security changes to systems containing customer information and the index evidencing the existence of relevant procedures, using the file name "F3K.Doc"

81) Please describe whether rules for customer authentication been defined by the company and implemented to support the corporate privacy statement. (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4 (A, B, C), 9; Market Conduct Examination Standard 17, Procedure A)

Please provide a narrative description, as well as any relevant policies pertaining to methods used to authenticate a customer prior to disclosing non-public personal information to them and the index evidencing the existence of relevant procedures, using the file name "F3L.Doc"

82) Please describe whether policies and procedures require dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information and detail which sensitive information/transmission/functions have dual controls in place and who has responsibility for these controls that address the following items, which may include, but not necessarily be limited to: (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation —3, 4, 6, 7 (A), 9; Market Conduct Examination Standard 12, Procedures A and B and Standard 17)

- Do procedures allow for the same user input and approve data?
- Do procedures allow for users in the Accounting Department access data in the Marketing Department systems?

- Do procedures require that background checks be performed that include previous work and criminal records for users with access to sensitive customer information?

Please provide a narrative description, as well as any relevant policies pertaining to dual controls, segregation of duties, and employee background checks, and the index evidencing the existence of relevant procedures, using the file name "F3M.Doc"

83) Please describe whether policies and procedures address monitoring and detection of actual and attempted attacks on customer information systems, networks, storage devices and whether they include: (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 6, 7; Market Conduct Examination Standard 17)

- Procedures governing the frequency with which monitoring is conducted and for what customer information systems.
- Procedures governing the use of automated Intrusion Detection Systems (ID's) to monitor Internet devices and critical internal systems.
- Procedures governing exception reports generated from system logs.
- Procedures governing instantaneous alerts if successful or unsuccessful intruder attempts occur.
- Procedures governing whether such attempts have been categorized based upon their criticality (e.g. general network penetration, unauthorized access to database systems maintaining customer information, etc).
- Procedures governing unusual network activity monitoring.
- Procedures governing security related to operating systems events monitoring, including a daily review of systems access and activity logs.
- Procedures identifying the individual responsible for maintaining these procedures and for performing ongoing monitoring.
- Procedures governing the logging and reporting of security incidents to senior management.
- Procedures identifying the individual responsible for preparing the log and reporting incidents.
- Procedures identifying the individual responsible for reviewing incident logs and the frequency of review.

Please provide a narrative description and attach any relevant reports or other materials to illustrate that appropriate monitoring of actual and attempted attacks on customer information systems is identified, investigated and prevented from recurring, as well as any relevant policies and the index evidencing the existence of relevant procedures, using the file name "F3N.Doc"

84) Please describe whether policies are in place to ensure information system attack events are reported and whether the policies include the following: (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding

Customer Information Model Regulation — 7; Market Conduct Examination Standard 17, Procedures A and B)

- Policy to document an escalation response to unauthorized- access attempts to customer information.
- Policy to address recent unauthorized access attempts.
- Policy to address actions to be taken when a suspected intrusion occurs.
- Policy to documented action steps.
- Policy to ensure regulatory/law enforcement agencies are informed when intrusion attempts occur or when customer information has been compromised.
- Policy to ensure individual responsibility exits to inform regulatory/law enforcement agencies.

Please provide a narrative description, as well as relevant policies, using the file name "F3O.Doc"

85) Please describe whether all systems located in data centers maintain adequate controls to protect against environmental hazards and whether controls address fire, water damage, and temperature and power surges/outages. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 4; Market Conduct Examination Standard 17, Procedures A and B)

Please provide a narrative description, as well as any relevant documentation evidencing the existence of environmental controls, using the file name "F3P.Doc"

86) Please describe whether a formal business continuity program exists, includes a backup of systems/files containing customer information, requires testing for the retrieval of information from backup media, and includes each of the following requirements for each application, which may include, but not necessarily be limited to: (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3 6; Market Conduct Examination Standard 17)

- A requirement for a written disaster recovery plan.
- A requirement for an operational recovery facility.
- A requirement for documenting backup methods used (e.g. tape, mirroring, vaulting, etc).
- A requirement for documenting back up frequency and number of set procedures for manually duplicating data during recovery.

