



STATE OF OREGON

DEPARTMENT OF CONSUMER AND BUSINESS SERVICES

INSURANCE DIVISION

REPORT OF MARKET CONDUCT EXAMINATION

OF

**CALIFORNIA CASUALTY GROUP  
SAN MATEO, CALIFORNIA**

**Published on December 6, 2005**

## TABLE OF CONTENTS

<b>SALUTATION .....</b>	<b>3</b>
<b>CALIFORNIA CASUALTY GROUP .....</b>	<b>3</b>
<b>PROJECT OVERVIEW .....</b>	<b>3</b>
<b>GROUP PROFILE .....</b>	<b>6</b>
<b>METHODOLOGY .....</b>	<b>6</b>
QUESTION CATEGORIES .....	7
<i>NAIC Model Rule # 672</i> .....	7
QUESTION CATEGORIES .....	7
<i>NAIC Model Rule # 673</i> .....	7
<b>FINDINGS .....</b>	<b>8</b>
<b>ACKNOWLEDGEMENT .....</b>	<b>10</b>
<b>AFFIDAVIT .....</b>	<b>11</b>
<b>APPENDIX .....</b>	<b>12</b>

## **SALUTATION**

June 1, 2005

Honorable Joel S. Ario, Commissioner  
Department of Consumer and Business Services Insurance Division  
350 Winter St. NE, Room 440  
Salem, OR 97309-0405

Dear Mr. Commissioner:

In accordance with your instructions and pursuant to ORS 731.300, and procedures promulgated by the National Association of Insurance Commissioners, a targeted market conduct examination of the privacy compliance practices has been conducted of the:

### **CALIFORNIA CASUALTY GROUP**

The report is hereby respectfully submitted.

### **PROJECT OVERVIEW**

Substantial interest exists among state insurance regulators, legislators at both the state and federal level, and the wider public as to whether insurers are appropriately protecting the privacy of personal information in their possession on policyholders and applicants. Title V of the Gramm Leach Bliley Act of 1999 sets forth federal guidelines for the protection of the privacy of personal financial information, and most states have enacted laws to ensure the privacy of financial, and in many cases health, information held by insurers. Although there are variations among state laws, most are based substantially on the NAIC Model Privacy Act of 2000. Some also include provisions from the NAIC Model Privacy Act of 1982. In an attempt to avoid, as much as possible, a multitude of overlapping and repetitive examinations of the privacy protection practices of individual insurance companies, the District of Columbia agreed to be the lead jurisdiction in a nationwide survey of major insurance companies to assess whether public and governmental expectations about the protection of private

personal information are being met. Over a dozen states participated actively with the District of Columbia in the project, and most other states have agreed to accept the findings of this examination and not seek to examine separately those companies covered by the District's comprehensive study.

To carry out the examination, the District of Columbia Department of Insurance and Securities Regulation (now the Department of Insurance, Securities and Banking), retained the services of PricewaterhouseCoopers LLP, American Express Tax and Business Services Incorporated and Huff, Thomas & Company, who agreed to assist us in conducting among them an extensive, survey-type examination of approximately 100 of the largest U.S. insurers, both life/health and property/casualty companies. Some of the companies scheduled to be examined are not licensed in the District of Columbia and are therefore not subject to the jurisdiction of the D.C. Department. In those cases, examination notices were issued by participating states where the companies are licensed. This examination was conducted under the authority of the Oregon Insurance Division. A few companies scheduled for examination were excused on the basis of extensive prior examinations, focused on privacy compliance, by state insurance departments or by the federal Securities and Exchange Commission.

It was not the intent of the examination program to determine whether individual companies are 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. Based on the examination report issued by the District of Columbia, it is anticipated that each state insurance department will make its own determination of whether the examined company should be subject to further examination and whether the company is potentially in violation of that state's law.

Although contractors were involved in the development of the information that forms the basis of this report, and although other states worked closely with the District of Columbia in the design and implementation of the examination program, the end result

is solely the responsibility of the District of Columbia Department of Insurance, Securities and Banking.

## **FORWARD**

This report achieves two objectives. First, the report reflects Oregon's assessment of the insurance privacy practices of the California Casualty Group, hereinafter referred to as the Group and second, the report evaluates the Group's privacy compliance with the National Association of Insurance Commissioners Model Rule #672 and #673. Both evaluations used a comprehensive questionnaire followed by conferences with select Company representatives. The examination provides a report describing, at a high level, the procedures performed and matters that came to the examiner's attention.

