Dealership Compliance Training

A Step By Step Guide To Dealership Compliance

Introduction

Team One
RESEARCH AND TRAINING
LexisNexis®

- As you probably already know, 2008 has brought the automobile dealer a whole new set of compliance issues and requirements to deal with. Team One Research and Training, the nation's leading automotive research and process development company, has compiled this educational information to familiarize you with the basics of those compliance requirements. However, we have gone several steps further and actually will provide you with a workable, simple, and inexpensive solution to help you meet the compliance challenge. With our strategic alliance with Lexis Nexis we have provided the dealer with a simple turnkey process to meet most of the compliance burden that incorporates the very best, cutting edge, information science in a simple solution at a very low cost. The following presentation is only designed to give you a general understanding of the compliance issues and should not be construed as legal advise. Your national and state dealer association legal advisories should be referenced and followed on a continuing basis.

Compliance Areas Covered

- Red Flag Rules
- Graham Leach Bliley Act
- Cash Reporting Policy
- Federal Trade Commission
- Fair Credit Reporting
- OFAC
- Disclosure Rules
- Payment Quoting and F&I Presentation
- Lexis Nexis Solutions
- F&I Training Solutions

Team One
RESEARCH AND TRAINING

LexisNexis®

Red Flag Rules

Team One
RESEARCH AND TRAINING
LexisNexis®

What Are Red Flag Rules?

Called the "Red Flags Rules," the rules mandate that banks, credit unions, and similar institutions set up written plans for identifying suspicious "red flag" transactions that could indicate identity theft or fraud, and update their plans with changing trends in financial crimes. The rules were passed as part of the Fair and Accurate Transactions Act (FACTA) in 2003, but did not go into effect until January 1, 2008, and you must have your Red Flag Compliance Program In Place Before November 1, 2008

The days of just copying a driver's license and taking a verbal social security number are over with the finalization of the Red Flag Rule. Credit reports will need to be thoroughly checked. You will also need to know how to react when a red flag is raised, and will have to document each situation. Dealers need to implement an identity verification solution for their sales process, as well as F&I. Thankfully, our Lexis Nexis solution does all of that for you. More than just information, the powerful Lexis Nexis network actually provides you with an identity and risk score on every potential buyer. This allows you to use good judgment and due diligence in screening potential buyers and gives you automatic guidelines to take the appropriate action required by the law.

What Do You Have To Do?

Team One
RESEARCH AND TRAINING
LexisNexis®

1. Develop a Written Program

What might be the biggest headache for you is developing a written program to combat identity theft. However, this can be a very simple document. It must contain "reasonable policies and procedures for detecting, preventing and mitigating identity theft." Your written policy just needs to state:

- **The types of accounts you offer or maintain**
- **The methods you use to open covered accounts**
- **The methods you use to access covered accounts**
- **Your previous experiences with identity theft**

Using the Nexis Lexis identity program on every potential customer can serve meet all of the above from one single source. Once you sign up for the program, a major part of your written policy can simply state that every customer will be screened with the only identity protection program endorsed by the American Bankers Association.

Your action on potential red flags can be determined by the Lexis Nexis "risk score" and your personal Lexis Nexis compliance representative will always be just a phone call away to discuss the appropriate action needed in those transactions in question. That can be, in essence, your written plan and policy. This is the **only** source that our extensive research could find that provides the level of information checking and support the dealer needs to meet the rules.

2. Designate A Program Administrator

Aside from implementing the written program, you will also need to designate an individual (typically someone at the senior management level) to oversee the program's development, implementation and administration. In fact, this could be the first thing a dealership does. This is probably the person who should write your written plan. This individual is who dealership personnel will refer to whenever a situation related to the program arises. This is the person who will make the final call. He or she will also collect reports from staff about all matters related to the dealership's identity-theft program. This person will also be required to collect reports from employees on the effectiveness of the program. This could include how the program addresses the risk of identity theft, service provider arrangements, and significant incidents involving identity theft and management responses. This person will also be responsible for recommending and implementing changes to the program.

(Kind of like your monthly safety meetings)

Team One
RESEARCH AND TRAINING
LexisNexis®

3. Exercise Due Diligence

Just a little common sense here. Your sales and F&I managers can usually tell if there is something “not right” about a deal. In addition to the Lexis Nexis check, identification and documents should be thoroughly scrutinized for:

•Documents provided for identification appear to have been altered or forged.

