

Prepared for the ADAI by:

HARRISON & MOBERLY, LLP

William N. Ivers

wivers@h-mlaw.com

David I. Rubin

drubin@h-mlaw.com

HARRISON & MOBERLY, LLP

10 W. Market Street

Suite 700

Indianapolis, IN 46204

(317) 639-4511

(317) 639-9565

Exhibits for your use and reference:

- A. Corporate Policy –Mission
- B. Designing and Drafting Checklist
- C. Sample ITPP with Red Flags List
- D. Board Approval
- E. Training Outline
- F. Compliance Officer Report
- G. Banking Industry
Know your Customer Rules

Corporate Policy – Mission Statement

ABC MOTORS in compliance with the purposes of state and federal law states that it is our mission to establish policies and procedures designed to detect, deter and defend against the threat of identity theft. In furtherance of this mission ABC Motors appoints a Compliance Officer to design, draft, implement and monitor an Identity Theft Prevention Program (ITPP). The Compliance Officer shall present the ITPP to the Board of Directors for approval. Following approval, all applicable employees shall be trained and shall comply with the terms of the ITPP on or before November 1, 2008..

Designing and Drafting Checklist

ITPP Requirements:

- In writing;
- Responsible Person appointed (Senior level manager);
- Analysis and Identification of Covered Accounts;
- Identification of Relevant Red Flags;
- Customer Identification and Verification;
- Response Procedures for Red Flags suggesting ID Theft;
- Training for employees;
- Oversight of service providers;
- Reporting and updating of ITPP;
- Approved by board of directors or committee

Sample ITPP with Red Flags List

See attached

Board Approval of ITPP

APPROVAL OF IDENTITY THEFT PREVENTION PROGRAM

By signing below, the undersigned, constituting all of the members of Dealership's [board of directors, appropriate committee of board of directors, managers, or members], acknowledge the approval of the Dealership's Identity Theft Prevention Program and the appointment of the Program's Compliance Officer and Program Coordinator(s).

_____ [name]

_____ [name]

_____ [name]

_____ [name]

_____ [name]

Training Outline

- A. Review Written ITPP;
- B. Obtain Customer Information;
- C. Review Information (Red Flags Searching);
- D. Investigate, Evaluate, and Decide if ID Theft is present when red Flag is detected;
- E. Respond to Situation based on decision (Complete deal or reject deal); and
- F. If deal rejected for ID theft (Notify CRAs, customer and possibly law enforcement).

Compliance Officer ITPP Report

The undersigned Compliance Officer, in conformance with the Dealerships Identity Theft Prevention Program (ITPP), hereby submits this Report to the Dealerships Board of Directors as follows:

1. Adoption and implementation of ITPP and any amendments thereto.

Pursuant to the authorization and approval of the dealership board of directors, the ITPP was implemented and became effective on November 1, 2008. Pursuant to the terms of the ITPP all dealership employees having duties and involvement with the opening and maintaining of covered accounts were provided a copy of and training concerning the ITPP and signed acknowledgements agreeing to comply with the ITPP.

Additional comments regarding updates or amendments: _____

2. Incidents of Identity Theft, if any: (list all incidents since last report or state none) _____

3. Compliance with Regulations and amendments thereto.

The Compliance Officer or a designated assistant has complied with the requirements of the Red Flags Rules and has reviewed the rules to determine if any changes have been made by the Federal Trade Commission or if any additional guidance has been provided regarding the ITPP. The most recent guidance from the FTC, if any, is attached hereto and incorporated herein by reference. The dealership's ITPP has been updated, as needed, to incorporate such guidance.

4. Service Providers. The dealerships Service Providers involved with covered accounts include the following: _____

These providers all have agreed to implement and follow the requirements of an ITPP consistent with the dealerships ITPP and have reported _____ (state number) incidents of identity theft. Based upon the service providers report the dealership's ITPP (does/does not) require amendment.

5. Compliance Officers opinion and Recommendations regarding the ITPP. The ITPP has worked effectively since the implementation of the ITPP or the date of the Compliance Officer's previous report. At present no additional amendments or modifications of the ITPP are necessary. [NOTE: If amendments are needed list what and why.]

6. Other matters: If any other matters pertinent to the ITPP are need to be presented to the board, provide a description in the following spaces. If more room is needed attach additional pages.

