Anthony A. Williams
Mayor

Lawrence H. Mirel
Commissioner

Market Conduct Examination

Government of the District of Columbia
Department of Insurance, Securities, and Banking

(NAIC ACCREDITED)

Government of the District of Columbia

Department of Insurance, Securities and Banking

Lawrence H. Mirel
Commissioner

July 8, 2005

I, Lawrence H. Mirel, Commissioner of Insurance, Securities and Banking of the District of Columbia, hereby certify that I have compared the annexed copy of the

LIMITED SCOPE MARKET CONDUCT EXAMINATION REPORT

ON THE

PRIVACY PRACTICES FOR THE

AMERITAS ACACIA GROUP

July 6, 2005

With the original on file in this Department and the same is a correct transcript there from, and of the whole of said original.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed the seal of this Department, at the City of Washington, the day and year first written

_____

Lawrence H. Mirel
Commissioner of Insurance, Securities and Banking

TABLE OF CONTENTS

SALUTATION

July 6, 2005

Honorable Lawrence H. Mirel, Commissioner
Department of Insurance and Securities Regulation
District of Columbia
810 First Street Northeast, Suite 701
Washington, DC 20002

Dear Mr. Commissioner:

In accordance with your instructions and pursuant to District of Columbia Official Code 31-1402 (a), 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:

AMERITAS ACACIA 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 the District of Columbia 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. 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 the District of Columbia's assessment of the insurance privacy practices of the Ameritas Acacia Companies, 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:

09377 Financial Benefit Life Ins Co	98213	AmerUs Group	KS
07407 IL Annuity and Ins Co	71692	AmerUs Group	KS
06467 Bankers Life Ins Co of NY	63932	AmerUs Group	NY
06552 Indianapolis Life Ins Co	64645	AmerUs Group	IN
06199 AmerUs Life Insurance Company	61689	AmerUs Group	IA
06075 American Investors Life Ins Co	60631	AmerUs Group	KS

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

NAIC Model Rule # 672	
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

NAIC Model Rule # 673	
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
1982 Model Rule	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.

	Questionnaire Reference	Finding
NAIC Model Rule # 672 – No Findings Noted.		

NAIC Model Rule # 673 – No Findings Noted.

1982 Model Rule – No Findings Noted.

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,

William F. McCune, Examiner-In-Charge
Supervisory Market Conduct Examiner Manager
DC Department of Insurance, Securities and Banking

APPENDIX

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 "B 1 .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 "B 1 B .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 "B 1 C .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 "B 1D.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 "B 1E.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 "B 1F.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? (NA1C 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 _____ B31

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 "B30.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"

<u>Policies and Procedures</u>

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 “Cl B .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 webs ite, 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 1 0(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 forjoint policyholders in company systems and:

- Does the licensee's privacy notice address how opt-out elections forjoint 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 "F 1 .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 “F 1 A.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 “F lB .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 “F 1 C .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-LeachBliley 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 “F 1 D.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 "Fl F.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 "F 1 G.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 "F 1H.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 accesspoint~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 comnpany 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-LeachBliley 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: (GrammLeach-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 Examnination 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-LeachBliley Act Section 501(a) & (b), Standards for Safeguarding Customner Information Model Regulation — 3, 4, 8 (A, B); Market Conduct Examnination 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"F30.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 addrôssing 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- au-dit, 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"