## **SCOPE AND APPROACH OF EXAMINATION**

A Privacy Status Review Questionnaire (See Appendix) was developed to assess the state of the Group's privacy compliance policies and procedures. The Privacy Status Review Questionnaire was designed to address the key elements of the significant privacy laws, regulations and standards applicable to the insurance industry (the "Key Elements of Privacy Protection"). The Key Elements of Privacy Protection included within the scope of this project are:

- Title V of GLBA,
- NAIC Model 672, Privacy of Consumer Financial and Health Information (2000 Model),
- NAIC Model 673, Standards for Safeguarding Customer Information (2000 Model),
- NAIC Model 670, Insurance Information and Privacy Protection Act (1982 Model) (sections addressing notice and access only), and
- NAIC Market Conduct Examiners Handbook Standards.

State variations to these laws are not explicitly addressed in the current version of the Privacy Status Review Questionnaire. (See Appendix)

## **GROUP PROFILE**

The scope of the Privacy Status Review included only the domestic operations of the Group, inclusive of the following legal entities:

00222 California Cas Indem Exch	20117	California Casualty Group	CA
03336 California Casualty Ins Co	20125	California Casualty Group	CA
California Casualty & Fire Ins Co	27464	California Casualty Group	CA
California Casualty General Ins Co	35955	California Casualty Group	CA
California Casualty Compensation Ins C	10063	California Casualty Group	CA

## **METHODOLOGY**

An objective, independent review of the Group's answers to the Privacy Status Review Questionnaire was performed. The Privacy Status Review Questionnaire focused on addressing both the Key Elements of Privacy Protection noted above and the underlying risks that may increase the risk of non-compliance with these requirements. The questionnaire asked the Group to make representations as to whether it is performing compliance activities with respect to the Key Elements of Privacy Protection. In addition to these representations, the Group was asked to provide a brief description of any existing process or procedures and attach relevant documentation to support the existence of such processes or procedures. This process was used to ensure, to the extent possible in a remote examination, that the processes the Group represented it is using contain viable controls for complying with the Key Elements of Privacy Protection and protecting the privacy and confidentiality of customer information. The overall privacy topics reviewed included:

- Privacy Notice and Customer Notification
- Policies and Procedures

- Customer Option Preferences
- Safeguarding of Customer Records

The scope of the work was limited and did not include a review of the Group’s efforts with respect to remediation activities. The scope of the work did **not** include (i) a detailed analysis of the effectiveness of the Group’s plans to correct privacy problems or to protect the business against the consequences associated with any privacy related occurrences, (ii) a determination of steps the Group must take to become privacy compliant or maintain privacy compliance, or (iii) testing.

**Question Categories**

<b><u>NAIC Model Rule # 672</u></b>	
Delivery of privacy notices.	Questions 1-7, 38
Content of privacy notices.	Questions 8 –23
Policies and procedures for preventing unauthorized disclosures of information.	Questions 31-32, 36-37, 39-40
Policies and procedures for obtaining authorization for disclosure of health information.	Questions 33-35
Policies and procedures for privacy complaints.	Question 41
Procedures for providing opt-out notifications.	Questions 42-43, 45-48, 54-55
Procedures for collecting opt-out elections.	Questions 44, 49-53

**Question Categories**

<b><u>NAIC Model Rule # 673</u></b>	
Licensee’s methodology in designing their information security policy.	Questions 56-58, 90
Content of information security policy.	Questions 59-61
Information security awareness and training.	Question 62, 87
Risk assessment process.	Questions 63-69, 88

Access controls.	Questions 70-71, 73, 79, 81, 82
Information storage.	Question 72, 74-76, 85
Information transmission.	Question 77, 78
Information integrity.	Question 77, 78, 80, 83, 84
Miscellaneous.	Questions 86, 89, 91-93
<b>1982 Model Rule</b>	Questions 24-30

## FINDINGS

This section provides a summary of findings identified during the course of the Privacy Status Review. The findings are in order of the questions with which they are associated in the Privacy Status Review Questionnaire. In summary, Company management should consider addressing the following findings:

Questionnaire Reference	Finding
NAIC Model Rule # 672 – No Findings Noted.	
NAIC Model Rule # 673 – No Findings Noted.	
1982 Model Rule	
29	<p>While the Company submitted an internal email and their privacy notice, the Company has not provided evidence of internal policies or procedures that ensure the following customer rights outlined in Section 8 are granted to customers:</p> <ol style="list-style-type: none"> <li>1) The ability for individuals to see a copy of their personal information in person,</li> <li>2) The requirement of provided personal information to include the source types of the information collected,</li> <li>3) The above rights will be granted within 30 days of the request being received.</li> </ol> <p>The Company has stated that they will develop specific written procedures to address the above elements by April 15<sup>th</sup>, 2005.</p>

<b>Questionnaire Reference</b>	<b>Finding</b>
30	<p>While the Company submitted an internal email and their privacy notice, the Company has not provided evidence of internal policies or procedures that ensure the following customer rights outlined in Section 9 are granted to customers:</p> <p>2) 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,.</p> <p>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,</p>

<b>1982 Model Rule</b>	<b>Findings</b>
30	<p>3) Within 30 days the recipient of a request must correct, amend or delete the personal information or notify the individual of a refusal: including reasons for the refusal, and their right as an individual to file a statement,</p> <p>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 9B1-3 of the NAIC Insurance Information and Privacy Protection Model Act.</p> <p>The Company has stated that they will develop specific written procedures to address the above elements by April 15<sup>th</sup>, 2005.</p>

## ACKNOWLEDGEMENT

PricewaterhouseCoopers' findings are included in the examination report and as such, PricewaterhouseCoopers is not responsible for the sufficiency of the procedures for the purpose of this report.