•The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

•Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

•Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

•An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Red Flag Summary

1. Develop a Written Program

2. Designate A Program Administrator

3. Exercise Due Diligence

4. Sign Up and Install the Lexis Nexis ID and Red Flag process

   At the end of this presentation, we will tell you how to set up the comprehensive Lexis Nexis program and how to implement it into your policies and procedures

Graham Leach Bliley Act

What Is The Graham Leach Bliley Act?

Protecting the privacy of consumer information held by "financial institutions" is at the heart of the financial privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999. The GLB Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information. Due to this federal law, dealers are required to protect the privacy of customers' nonpublic personal information and not share such information with third parties unless the customer is given the opportunity to "opt-out" of the sharing. GLB also requires giving a privacy notice at the time the customer relationship is established and annually thereafter if the person is still a credit customer. The FTC regulates auto dealers' compliance with GLB.

The FTC's rule that mandates formal information security programs must be adopted pursuant to the Gramm-Leach-Bliley Act. The rule requires a dealer to designate a named individual as responsible for implementing the program. This should probably be the same person designated as the Red Flag administrator

What Does Your Administrator Need To Do To Comply With Graham Leach Bliley?

1. Formal Risk Assessment

- Take inventory of all areas that customer information is collected and stored
- Identify/document all threats to customer data
- Evaluate and improve control environment
- Develop/document policies and procedures to secure information and enforce sanctions

2. Information Security Program

- Obtain dealership management's buy-in
- Define and communicate compliance responsibility
- Establish/document a formal training and awareness program for F&I and sales staff

3. Vendor Relationship Assessment

- Identify/document all vendors who access, process and store your customer data
- Assess/document how vendors are protecting customer data
- Review and monitor vendor agreements annually for compliance

4. Technical Security Management

- Develop virus standards and controls
- Perform security testing (external and internal penetration tests) at least annually
- Monitor your security environment by recording transactions and reviewing logs
- Develop security-incident response procedures

5. Annual Audit and Update Develop an audit strategy

- Perform audits on an annual basis
- Report audit findings to dealership management
- Revise vendor management practices as needed
- Test and revise your security compliance program as needed

Team One
RESEARCH AND TRAINING
LexisNexis®

Cash Reporting Rules and Patriot Act Compliance

Required on Cash Transactions Over $10,000

As some motor vehicle dealers are discovering, failing to comply with the Cash Reporting Rules can be costly. One dealer that was recently audited by the Internal Revenue Service (IRS) to determine compliance with the Rules was notified that the dealership owed more than $236,000 in fines and penalties for 10 non-reported cash transactions. Remember, failing to report cash transactions involving $10,000 or more is not only a violation of the Internal Revenue Code, but also the USA Patriot Act.

In order to comply with the Form 8300 filing requirements, it is important to understand how the term “cash” is defined for purposes of reporting. The term “cash” means U.S. and foreign currency in excess of $10,000. It also includes a cashier’s check, money order, bank draft, or traveler’s check having a face amount of $10,000 or less when two or more are presented or when it is combined with cash so that the total amount exceeds $10,000. The term “cash” does not include a personal check, a check drawn on the account of a business, certified personal and business checks, and amounts charged to a credit card are not considered cash.

Cash Reporting Requirements

The law requires dealers to file a Currency Transaction Report (CTR) with the Financial Crimes Enforcement Network (FinCEN) whenever they received large sums of money in one or a series of related transactions. If the dealership receives $10,000 or more in cash, the IRS Form 8300 must be also be filed by the 15th day after the date the cash was received. If the due date falls on a Saturday, Sunday or legal holiday, it should be filed on the next business day. If a dealership receives more than one cash payment for a single transaction or for related transactions, it must report the multiple payments if it receives a total amount that exceeds $10,000 within any 12-month period within 15 days of the date the dealership receives the payment that causes the total amount to exceed $10,000. Keep in mind that filing the Form 8300 is not the dealership's only obligation; it is also required to give a written statement to each person named on a required Form 8300 on or before January 31st of the year following the calendar year in which the cash is received. The statement must show the name, telephone number and address of the information contact for the dealership, the aggregate amount of reportable cash received, and that the information was furnished to the IRS.

