FREQUENTLY ASKED QUESTIONS (FAQs) ON DIVISION 1.4

The FAQs are divided into three segments: Part I provides guidance on how Financial Institutions should respond to specific questions on the Management Certification form; Part II provides guidance on questions that have been raised by Financial Institutions; and, Part III provides a list of statutory exemptions for more common circumstances in which Financial Institutions may share nonpublic personal information without first providing notices to the affected consumers.

PART I – HOW TO COMPLETE THE FORM

In completing the Management Certification form certain issues have arisen in answering certain questions. The following addresses two questions that have been a challenge for most licensees:

In completing Question #1, consider the following:

1. Does the Financial Institution share, or intend to share, nonpublic personal information with nonaffiliated third parties? *[FC 4052.5]* If the answer is "yes", please continue. If the answer is "no" please skip to question #2 below.

Many licensees have responded "No" to this question even though the licensees do share nonpublic personal information with nonaffiliated third parties. Examples of the sharing include: check printing vendors, Information Systems vendors, Trust Accounting System vendors, etc. Although these vendors are covered by the statutory exemptions contained in FC 4056, the response to this part of question #1 should be "Yes" unless the licensee performs all of the above-mentioned activities in-house.

1.a. Using the attached Schedule of Nonaffiliates, please provide a list of <u>all</u> nonaffiliated third parties and detail the intended purpose for the sharing of such information.

List each vendor with whom the licensee shares nonpublic personal information and give the reason for sharing.

Example response: "The (<u>name of Financial Institution</u>) contracts with <u>ABC Check Printers</u> to provide printed checks that were ordered by the customer. Please see the attached service agreement/contract with the vendor."

1.b. Did the Financial Institution obtain the explicit prior consent of the consumer to whom the nonpublic personal information relates prior to sharing such information?

If the answer is "no", please cite and explain the statutory exemption, or any other statutory authority, under which your judgment not to seek the "opt-in" is authorized using the attached Schedule of Nonaffiliates. Refer to FAQ Part III –

Statutory Exemptions for a list of common circumstances in which a financial institution may share nonpublic personal information.

If the licensee did not provide a notice and obtain explicit prior consent of the consumer, the response should be "No". The explanation of the statutory exemption for the above example involving the check printers should be, "Statutory exemption under FC Section 4056(b)(1)."

1.c. How does the Financial Institution obtain the explicit prior consent of the consumer?

The licensee should indicate in its response whether a notice is mailed or emailed to its customers. Or, following the example in 1.a. and 1.b. above, the response to question 1.c. should be "Not applicable." since the sharing of information with the check printers is specifically exempted by the statute.

1.d. Please provide a copy of the consent form(s), and indicate the date(s) when the consent form(s) was approved and who approved the form(s).

If the licensee does in fact share nonpublic personal information with a nonaffiliated third party vendor under circumstances that are not exempted by the statute, the licensee's response to this question should include: (1) a copy of the notice and consent form; (2) the date when the consent form was revised and approved; and, (3) the individual/committee that approved the form (i.e., the board of directors, the compliance committee, etc.).

An example question from a licensee on how a Financial Institution should respond to the Management Certification form Question #1:

The Financial Institution shares nonpublic information with its third party vendors such as: a) data processor, b) item processor, c) ATM processor, d) Internet banking provider e) etc. However, all of these sharing relationships exempt the Bank from acquiring "explicit prior consent of the consumer" under the provisions of Sections 4053, 4054, & 4056. Should the Financial Institution answer "Yes" to #1., and in question #1.a. list all the vendors including the IRS, Franchise Tax Board, and other authorized entities/parties with which the Financial Institution shares information? In question #1.b. reply "No" and cite FC Sections 4056? In question #1.c. reply "Not applicable"? In question #1.d. reply "Not applicable"? Or should the Financial Institution reply "No" because it does not share information with third parties under circumstances that would require the Financial Institution to obtain "explicit prior consent"?