The undersigned's participation in this limited scope examination as the Examiner-In-Charge encompassed responsibility for administrative coordination, report writing and work paper compilation.

The cooperation and assistance of staff from the following jurisdictions is herein acknowledged:

Alabama Department of Insurance;  
Arkansas Insurance Department;  
California Department of Insurance;  
Indiana Department of Insurance;  
New Hampshire Department of Insurance;  
New Jersey Department of Banking and Insurance;  
New York State Department of Insurance;  
Ohio Department of Insurance;  
Oregon Insurance Division; and  
South Carolina Department of Insurance

Respectfully submitted,

---

Cindy J. Jones, AIE, CPCU, AIRC  
Manager, Market Surveillance  
Insurance Division  
Department of Consumer and Business Services  
State of Oregon



## APPENDIX

### **Privacy Notice and Customer Verification**

Please provide the name, title, and telephone number of the company contact person responsible for the answers to this Privacy Status Review Questionnaire using the file name "B1C.Doc"

1) Has the company published 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 B](#))

Yes \_\_\_\_\_

No \_\_\_\_\_

B1A

2) Has the company disseminated this privacy notice to all existing customers as of July 1, 2001 and is there a process to facilitate distribution to new customers? ([Model 672 Sections 5&6, Market Conduct Examination Standard - Standard B, Procedure E](#))

Yes \_\_\_\_\_

No \_\_\_\_\_

B1B

3) What was management's strategy for the distribution of privacy notices to customers, and if applicable, to consumers, both the initial and annual notice to customers and subsequent delivery of notice? Also, please explain how the company determined who all of their customers were, such as by performing an analysis defining customer and consumer status for each class or type of insured, beneficiary, annuitants, mortgagors and claimants. ([NAIC Model 672 Section 4\(F\)&\(I\), Market Conduct Examination Standard - Standard B, Procedure D](#))

Please attach a brief explanation and relevant documents using the file name "B1D.Doc"

4) Explain the procedure for ensuring privacy notices were distributed in such a manner that customers could be reasonably expected to receive them by July 1, 2001. ([NAIC Model 672 Section 26\(B\), NAIC Market Conduct Standard B Procedures E&F](#))

Please attach an explanation and any relevant documents using the file name "B1E.Doc"

5) What procedures has the company implemented to provide the 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 26\(B\), Market Conduct Examination Standard - Standard B, Procedure E](#))

Please attach an explanation of the procedure, a copy of the initial privacy notice and/or any relevant documents using the file name "B1F.Doc"

6) What is 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 B, Procedure E](#))

Please attach an explanation of the procedure and a copy of the annual privacy notice using the file name "B1G.Doc"

7) What is the procedure for providing revised notices to customers and if applicable, to consumers? (NAIC Model 672 Section 9, NAIC Market Conduct Standard B Procedure D(1))  
Please provide an explanation and attach a copy of any revised privacy notices using the file name "B1H.Doc"

8) Was the notice 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 B, Procedure I)  
Please attach an explanation and/or any relevant documents using the file name "B1I.Doc"

9) Provide mailing dates for the privacy notices to facilitate a determination of whether customers could have reasonably been expected to receive the notices prior to the July 1, 2001 deadline.  
Please attach an explanation and/or any relevant documents using the file name "B1K.Doc"

10) What was management's strategy for ensuring the format of the privacy notice meets the definition of "clear and conspicuous?" Also, what procedures were performed to ensure that the language used in the privacy notice is understandable to the average consumer by using everyday words, simple sentences, and avoiding technical language? (NAIC Model 672 Section 4(B)(2), NAIC Market Conduct Standard B, Procedure A).  
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 "B2B.Doc"

11) Were privacy notices provided to customers and, if applicable, consumers focusing on both the legal requirements for notice (Section 7 of NAIC Model 672) and management's due diligence efforts to ensure that the notice accurately represents the company's information handling practices? (Section 7 of NAIC Model 672, NAIC Market Conduct Standard B Procedure A)

Yes \_\_\_\_\_

No \_\_\_\_\_

B3A

12) 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 B Procedure A(1))

Yes \_\_\_\_\_

No \_\_\_\_\_

B3B

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

Yes \_\_\_\_\_

No \_\_\_\_\_

B3C

14) 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 B Procedure A(3))