Please provide a narrative description, as well as the index evidencing the existence of relevant business continuity/disaster recovery plan components and evidence of the last test results, using the file name "F3Q.Doc"

87) Please describe whether the company has established a security training program for all employees that have access to customer information, which may include but not necessarily be limited to the following: (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 7(B); Market Conduct Examination Standard 17, Procedures A and C)

- Procedures addressing the content of training programs.
- Procedures addressing the personnel who can conduct training.
- Procedures addressing the personnel who must attend training.
- Procedures addressing the frequency of training courses.
- Procedures addressing training course content (e.g. how to safeguard customer information, detect fraudulent activity, prevent unauthorized access, etc.).

Please provide a narrative description and attach any relevant reports or other materials that show training programs or communications to employees regarding the security program exist, as well as any relevant policies and the index evidencing the existence of relevant content, using the file name "F3R.Doc"

88) Please describe whether an independent third party has been identified to test or review the key controls, systems and procedures of the information security program, which may include but not necessarily be limited to the following: (Gramm-Leach-Bliley Act Section 501 (a) & (b), Standards for Safeguarding Customer Information Model Regulation —3, 7 (C); Market Conduct Examination Standard 17)

- Procedures addressing the testing performed by internal audit, a security officer or a third party.
- Procedures addressing the frequency of testing.
- Procedures addressing the nature of testing.
- Procedures addressing the results of testing reported to management.
- Procedures addressing actions taken.

Please provide a narrative description, as well as any relevant reports or other materials evidencing the involvement of an independent third party to test or review key controls, systems and procedures of the information security program, using the file name "F3S.Doc"

89) Please describe whether the company's board or management designated an individual to act as a liaison with the Corporate Information Security Group to facilitate the administration of the information security program. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3; Market Conduct Examination Standard 17, Procedure A)

Please provide the name, title and telephone number of the company's contact person responsible for being the liaison between the corporate information security group and the board and/or management of the information security program, using the file name "F4A.Doc"

90) Please describe whether policies and procedures have been implemented to address the process for adjustments to the information security program in light of changes in technology, laws and regulations, sensitivity of customer information, security incidents, new ventures, etc. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 3, 9; Market Conduct Examination Standard 12, Procedure A)

Please provide a narrative description that addresses the process for adjustments to the information security program and attach any relevant policy documentation and the index of relevant procedures evidencing the existence for adjustments to the information security program using the file name "F4B.Doc"

91) Please describe the company's process for determining service providers to be selected, which may include but not necessarily be limited to the following policies: (NAIC Model 672 — 8 (A, B); Market Conduct Examination Standard D and Standard 17, Procedure B)

- Policies for assessing a service provider's privacy policies and practice.
- Policies for assessing of a service provider's security policies and practices.
- Policies for assessing a service provider's general business reputation.

Please provide a narrative description and attach relevant documentation that supports the existence of the process, as well as relevant policies and the index evidencing the existence of relevant procedures, using the file name "F4C.Doc"

92) Please describe whether the company requires service providers to implement appropriate measures designed to meet the objectives of the NAIC Standards for Safeguarding of Customer Information? (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 8; Market Conduct Examination Standard 17)

Please provide a narrative description and attach relevant policies and an index evidencing the existence of relevant procedures in place to ensure that service providers have implemented appropriate security measures, using the file name "F4D.Doc"

93) Please describe whether the company takes appropriate steps, where indicated by their risk assessment, to confirm that service providers have implemented appropriate steps to safeguard non-public personal-information. (Gramm-Leach-Bliley Act Section 501(a) & (b), Standards for Safeguarding Customer Information Model Regulation — 8 (B); Market Conduct Examination Standard 17)

Please provide a narrative description, including a discussion of the relevant criteria for selecting service providers for review and a listing of service providers that have been reviewed, using the file name “F4E.Doc”

ATTACHMENT D

ACKNOWLEDGMENT

The courteous cooperation extended to all persons associated with this examination project by the before mentioned companies' officers and staff is gratefully acknowledged.

In addition to the undersigned, Barry Kreiswirth, attorney to the DC Department of Insurance, Security and Banking assisted in the project through his review of the supporting documents and in the preparation of the September 2005 preliminary report.

Respectfully submitted,

_____

WILLIAM FORREST McCUNE, CIPP
Examiner-in-charge