Respectfully submitted,

Signed: _____

Printed: _____

Date: _____

Title: Compliance Officer

BANKING INDUSTRY Know your Customer Rule

Title 31, Volume 1]

[Revised as of July 1, 2003]

From the U.S. Government Printing Office via GPO Access

[CITE: 31CFR103.121]

[Page 405-409]

TITLE 31--MONEY AND FINANCE: TREASURY

DEPARTMENT OF THE TREASURY

PART 103--FINANCIAL RECORDKEEPING AND REPORTING OF CURRENCY AND FOREIGN
TRANSACTIONS--Table of Contents

Subpart I--Anti-Money Laundering Programs

Sec. 103.121 **Customer Identification Programs for banks**, savings associations, credit unions, and certain non-Federally regulated banks.

(a) Definitions. For purposes of this section:

(1)(i) **Account** means a formal banking relationship established to provide or engage in services, dealings, or other financial transactions

including a deposit account, a transaction or asset account, a credit account, or other extension of credit. Account also includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian, and trust services.

(ii) Account does not include:

(A) A product or service where a formal banking relationship is not established with a person, such as check-cashing, wire transfer, or sale of a check or money order;

(B) An account that the bank acquires through an acquisition, merger, purchase of assets, or assumption of liabilities; or

(C) An account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

(2) **Bank** means:

(i) A bank, as that term is defined in Sec. 103.11(c), that is subject to regulation by a Federal functional regulator; and

(ii) A credit union, private bank, and trust company, as set forth in Sec. 103.11(c), that does not have a Federal functional regulator.

(3)(i) **Customer** means:

(A) A person that opens a new account; and

(B) An individual who opens a new account for:

(1) An individual who lacks legal capacity, such as a minor; or

(2) An entity that is not a legal person, such as a civic club.

(ii) Customer does not include:

(A) A financial institution regulated by a Federal functional regulator or a bank regulated by a state bank regulator;

(B) A person described in Sec. 103.22(d)(2)(ii) through (iv); or

(C) A person that has an existing account with the bank, provided that the bank has a reasonable belief that it knows the true identity of the person.

(4) **Federal functional regulator** is defined at Sec. 103.120(a)(2).

(5) **Financial institution** is defined at 31 U.S.C. 5312(a)(2) and (c)(1).

(6) **Taxpayer identification number** is defined by section 6109 of the Internal Revenue Code of 1986 (26 U.S.C. 6109) and the Internal Revenue Service regulations implementing that section (e.g., social security number or employer identification number).

(7) **U.S. person** means:

(i) A United States citizen; or

(ii) A person other than an individual (such as a corporation, partnership, or trust), that is established or organized under the laws of a State or the United States.

(8) **Non-U.S. person** means a person that is not a U.S. person.

(b) **Customer Identification Program: minimum requirements—**

(1) **In general.** A bank must implement a written Customer Identification Program (CIP) appropriate for its size and type of business that, at a minimum, includes each of the requirements of paragraphs (b)(1) through (5) of this section. If a bank is required to have an anti-money laundering compliance program under the regulations implementing 31 U.S.C. 5318(h), 12 U.S.C. 1818(s), or 12 U.S.C. 1786(q)(1), then the CIP must be a part of the anti-money laundering compliance program. Until such time as credit unions, private banks, and trust companies without a Federal functional regulator are subject to such a program, their CIPs must be approved by their boards of directors.

(2) **Identity verification procedures.** The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer. These procedures must be based on the bank's assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying information available, and the bank's size, location, and customer base. At a minimum, these procedures must contain the elements described in this paragraph (b)(2).

(i) **Customer information required--(A)** In general. The CIP must contain procedures for opening an account that specify the identifying information that will be obtained from each customer. Except as permitted by paragraphs (b)(2)(i)(B) and (C) of this section, the bank must obtain, at a minimum, the following information from the customer prior to opening an account:

(1) Name;

(2) Date of birth, for an individual;

(3) Address, which shall be:

(i) For an individual, a residential or business street address;

(ii) For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of next of kin or of another contact individual; or

(iii) For a person other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location; and

- (4) Identification number, which shall be:
- (i) For a U.S. person, a taxpayer identification number; or
 - (ii) For a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

Note to paragraph (b)(2)(i)(A)(4)(ii):

When opening an account for a foreign business or enterprise that does not have an identification number, the bank must request alternative government-issued documentation certifying the existence of the business or enterprise.

(B) Exception for persons applying for a taxpayer identification number. Instead of obtaining a taxpayer identification number from a customer prior to opening the account, the CIP may include procedures for opening an account for a customer that has applied for, but has not received, a taxpayer identification number. In this case, the CIP must include procedures to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

(C) Credit card accounts. In connection with a customer who opens a credit card account, a bank may obtain the identifying information about

a customer required under paragraph (b)(2)(i)(A) by acquiring it from a third-party source prior to extending credit to the customer.