Yes \_\_\_\_\_

No \_\_\_\_\_

N/A \_\_\_\_\_

B3D

15) 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 B Procedure A(4))

Yes \_\_\_\_\_

No \_\_\_\_\_

N/A \_\_\_\_\_

B3E

16) 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 B Procedure A(5))

Yes \_\_\_\_\_

No \_\_\_\_\_

N/A \_\_\_\_\_

B3F

17) 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))

Yes \_\_\_\_\_

No \_\_\_\_\_

N/A \_\_\_\_\_

B3G

18) 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))

Yes \_\_\_\_\_

No \_\_\_\_\_

N/A \_\_\_\_\_

B3H

19) 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))

Yes \_\_\_\_\_  
No \_\_\_\_\_

B3I

20) 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))

Yes \_\_\_\_\_  
No \_\_\_\_\_

B3J

21) 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))

Yes \_\_\_\_\_  
No \_\_\_\_\_

B3K

22) Does the company use a simplified privacy notice? (NAIC Model 672 Section 7(C)(5))

Yes \_\_\_\_\_  
No \_\_\_\_\_

B3L

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)). Also, please provide copies of the simplified privacy notice using the file name "B3N.Doc"

23) Does the company use a short form privacy notice? (NAIC Model 672 Section 7(D))

Yes \_\_\_\_\_  
No \_\_\_\_\_

B3O

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". (NAIC Model 672 Section 7(D)). Also, please provide a copy of the short form notice using the file name "B3P.Doc"

24) Has the company performed due diligence to verify the accuracy and content of the privacy notice? (NAIC Model 672 Section 5(A) and Section 6(A))

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please attach an explanation and/or relevant sample documents using the file name "B3Q.Doc"

25) Do the licensee's privacy notices include all necessary disclosures as determined by their review of information handling practices? (NAIC Model 672 Section 7)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide copies of the privacy notice(s) delivered to customers and, if applicable, to consumers using the file name "B3R.Doc"

**26) 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)**

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide copies of the privacy notice(s) delivered to applicants and policyholders using the file name "B3S.Doc"

**27) 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))**

Yes \_\_\_\_\_  
No \_\_\_\_\_

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

**28) 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))**

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide copies of any relevant policies and the index evidencing the existence of relevant procedures using the file name "B3U.Doc"

**29) Does the licensee have policies and procedures in place to 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))**

Yes \_\_\_\_\_

No \_\_\_\_\_

Provide copies of any relevant policies and the index evidencing the existence of relevant procedures using the file name "B3V.Doc"

**30) 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))**

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide copies of the privacy notice(s) delivered to applicants and policyholders using the file name "B3W.Doc"

**31) Does the licensee have policies and procedures in place to provide access to recorded personal information? (NAIC Insurance Information and Privacy Protection Model Act, Section 8)**

Yes \_\_\_\_\_

No \_\_\_\_\_

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 "B3X.Doc"

**32) Does the licensee have policies and procedures in place to allow individuals to request that recorded personal information be corrected, amended, or deleted? (NAIC Insurance Information and Privacy Protection Model Act, Section 9)**

Yes \_\_\_\_\_

No \_\_\_\_\_

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 "B3Y.Doc"

**Policies and Procedures**

33) Did the licensee initiate a formal process or project to determine what non-public personal information (NPPI) is collected across the business units of the company and how that information is shared internally and externally? (NAIC Model 672 Section 5 and Section 6(A))

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please attach an explanation and any relevant documents using the file name “C1A.Doc”

34) Has management developed policies and procedures to ensure that the company uses and discloses nonpublic personal financial information that it receives from a nonaffiliated financial institution in compliance with the NAIC model regulation? (NAIC Market Conduct Standard D, Procedure B)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please attach an explanation and/or any relevant documents using the file name “C1B.Doc”

35) Has management performed a survey or used some other method for identifying sharing practices with affiliated third parties to specifically identify any information shared with affiliates that meet the FCRA definition of a credit report? (NAIC Model 672 Section 7(A)(7))

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please attach an explanation and/or any relevant sample documents using the file name “C1C.Doc”

36) Does the company have policies and procedures to 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 or use telemarketing, direct mail marketing, or other marketing (i.e. electronic mail) to the consumer? (NAIC Model 672 Section 13, NAIC Market Conduct Standard A Procedure A)

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 “C1D.Doc”

37) Has the company performed due diligence of sharing of health information with affiliated and non-affiliated third parties to determine if any sharing of health information exists that would require an authorization? (NAIC Model 672 Section 17)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide an explanation of any due diligence activities that were performed to determine whether an authorization was needed for sharing of health information relevant sample documents using the file name “C2A.Doc”

38) Has the licensee developed policies and procedures to secure 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 17B of the NAIC Model Regulation? (NAIC Model 672 Section 17(B), NAIC Market Conduct Standard E Procedure A)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide a copy of the policies for securing authorization using the file name “C2B.Doc”. If no authorization is required based upon due diligence activities, note accordingly.