DFPI Response to the Example Question:

In the scenario described above, the response to question 1.a. should be "Yes". The response to question 1.b. should indicate the applicable Division 1.4 exceptions that

permit the institution to share nonpublic personal information with each nonaffiliated third party. For example, the Financial Institution lists the following nonaffiliated third party vendors with whom it shares consumers' nonpublic personal information:

a) data processor
b) item processor
c) ATM processor
d) Internet banking provider

The response to question 1.b. should indicate that sharing of information with each of the above vendors would be permitted by the exemption found in Section 4056(b)(1) because the vendors are required to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with servicing or processing a financial product or service requested or authorized by the consumer, or in connection with maintaining or servicing the consumer's account with the Financial Institution. Sharing of information with other nonaffiliated third parties may be exempted by other subsections of 4056.

The Financial Institution should clearly understand which exemption applies to each nonaffiliated third party; and be able to explain the applicability of the exemption for each. Thus, the Financial Institution should not reply "No" to question 1.a. The intent of this question is to determine that each licensee understands the exemption that would apply to its sharing of nonpublic personal information with nonaffiliated third parties.

Based on the above responses to 1.a. and 1.b., the responses to 1.c. and 1.d. would be "Not applicable".

In addressing Question #6, consider the following:

6. How does the board assess sufficiency of policy, procedures, information systems, and other arrangements in place to control financial privacy risk? Please indicate the date when the board or a designated committee approved the policy and procedures for the Financial Institution's compliance with Division 1.4.

The licensee's response should include the following:

- *Frequency of the board's review of policies and procedures related to privacy and information systems. For example, "The board approves the privacy policy on an annual basis."*

- *Date of when the board last approved the licensee's Division 1.4 privacy policy and procedures. For example, "The board approved the privacy policy on MM/DD/YY."*

Even though a licensee may choose to not share nonpublic personal information of its consumers with either affiliates and/or nonaffiliated third parties, the licensee's philosophy of such practice should be reflected in the formal policies.

PART II – QUESTIONS AND ANSWERS

Question 1: When should an institution draft "Opt-in" or "Opt-out" Notices?

Management's response to the Management Certification indicates that management does not currently, nor do they plan on, sharing non-public personal information with non-affiliates. Should the institution be excluded from drafting "opt-in" or "opt-out" notices?

If the institution is not sharing information, there would be no need to draft the notices.

Question 2: Does "Consumer" as defined in FC Section 4052(f) include a trustor of a personal trust?

The definition of "Consumer" does not appear to address the trustor of a personal trust. Part (4) only addresses the beneficiary of a trust. Part (5) sounds like the person who sets up an employee benefit plan or group policy holder. Thus, would a trustor of a personal trust be considered a "consumer" of a Financial Institution since such person is not specifically exempted in FC 4052(f)?

A trustor is not covered by either part (4) or (5). The trustor should be considered a consumer since he/she is availing him/herself of the services of the Financial Institution.

Question 3: Does Division 1.4 apply to Foreign Banking Organizations (FBOs)?

Division 1.4 applies to FBOs. Division 1.4 defines "Financial Institution" to mean "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 of the United States Code and doing business in this state." Section 1843(k) is located in the Bank Holding Company Act (which is under the Federal Reserve Bank's jurisdiction). Section 1843(k)(4) defines "Activities that are financial in nature," and it is a broad definition that includes "lending, exchanging, transferring, investing for others, or safeguarding money or securities." That definition also allows the Federal Reserve Bank to interpret other activities as financial in nature. Since the activities of FBOs undoubtedly involve lending, they are considered Financial Institutions under Division 1.4.

Question 4: Is a Financial Institution required to have customers "opt-in" on information given to vendors for normal business operations?

There are exemptions to the notice requirements that could be construed as normal business operations (e.g., data processing, printing services, etc.) and other exemptions that exist because the normal business operations are authorized by the customer at some point. These exemptions can be found in Section 4056. If these "normal business operations" do not fit into a statutory exempted sharing relationship, but are transacted under a joint marketing agreement, then the Financial Institution would also not have to provide the "opt-in" notice; however, they would have to provide an "opt-out" notice. The Financial Institution should be able to provide documented support as to why they

feel they don't need to provide the "opt-in" notice for any sharing of nonpublic personal information with nonaffiliated third parties.