(ii) Customer verification. The CIP must contain procedures for verifying the identity of the customer, using information obtained in accordance with paragraph (b)(2)(i) of this section, within a reasonable time after the account is opened. The procedures must describe when the bank will use documents, non-documentary methods, or a combination of both methods as described in this paragraph (b)(2)(ii).

(A) Verification through documents. For a bank relying on documents, the CIP must contain procedures that set forth the documents that the bank will use. These documents may include:

- (1) For an individual, unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- (2) For a person other than an individual (such as a corporation, partnership, or trust), documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument.

(B) Verification through non-documentary methods. For a bank relying on non-documentary methods, the CIP must contain procedures that describe the non-documentary methods the bank will use.

- (1) These methods may include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement.

- (2) The bank's non-documentary procedures must address situations where an individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the bank is not familiar with the documents presented; the account is opened without obtaining documents; the customer opens the account without appearing in person at the bank; and where the bank is otherwise presented with circumstances that increase the risk that the bank will be unable to verify the true identity of a customer through documents.

(C) **Additional verification for certain customers.** The CIP must address situations where, based on the bank's risk assessment of a new account opened by a customer that is not an individual, the bank will obtain information about individuals with authority or control over such account, including signatories, in order to verify the customer's identity. This verification method applies only when the bank cannot verify the customer's true identity using the verification methods described in paragraphs (b)(2)(ii)(A) and (B) of this section.

- (iii) **Lack of verification.** The CIP must include procedures for responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe:

- (A) When the bank should not open an account;
- (B) The terms under which a customer may use an account while the bank attempts to verify the customer's identity;
- (C) When the bank should close an account, after attempts to verify a customer's identity have failed; and
- (D) When the bank should file a Suspicious Activity Report in accordance with applicable law and regulation.

- (3) **Recordkeeping.** The CIP must include procedures for making and maintaining a record of all information obtained under the procedures implementing paragraph (b) of this section.

- (i) **Required records.** At a minimum, the record must include:

- (A) All identifying information about a customer obtained under paragraph (b)(2)(i) of this section;
- (B) A description of any document that was relied on under paragraph (b)(2)(ii)(A) of this section noting the type of document, any identification number contained in the document, the place of issuance and, if any, the date of issuance and expiration date;

- (C) A description of the methods and the results of any measures undertaken to verify the identity of the customer under paragraph (b)(2)(ii)(B) or (C) of this section; and
- (D) A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

- (ii) **Retention of records.** The bank must retain the information in paragraph (b)(3)(i)(A) of this section for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant. The bank must retain the information in paragraphs (b)(3)(i)(B), (C), and (D) of this section for five years after the record is made.

(4) **Comparison with government lists.** The CIP must include procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. The procedures must require the bank to make such a determination within a reasonable period of time after the account is opened, or earlier, if required by another Federal law or regulation or Federal directive issued in connection with the applicable list. The procedures must also require the bank to follow all Federal directives issued in connection with such lists.

- (5)(i) **Customer notice.** The CIP must include procedures for providing bank customers with adequate notice that the bank is requesting information to verify their identities.
- (ii) **Adequate notice.** Notice is adequate if the bank generally describes the identification requirements of this section and provides the notice in a manner reasonably designed to ensure that a customer is able to view the notice, or is otherwise given notice, before opening an account. For example, depending upon the manner in which the account is opened, a bank may post a notice in the lobby or on its website, include the notice on its account applications, or use any other form of written or oral notice.
- (iii) **Sample notice.** If appropriate, a bank may use the following sample language to provide notice to its customers:

IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

(6) **Reliance on another financial institution.** The CIP may include procedures specifying when a bank will rely on the performance by another financial institution (including an affiliate) of any procedures of the bank's CIP, with respect to any customer of the bank that is opening, or has opened, an account or has established a similar formal banking or business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions, provided that:

- (i) Such reliance is reasonable under the circumstances;
- (ii) The other financial institution is subject to a rule implementing 31 U.S.C. 5318(h) and is regulated by a Federal functional regulator; and
- (iii) The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.

(c) **Exemptions.** The appropriate Federal functional regulator, with the concurrence of the Secretary, may, by order or regulation, exempt any bank or type of account from the requirements of this section. The Federal functional regulator and the Secretary shall consider whether the exemption is consistent with the purposes of the Bank Secrecy Act and with safe and sound banking, and may consider other appropriate factors. The Secretary will make these determinations for any bank or type of account that is not subject to the authority of a Federal functional regulator.

(d) **Other requirements unaffected.** Nothing in this section relieves a bank of its obligation to comply with any other provision in this part, including provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction.

[68 FR 25109, May 9, 2003]