39) Does the licensee's authorization form include "all" of the elements required by Article V of the NAIC Model Regulation #672? The elements include: (NAIC Model 672 Section 18, NAIC Market Conduct Standard E 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”

40) 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 Market Conduct Standard C, Procedure B, NAIC Model 672 Section 17)

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"

41) Did the licensee have policies and procedures in place so that non-public personal financial information is not disclosed outside the allowable exceptions without offering an opt-out? (NAIC Model 672 Section 11(A)(1), NAIC Market Conduct Standard A 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"

42) Has management developed policies and procedures for identifying non-public personal information to specifically identify what policies, procedures, or other operational controls exist to prevent non-public information from being shared with non-affiliated third parties, if the customer opts-out? (NAIC Market Conduct Standard C Procedure B)

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 "C3B.Doc"

43) 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 B Procedure J).

Yes \_\_\_\_\_  
No \_\_\_\_\_

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

44) 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? (NAIC Model 672 Section 14 (A)(1)(b), NAIC Market Conduct Standard D Procedure (A)(2) & Procedure C)

Yes \_\_\_\_\_

No \_\_\_\_\_

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

45) Has the licensee developed and implemented policies and procedures to ensure that information obtained from non-affiliated third parties not reused or re-disclosed for a purpose other than that is allowed pursuant to NAIC Model 672? (NAIC Model 672 Section 14, NAIC Market Conduct Standard D - Procedure (B))

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 "C6A.Doc"

46) Has the licensee developed a method for tracking, logging and analyzing privacy complaints? (NAIC Market Conduct Standard A, Procedure D)

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 "C7A.Doc"

47) Provide an explanation of the methodology for tracking or logging privacy complaints. Provide copies of any privacy related complaints and an explanation of the resolution of such complaints. (NAIC Market Conduct Standard A, Procedure D)

Please attach an explanation and/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "C8B.Doc"

### **Customer Option Preferences**

48) 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 C Procedure A)

Yes \_\_\_\_\_

No \_\_\_\_\_

D1A

49) 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 B Procedure A(8))

Yes \_\_\_\_\_  
No \_\_\_\_\_  
N/A \_\_\_\_\_

D1B

50) What was the process used by management for determining whether opt-out notices were necessary and did the process consider, if opt-out is offered, whether the licensee developed processes and controls to ensure that customers that have chosen to opt-out of such sharing have their information removed from customer lists prior to sharing? (NAIC Market Conduct Standard C, Procedure A)

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

51) 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 C Procedure D)

Please attach an explanation and any/or any relevant policies, as well as the index evidencing the existence of relevant procedures, using the file name "D2B.Doc"

52) 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"

53) What was the process used for ensuring the delivery of opt-out notices.

Please attach an explanation and any relevant documents using the file name "D2D.Doc"

54) 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 include:

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

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

- Does the licensee's privacy notice address how opt-out elections for joint policies will be handled? (NAIC 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 attach an explanation of the treatment of joint customers and/or any relevant documents using the file name "D3B.Doc"

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

57) 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"

58) 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 C 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 "D3E.Doc"

59) Has the licensee communicated consumers' and customers' opt-out elections to the agent of record, and communicated in a reasonable and timely manner with its producers with regard to the effect of opt-out on the agent's ability to share information about that consumer or customer? (NAIC Market Conduct Standard C Procedure F)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please attach an explanation of how opt-out elections are communicated to agents and producers and a sample copy of such communications that were sent using the file name "D3F.Doc"

60) 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 A Procedure C)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please attach an explanation of the controls in place to prevent discrimination against customers that have opted out and/or any relevant documents using the file name "D3G.Doc"

61) 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)(1)(a), NAIC Market Conduct Standard C Procedure E(1))

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 "D3H.Doc"

62) 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 C Procedure E(2) & E(3))

Yes \_\_\_\_\_

No \_\_\_\_\_

Please attach an explanation and/or relevant documents using the file name "D3I.Doc". Please provide a copy of the company's opt-out notice using the file name "D3J.Doc"

**Safeguarding of Customer Records**

63) Does the licensee have a formal information security policy defining the scope, objectives, risk assessment, roles and responsibilities relating to administrative, technical and physical safeguards? (NAIC Model 672 – 3, 4, 6, 7; Market Conduct Examination Standard F, Procedure C)

Yes \_\_\_\_\_

No \_\_\_\_\_

F1A

64) Does the formal information security policy include the following: (NAIC Model 672 – 4; Market Conduct Examination Standard F, Procedure C)

- Policies to insure 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?