PART III – STATUTORY EXEMPTIONS

This segment lists the statutory exemptions presented in Financial Code Section 4056. The list is also included as an Addendum to the Management Certification. This segment is not meant as a definitive interpretation of the cited exemptions. **Financial Institutions are advised to consult with their own legal counsel and the Financial Code regarding the details of these exemptions** as the applicability of many of them is dependent on satisfying certain factors, which will not be discussed herein. In addition to the exemptions listed here, there are other exemptions available. **Financial Institutions are advised to consult with their legal counsel as to the availability of such other exemptions**.

The following is an overview of the more common circumstances in which a financial institution may release nonpublic personal information without first providing notices to the affected consumers:

(1) The nonpublic personal information is necessary to maintain a consumer's account or to effect a transaction requested by the consumer. (Financial Code ("FC") 4056(b)(1).)

(2) The nonpublic personal information is released at the direction of the consumer. (FC 4056(b)(2).)

(3) The nonpublic personal information is released to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product. (FC 4056(b)(3)(A).)

(4) The nonpublic personal information is released to protect against fraud, identity theft, unauthorized transactions, claims, or other liability. (FC 4056(b)(3)(B).)

(5) The nonpublic personal information is released for required institutional risk control or for resolving customer disputes or inquiries. (FC 4056(b)(3)(C).)

(6) The nonpublic personal information is released for purposes of debt collection. (FC 4056(b)(3)(D).)

(7) The nonpublic personal information is released to persons acting in a fiduciary or representative capacity on behalf of the consumer. (FC 4056(b)(3)(E).)

(8) The nonpublic personal information is released to provide information to insurance rate advisory organizations, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors. (FC 4056(b)(4).)

(9) The nonpublic personal information is released to law enforcement agencies, including federal and state regulators. (FC 4056(b)(5).)

(10) The nonpublic personal information is released in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of the business or unit. (FC 4056(b)(6).)

(11) The nonpublic personal information is released to comply with federal, state, or local laws, rules, regulatory investigations, subpoenas, or other purposes as authorized by law. (FC 4056(b)(7).)

(12) The nonpublic personal information is released under a written contract to an affiliate or a nonaffiliated third party in order for the affiliate or nonaffiliated third party to perform business or professional services, such as printing, mailing services, data processing, on behalf of the financial institution. (FC 4056(b)(9).)

(13) The nonpublic personal information is released to a licensed real estate appraiser, and the information is compiled strictly to complete other real estate appraisals and is not used for any other purpose. (FC 4056(b)(11).)

(14) The nonpublic personal information is released as required by the USA Patriot Act. (FC 4056(b)(12).)

(15) The nonpublic personal information is released to a consumer reporting agency pursuant to the Fair Credit Reporting Act. (FC 4056(b)(13).)

(16) The nonpublic personal information is released in connection with a written agreement between a consumer and a broker-dealer or an investment adviser to provide investment management services, and the nonpublic personal information is released for the sole purpose of providing the products and services covered by that agreement. (FC 4056(b)(14).)

(17) The nonpublic personal information is disclosed, in the ordinary course of business, in order for insurance brokers to provide quotes to consumers seeking price quotes on insurance products and services. (FC 4056.5(b).)

(18) The nonpublic personal information from an insurer or its affiliates is disclosed or shared with an exclusive agent, who may not share nonpublic personal information with any insurer other than the insurer with whom the agent has a contractual or employment relationship. An insurer or its affiliates do not disclose or share nonpublic personal information with exclusive agents merely because information is maintained in common information systems or databases, and exclusive agents of the insurer or its affiliates have access to those common information systems or databases, provided that where a consumer has exercised his or her rights to prohibit disclosure pursuant to this division, nonpublic personal information is not further disclosed or used by an exclusive agent except as permitted by this division. (FC 4056.5(c)(1).)

(19) The nonpublic personal information is shared between a financial institution and its wholly owned financial institution subsidiaries; among financial institutions that are each wholly owned by the same financial institution; among financial institutions that are wholly owned by the same holding company; or among the insurance and management entities of a single insurance holding company system consisting of one or more reciprocal insurance exchanges which has a single corporation or its wholly owned subsidiaries providing management services to the reciprocal insurance exchanges. (FC 4053(c).)