

Regulatory Compliance: How to navigate the new data compliance rules

Recommended Practices Checklist

1. Run an OFAC SDN list check on every customer (cash or credit). Keep a record of the OFAC check for five years.
2. Establish a step-by-step process to verify the identity of all customers as legitimately being who they claim to be.
3. Create a data security plan that details how you safeguard and securely dispose of your customer information.
4. Limit access to customer information to only those employees and vendors who need it to perform their jobs.
5. 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.
6. Set up a process in your dealership to collect opt-outs from information sharing, telemarketing, e-mails, and fax transmissions.
7. Layout a plan to deal with data security breaches.
8. Put in place a comprehensive record retention policy.
9. Consider using electronic documents and obtaining electronic signatures instead of paper ones.
10. Retain company records until they are of no further use or value to you and after any legally imposed retention time periods have expired.
11. Retain any records that may be relevant to a lawsuit or possible inquiry.
12. Secure records that contain consumer information in accordance with your FTC Safeguards Rule data security program.
13. Exercise due diligence in hiring a vendor to dispose of and destroy your records.

In today's busy and complex world, dealers must be continually aware of laws and regulations regarding record keeping and storage of customer data. Compliance with recent federal and state laws and regulations ensures that dealerships and their customers are protected.

To this point, the Federal Trade Commission (FTC) estimates that the identities of approximately 10 million U.S. consumers are stolen each year. Since 1999, federal law has required that dealerships disclose to consumers how data is collected, shared, and used. FTC enforcement activity is increasing to make certain that dealers are adhering to consumer data safeguarding and disposal guidelines.

Not properly storing and protecting consumer data can cost you in the form of fines and class action lawsuits. Here are just a few recent headlines that demonstrate that dealers are, and will be, held accountable: "Dealership to Pay Refunds, Half Million in Fines," *Anchorage Daily News*; "Car Dealer Settles Suit with State for \$7.1 Million," *Louisville Courier-Journal*; and "Dealer Settles 59 Lawsuits," *Fort Smith Arkansas Times Record*.

Compliance is no longer just a desirable precaution to take, but an absolute requirement for any dealership that wants to stay in business. As an F&I manager from Pennsylvania stated, "Compliance is a hidden cost. It takes only one very dissatisfied customer to cost the dealership a tremendous amount of money." It is necessary to store data of customers that purchased as well as any consumer from whom you take a credit application, regardless of whether or not they actually purchased a vehicle. To put that into perspective, you need to review the number of credit applications your dealership pulls on a monthly basis and investigate the steps your dealership currently takes to store and safeguard all those credit applications.

Regulatory compliance covers a lot of territory. Just what are some the most important laws and regulations of which a dealership should be aware? A good start for any dealer would be to read about and be familiar with the following terms, laws, and legislation:

Office of Foreign Assets Control's (OFAC) Specially Designated Nationals and Blocked Persons List - This list contains persons, countries, and organizations, such as known terrorists with whom U.S. entities are prohibited from doing business. Every customer must be checked against the SDN list at the time the customer relationship is established.

Regulatory Compliance: How to navigate the new data compliance rules

If there is a match, the dealership must notify the OFAC and cannot do business with the individual or entity. OFAC updates the SDN list several times a month and publishes it on its web site.

FTC Safeguards Rule - 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.

Gramm-Leach-Bliley Act (GLB Act) - 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.

Fair Credit Reporting Act (FCRA) - Disclosures must be made to consumers when a credit report is used in making a credit decision. Customers are also given opt-out rights with respect to sharing of consumer report information with affiliates for marketing purposes.

National Do-Not-Call Registry - This is a consumer-initiated list of telephone numbers maintained by the FTC that cannot receive telemarketing calls except where a prior business relationship exists during the preceding 18 months.

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.

The laws and regulations previously described and many others should be studied and addressed by every dealership. Compliance requires complete buy-in from dealership management and employees. The benefits are real and can save the dealership money and much time in the long term. Management planning, checklist development, and guideline implementation should take place in every dealership.

Staying current on all the regulations is imperative today, and your DMS provider should be able to assist you in staying compliant. In today's litigious society, knowing how to protect your dealership is essential because one unhappy customer can create legal and financial disaster.

Richard Holland is the president of Arkona – a DealerTrack Company – and has been designing and developing cutting-edge technology systems for more than 28 years. Holland was the national sales manager for Cars/Dyatron, a specialist in General Motors dealership software. He is also a Certified IBM Professional. As president of Arkona, Holland directs product strategy and keeps Arkona on the forefront of innovation and developing products that meet the needs and wants of the customer.