Yes \_\_\_\_\_

No \_\_\_\_\_

F1B

Please provide relevant policies and the index evidencing the existence of relevant procedures pertaining to the safeguarding of customer or consumer records and information using the file name “F1C.Doc”

65) Was the information security program designed to meet the objectives of the Gramm-Leach-Bliley Act Standards for Safeguarding of Customer Information? (NAIC Model 672 – 1, 2, 3, 4, 5, 6, 7, 8, 9; Market Conduct Examination Standard F Procedures A, B, C)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and/or any relevant policies using the file name “F1D.Doc”.

66) Is the program formally documented to include:

- information security standards? (NAIC Model 672 – 3,4; Market Conduct Examination Standard F, Procedure A)
- policies and procedures? (NAIC Model 672 – 3, 4; Market Conduct Examination Standard A, Procedure A, Standard F, Procedures A and C)
- established baselines for security over operating systems and databases? (NAIC Model 672 – 3, 7, 9; Market Conduct Examination Standard F, Procedures A and C)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide a copy of the information security program using the file name “F1F.Doc”

67) Does the program address the IT organizational structure? (NAIC Model 672 – 3, 4; Market Conduct Examination Standard F, Procedure A)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide organization charts showing where responsibility for information security resides in relation to the IT department and other control and administration departments within the company using the file name “F1J.Doc”

68) Has specific responsibility been assigned for creating, implementing and maintaining the program? (NAIC Model 672 – 3, 5, 8, 9; Market Conduct Examination Standard F, Procedure A and C)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and job description of who is responsible for implementing the information security program within the company using the file name “F1K.Doc”

69) Does the program address information security awareness and training? (NAIC Model 672 – 3, 7; Market Conduct Examination Standard F, Procedure A)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation of the information security awareness and training program within the company and any sample materials, policies, or training guides using the file name “F1L.Doc”

70) Has the program been designed in accordance with regulatory guidance? (NAIC Market Conduct Examination Standard A, Procedure A)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide reference to the regulation(s) (GLBA, NAIC Model Laws, state statutes or regulations, other model laws) for which the security program was designed to comply using the file name “F1M.Doc”

71) Has a risk assessment been documented that identifies systems involved in the creation, processing and storing of customer information, and does it identify and assess 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: [\(NAIC Model 672 – 6; Market Conduct Examination Standard F, Procedure C\)](#)

- Whether the assessment addresses all potential external (Internet and Dial-up) network remote access points?
- Whether the assessment addresses the inventory of systems containing customer information, including platforms on which these systems reside?
- Whether the assessment addresses all extranet access points or all other methods of transmitting data outside the company (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 systems hardware?
- Whether the assessment addresses storage points for hard copy documentation?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please attach a copy of the risk assessment using the file name “F2A.Doc”. Please provide an explanation of risk assessment activities that have been undertaken and documentation of information security risk assessment activities using the file name “F2B.Doc”

72) Has the licensee addressed the likelihood and potential damage of the threats noted in the risk assessment and did the licensee identify the likelihood of occurrence and potential threat based on the sensitivity of customer information? [\(NAIC Model 672 – 6; Market Conduct Examination Standard F, Procedure C\)](#)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide the vulnerability assessment, if different from the risk assessment, that takes into account the risks that have been identified, the likelihood of occurrence and potential threat based on the sensitivity of customer information using the file name “F2C.Doc”

73) Does the risk assessment consider confidentiality and integrity of customer information whether it is being stored, processed or transmitted? [\(NAIC Model 672 – 6; Market Conduct Examination Standard F, Procedures B and C\)](#)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please describe how the risk assessment takes into account the location of sensitive customer information using the file name “F2E.Doc”

74) Has the licensee considered the sensitivity and classification of information in assessing the risk of customer data? (NAIC Model 672 – 7; Market Conduct Examination Standard F, Procedure B)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide an explanation of any data classification strategies, as well as any relevant policies, using the file name “F2G.Doc”

75) Has an assessment of the data classification strategies, policies or procedures and related controls for sensitive information been formally conducted and documented, and has 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 on: (NAIC Model 672 – 6, 7; Market Conduct Examination Standard F, Procedures B and C)

- internal/external network access points?
- logical access to information systems included in internal audit reviews?
- physical access secured server rooms?

