AAS AUTO ADVISORY SERVICES | KPA

TRANSMISSION

Helping make compliance automatic

Inside this issue:

Volume 42
Issue 12
July 2019

Questions? Contact the Compliance Hotline!

Monday-Friday, 9 a.m.-5 p.m. (PT)

Phone: (800) 785-2880, Select Option 4 | **Email:** questions@autoadvisory.com

Reader Survey: Tell Us What You Think!

We are always looking for ways to improve the information we share and how we share it. In 7 quick questions, tell us what we can do to make KPA Transmission a better resource for you.

If desired, you can enter your contact information to be entered into a $50 Amazon gift card drawing!

Take Survey

A Refresher on Service Contracts

by Robert Ebin

Recently, I have had many telephone conversations with people in the auto industry about none other than service contracts. To my surprise, a fair amount of these conversations began the same way with a mistaken reference to an “extended warranty” rather than a “service contract.” Admittedly, service contracts may not be the most scintillating subject. But with the uptick in calls, and the continued incorrect practice of calling them “extended warranties,” there appears to be no better time for a refresher on service contracts. The distinction is an important one and we need to begin calling it what it is.

What's a Service Contract?

California Insurance Code § 12800 broadly defines service contracts as a contract or agreement for separately stated consideration (i.e., payment) and a specific duration for:

- Repair, replacement, or maintenance of a vehicle necessitated by an operational or structural failure due to a defect or due to normal wear and tear.
- Routine maintenance for at least one year.
- Tire or wheel repair or replacement necessitated by wear and tear, defect, or damage due to a road hazard.
- Glass or windshield repair or replacement necessitated by wear and tear, defect, or damage caused by a road hazard.
- Paintless dent, ding, or crease removal.
- Replacement of a key or key fob.

The law also permits service contracts to include incidental payments of coverage for towing, substitute transportation, emergency road service, rental car reimbursement, reimbursement of deductible amounts under a manufacturer's warranty, and reimbursement for travel, lodging, or meals. [Insurance Code § 12800(c)(2)].

A service contract also includes an agreement "covering any of a vehicle's mechanical components, provided with or without separate consideration, that promises to repair, replace, or maintain a motor vehicle or watercraft, or to indemnify for the repair, replacement, or maintenance of a motor vehicle or watercraft, conditioned upon the use of a specific brand or brands of lubricant, treatment, fluid, or additive." [Insurance Code § 12800(c)(5)].

What is NOT a Service Contract?

They are not warranties.

A service contract is *not* a warranty nor an "extended" warranty. The federal Magnuson-Moss Warranty Act, codified under 15 U.S.C. § 2301, defines a "written warranty" as:

a) Any written affirmation of fact or written promise made in connection with the sale of a consumer product by a supplier to a buyer which relates to the nature of the material or workmanship and affirms or promises that such material or workmanship is defect-free or will meet a specified level of performance over a specified period of time, or

b) Any undertaking in writing in connection with the sale by a supplier of a consumer product to refund, repair, replace, or take other remedial action with respect to such product in the event that such product fails to meet the specifications set forth in the undertaking, which written affirmation, promise, or undertaking becomes part of the basis of the bargain between a supplier and a buyer for purposes other than resale of such product.

Similarly, California's Song-Beverly Consumer Warranty Act in Civil Code § 1791.2(a), defines "express warranty," in pertinent part, as:

(1) A written statement arising out of a sale to the consumer of a consumer good pursuant to which the manufacturer, distributor, or retailer undertakes to preserve or maintain the utility or performance of the consumer good or provide compensation if there is a failure in utility or performance.

Conceivably, the definitions of warranty provided in the Magnuson-Moss Warranty Act and Song-Beverly Consumer Warranty Act could encompass a service contract. However, an important distinction between the two is that service contracts generally involve a separate charge over and above the cost of the vehicle, while a warranty comes with the purchase of the vehicle and cannot be sold separately to the customer. Characterizing them as one or the other does have serious consequences. In a 2004 case, the California Supreme Court ruled that what a service contract is called or advertised as can transform it into a warranty. [*See* Gavaldon v. Daimler Chrysler Corporation, (2004) 32 Cal. 4th 1246]. Because of this, dealer personnel must avoid calling service contracts "extended warranties," "warranties," or "guarantees," or use other similar terms, when describing service contracts to a customer. Such characterizations can land your dealership in hot water.