Patriot Act Cash Reporting Compliance

Section 365 of the USA Patriot Act expands the scope of entities required to file reports to include “anyone” engaged in a trade or business that receives more than $10,000 in cash in one transaction (or two or more related transactions). Section 365 also requires financial institutions to establish procedures that enable employees to track all cash transactions to determine when a report should be filed and prohibits anyone from structuring a transaction to avoid the cash reporting requirements.
The Form used to report such transactions, titled “IRS Form 8300/FinCEN Form 8300,” is virtually identical to the IRS Form 8300 that motor vehicle dealers are required to complete pursuant to a similar provision under the Internal Revenue Code. After enactment of the Patriot Act, the IRS issued a Rule amending its regulations to clarify that the information reported to the IRS on cash transactions is also required to be reported to FinCEN. Motor vehicle dealers were required to begin using the new Form as of January 1, 2002.

Cash Reporting Summary

It is important that your dealership has a written policy that explains how cash transactions involving $10,000 or more will be handled and provide ongoing training programs for its employees. In addition, the dealership should implement auditing procedures to ensure that it remains in full compliance with the filing requirements. If you discover that a cash transaction has not been properly reported, you can file the Form 8300 late. Filing late may result in some fines and penalties, but they are insignificant compared to the fines and penalties the dealership may incur for not filling at all, which include fines of up to $500,000, seizure of assets and, in some cases, imprisonment for up to five years

FTC Compliance

FTC Consumer Information Disposal Rule

Dealers are required to securely dispose of sensitive information derived from consumer reports by taking reasonable measures to protect against any unauthorized access to or use of this information. The rule applies to both paper and electronic files.

Records the auto dealer keeps become the assets of the business. Dealer records include all information produced and received in connection with the operation of the dealership, whether such records are in a physical format or electronic. Dealer records may be as obvious as a memorandum, an e-mail, or a contract, or something not quite as obvious, such as a computerized desk calendar, an appointment book, an instant message, or an expense record. Even information contained in PDAs, Blackberries, and other wireless devices can be considered dealer records.

Because of the broad definition of what might constitute a dealership record, auto dealers must maintain certain types of company records for specific periods of time. These requirements apply no matter what the record's format or characteristic (i.e. both physical and electronic). Failure to retain records for the required time periods could subject the dealership to penalties or fines, or seriously disadvantage the dealership in litigation.

Since time requirements for retention of documents can vary from state to state, the dealership should consult an attorney for the legal requirements for retaining records that apply to your dealership.

(For FTC Safeguards Rule see Gramm-Leach-Bliley Act)

Recommended Practices

1. Sign up with the Lexis Nexis Accurint ID Program

This is the only program endorsed by the American Bankers Association for identity theft and verification issues. Our research shows that this is the only program that meets the standard for complete information and security. Unlike other programs in the marketplace, Lexis Nexis will appoint a personal representative, assigned to your dealership, who will contact you, be available for ongoing assistance, and help manage your compliance program.

To sign up, go to: http://www.accurint.com/signup.html

Once you are registered, your regional personal representative will contact you immediately. The cost for the program is surprisingly reasonable. $75 per month per person using the program, (minimum of 2) plus 65 cents per record provided.

Additional Recommended Practices

2. Create a data security plan that details how you safeguard and securely dispose of your customer information.

3. Limit access to customer information to only those employees and vendors who need it to perform their jobs.

4. Give your privacy notice to each customer with whom you do business (cash or credit), and make sure that your employees comply with your privacy policy.

5. Layout a plan to deal with data security breaches.

6. Put in place a comprehensive record retention policy.

7. Retain company records until they are of no further use or value to you and after any legally imposed retention time periods have expired.

8. Secure records that contain consumer information in accordance with your FTC Safeguards Rule data security program.

And Finally

Use America's #1 Performing, (and compliant), F&I Process Go to www.teamonegroup.com and see why 87 of the top 100 F&I departments in the country use the Team One Program

The preceding compliance training is a good introduction to dealer compliance issues.
For more links, resources, and updated information go to: www.teamonegroup.com

Team One Research and Training
PO Box 11563, Chandler, AZ 85248
1-800-928-1923

Team One
RESEARCH AND TRAINING