Yes \_\_\_\_\_  
No \_\_\_\_\_

Provide an explanation of any internal or external activities that have been undertaken to assess the effectiveness of the information security program and relevant results, such as any reports issued, using the file name “F2I.Doc”

76) Does the licensee re-perform a security assessment when new hardware or software is deployed on systems maintaining customer information? (NAIC Model 672 – 9)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide an explanation and results of any recent security assessments performed as a result of the installation of new hardware or software using the file name “F2K.Doc”

77) Does the company monitor, evaluate and adjust risk assessments based on changes in technology or the sensitivity of the information? (NAIC Model 672 – 7, 9; Market Conduct Examination Standard F, Procedure B)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide an explanation of any planned risk assessment activities that will take place over the next 12 to 24 months that will re-assess all risk areas and all levels of risk using the file name “F2M.Doc”

78) Do the licensee's policies and procedures address access controls on systems maintaining customer information and does it contain the following:

- Formal procedures to ensure only authorized individuals are granted access to data as needed? (NAIC Model 672 –3, 4; Market Conduct Examination Standard F, 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? (NAIC Model 672 – 7, 9; Market Conduct Examination Standard F, Procedures A and C)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and 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”

79) Are user access rights to customer information are determined and granted to ensure: (NAIC Model 672 – 3; Market Conduct Examination Standard F, Procedure B)

- Granting of access occurs on an individual or group basis?
- Validation of customer authentication occurs (ex. DOB, mothers maiden name)?
- Review of user access control is performed periodically to ensure that user access is commensurate with job function?
- Authorization for new system user accounts?
- Termination and job change procedures are enforced?
- Identification and removal of inactive user accounts occurs?

Please provide an explanation and 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 “F3C.Doc”

80) Do the security policies and procedures address password controls at the network, operating systems, application and database levels and do they include: (NAIC Model 672 – 3; Market Conduct Examination Standard F, 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?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and reports or other materials that show password controls exist and are maintained at the network, operating system and database levels, as well as any relevant policies and the index evidencing the existence of procedures, using the file name “F3F.Doc”

81) Do the security policies and procedures address dial-up access and do they include: (NAIC Model 672 – 3, 4, 7(A), 9; Market Conduct Examination Standard A, Procedure A and Standard F, 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)?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and 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 “F3H.Doc”

82) Do database controls exist to authenticate users, achieve data confidentiality (i.e. through encryption), and maintain data integrity for databases supporting customer related applications? (NAIC Model 672 – 3, 4; Market Conduct Examination Standard F)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and 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 "F3J.Doc"

83) Are physical security controls incorporated in the information security policies and procedures and do they include: (NAIC Model 672 – 3, 4; Market Conduct Examination Standard A, Procedure A and Standard F, 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 personnel, surveillance cameras and access logs?
- Policies requiring the locking of file drawers and security cages for paper forms containing customer information?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and 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 "F3L.Doc"

84) Do controls exist over external storage vendors used for archiving customer information and are there a list of these vendors used to store records, which include: (NAIC Model 672 – 3, 4, 8 (A, B); Market Conduct Examination Standard A, Procedure A and Standard F, 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?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and 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 "F3N.Doc"

85) Do the external transmission policies and procedures that address customer information include: (NAIC Model 672 – 6; Market Conduct Examination Standards F)

- 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, sensitivity of information is understood and communicated appropriately and safeguards are in place?
- Policies governing the type of security used to protect against unauthorized access (encryption, frame relay, other)?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and 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 "F3P.Doc"

86) What forms and use of data encryption products and algorithms are being employed by the company (e.g. SSL 128 Secure Data)? [\(NAIC Model 672 – 3, 4; Market Conduct Examination Standard F\)](#)

Please provide an explanation and reports or other materials that list forms and use of data encryption products/algorithms in use using the file name "F3Q.Doc"

87) Is "live production" customer information used in a test environment and has a business case been developed for the need to use "live production" customer information? [\(NAIC Model 672 – 3, 4 \(A, B, C\), 6\(A, B, C\); Market Conduct Examination Standard A, Procedure A\)](#)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide 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 "F3R.Doc"

88) Do formal policies and procedures exist to assess the impact of information security changes to systems containing customer information? [\(NAIC Model 672 – 3, 4 \(A, B, C\), 9; Market Conduct Examination Standard A, Procedure A\)](#)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide 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 "F3T.Doc"

89) Have rules for customer authentication been defined by the company and implemented to support the corporate privacy statement? [\(NAIC Model 672 – 3, 4 \(A, B, C\), 9; Market Conduct Examination Standard F, Procedure A\)](#)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide 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 "F3V.Doc"

90) Do 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 and they address such control items as: [\(NAIC Model 672 – 3, 4, 6, 7 \(A\), 9; Market Conduct Examination Standard A, Procedures A and B and Standard F\)](#)

- 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?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide 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 "F3X.Doc"

91) Do the policies and procedures address monitoring and detection of actual and attempted attacks on customer information systems, networks, storage devices and do they include: [\(NAIC Model 672 – 6, 7; Market Conduct Examination Standard F\)](#)

- Procedures governing the frequency with which monitoring is conducted and for what customer information systems?
- Procedures governing the used 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 detailed to their criticality (general network penetration or unauthorized access to database systems maintaining customer information)?
- 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 their logging and reporting 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 how often are they reviewed?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and reports or other materials to illustrate that appropriate monitoring of actual and attempted attacks on customer information systems takes place, periodically reviewed and appropriate action is taken, as well as relevant policies and the index evidencing the existence of relevant procedures, using the file name "F3Z.Doc"

92) To whom are the information system attack events reported to and are they responsible for determining a formal response, which addresses the following: (NAIC Model 672 – 7; Market Conduct Examination Standard F, Procedures A and B)

- Process to documented escalation response to respond to unauthorized access attempts to customer information?
- Process to address recent unauthorized access attempts?
- Process to address Actions to be taken when a suspected intrusion occurs?
- Process to documented action steps?
- Process to ensure regulatory/law enforcement agencies are informed when intrusion attempts occur or when customer information has been compromised?
- Process to ensure individual responsibility exists to inform regulatory/law enforcement agencies?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and relevant policies to illustrate that appropriate event response and escalation of actual and attempted attacks on customer information systems takes place, are periodically reviewed and appropriate action is taken, using the file name "F3bb.Doc"

93) Are all systems located in data centers maintain adequate controls to protect against environmental hazards? (NAIC Model 672 – 3, 4; Market Conduct Examination Standard F, Procedures A and B)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please describe the types of controls in place to protect against environmental risks listed below, using the file name "F3dd.Doc"

- Control pertaining to fire
- Control pertaining to water damage
- Control pertaining to temperature
- Control pertaining to power surges/outages

94) Does a formal business continuity program exist, including backup of systems/files containing customer information, testing retrieval of information from backup media and does this program incorporate for every application: (NAIC Model 672 – 3 6; Market Conduct Examination Standard F)

- Requirement for a written disaster recovery plan?
- Requirement for an operational recovery facility?
- Requirement for documenting backup methods used (tape, mirroring, vaulting)?
- Requirement for documenting back up frequency and number of set procedures on manually duplicating data during recovery?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide the index evidencing the existence of relevant business continuity/disaster recovery plan components and evidence of last test results, using the file name “F3ff.Doc”

95) Has the licensee established a security training program for all employees that have access to customer information and does this program include: (NAIC Model 672 – 3, 7(B); Market Conduct Examination Standard F, Procedures A and C)

- Procedures addressing the content of existing training program?
- Procedures addressing who conducts training?
- Procedures addressing who attends training?
- Procedures addressing frequency of training?
- Procedures addressing content, i.e., policies and procedures for safeguarding customer information, how to detect fraudulent activity, how to prevent unauthorized access, password policies, and physical access policies, among others?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and 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 “F3hh.Doc”

96) Has an independent third party been identified to test or review the key controls, systems and procedures of the information security program, which include: (NAIC Model 672 – 3, 7 (C); Market Conduct Examination Standard F)

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

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation and reports or other materials evidencing the assignment of an independent third party to test or review key controls, systems and procedures of the information security program, using the file name “F3hi.Doc”

97) Has the licensee’s board or management designated an individual to act as a liaison with the Corporate Information Security Group to facilitate the administering of the information security program? (NAIC Model 672 – 3; Market Conduct Examination Standard F, Procedure A)

Yes \_\_\_\_\_

No \_\_\_\_\_

F4B

98) Have policies and procedures been documented that 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...? (NAIC Model 672 – 3, 9; Market Conduct Examination Standard A, Procedure A)

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide an explanation or other materials that show adjustments to the corporate information security program, as well as any relevant policies and the index evidencing the existence of relevant procedures, using the file name “F4D.Doc”

99) Has the Licensee developed a process for performing appropriate due diligence in selecting service providers? Does this process involve the following elements: (NAIC Model 672 – 8 (A, B); Market Conduct Examination Standard D and Standard F, Procedure B)

- Provisions for due diligence performed for all service providers?
- Provisions for due diligence performed based upon a formal risk assessment?
- Provisions for the assessment of a service providers privacy policies and practice?
- Provisions for the assessment of a service providers security policies and practices?
- Provisions for the assessment of a service provider’s general business reputation?

Yes \_\_\_\_\_

No \_\_\_\_\_

Please provide a summary of your due diligence program that addresses the elements as noted. Attach relevant documentation that supports the existence of the program. Include relevant policies and the index evidencing the existence of relevant procedures, using the file name “F4E.Doc”

100) Does the licensee require service providers to implement appropriate measures designed to meet the objectives of the NAIC Standards for Safeguarding of Customer Information? (NAIC Model 672 – 8; Market Conduct Examination Standard D)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide a summary of the 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 “F4F.Doc”

101) Does the licensee take appropriate steps, where indicated by their risk assessment, to confirm that service providers have implemented appropriate steps to safeguard non-public personal-information? (NAIC Model 672 – 8 (B); Market Conduct Examination Standard D and Standard F, Procedure B)

Yes \_\_\_\_\_  
No \_\_\_\_\_

Please provide a summary of the process your organization has in place to ensure that service providers have implemented appropriate safeguards. Include 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 “F4G.Doc”