The distinction between warranty and service contract is also extremely important as it relates to the Department of Insurance (DOI). Service contracts fall within the purview of the DOI, and the law requires that service contracts be filed with the DOI and that they are backed by insurance covering 100% of the obligor's service contract obligations. [Insurance Code § 12830] . Service contracts must also comply with the extensive disclosure requirements of Civil Code §§ 1794.4 and 1794.41 as well as Insurance Code § 12820. There are no such requirements for warranties.

They are not insurance.

Service contracts are also not insurance. Insurance is defined as "a contract whereby one undertakes to indemnify another against loss, damage, or liability arising from a contingent or unknown event." [Insurance Code § 22] . Although a service contract could also conceivably fall under the definition of "insurance," Insurance Code § section 12805(a) creates the exception.

As a reminder, you must not sell insurance products (mechanical breakdown insurance included) unless 1) you are a properly licensed insurance broker; 2) all your F&I personnel selling insurance products are licensed insurance agents; and 3) your computer system allows you to properly disclose insurance premiums in the Statement of Insurance section of the LAWCA-553 Retail Installment Sale Contract.

Beware of hybridized products.

You should be wary of hybridized F&I products pitched by vendors—those that make you scratch your head and ask: Is this a service contract, a hard add, or a theft deterrent device? You are responsible for ensuring that products are disclosed properly and that they are legal to sell in California. Always only do business with reputable vendors and consider putting the onus on the vendor to classify its product (and to provide documentation of the classification) before deciding to sell the product at your dealership. For a further discussion on this topic, please read the 2014 Transmission article, Frankenstein's F&I Laboratory.

Disclosure Requirements

Not too long ago, I was speaking to an auto industry veteran about a practice he observed regarding the sale of service contracts. He observed a dealer selling a service contract to a customer at the same time the customer was purchasing a vehicle. The problem was that the service contract was not disclosed on either the LAWCA-553 or a Pre-Contract Disclosure form. In fact, the only thing tying the service contract to the deal (other than the same date on the sale contract and service contract) was mention of the service contract on the internal deal recap. What was more puzzling, the service contract was separately financed over two years (with a $75 monthly payment) from a different lender than the captive who bought the vehicle sale contract. Essentially, it was two separate agreements tied to the same deal that didn't refer to one another in any of the paperwork! Not only could this practice be construed as an ASFA Single Document Rule violation and a violation of the pre-contract disclosure requirements (to name a few), but it can also be considered fraud on the captive lender.

When a customer purchases a service contract as part of the sale transaction for a vehicle, the service contract must be disclosed on the Pre-Contract Disclosure [Civil Code § 2982.2] as well as on the RISC in the Optional Service Contract(s) box (with terms of the service contract) and on line 1.I.1 of the 553 [Civil Code § 2982]. If part of a lease transaction, the service contract must be disclosed in the itemization of gross capitalized costs section of the lease agreement. Remember also to mark the box on the Buyers Guide indicating that a service contract is available if a service contract is offered on that particular used vehicle. [16 Code of Federal Regulations § 455.2(b)(3)].

I have heard of rare instances where a customer insists on purchasing a service contract, but the lender will not finance the deal if the service contract is included in the sale contract. This situation is a bit of a pickle, and what is certain is that the dealer must not follow the practice discussed above. Perhaps consider informing the customer to hold off on purchasing the service contract for the time being. If the customer still insists on purchasing a service contract after a few weeks, you could have the customer come back to the dealer and sell the service contract through the service drive as a non-financed transaction. Outside of this, the dealer may have to abstain from selling the customer a service contract.

Questions?
If you have any questions regarding this issue, or any other situation that may arise in your sales or service departments, hotline clients are invited to contact us at (800) 785-2880 (then press "4" for hotline) or hotline@autoadvisory.com.

Third Party Liability Keeps Creeping on Dealers– FTC Settles Case With DMS Provider Regarding Data Breach

by Shane McCallan

Last month, the Federal Trade Commission (FTC) settled a case against a large DMS provider, DealerBuilt, for allegedly failing to properly encrypt sensitive data and conduct necessary vulnerability and penetration testing. The breach, which occurred in 2016 over 10 days, included both customer and employee sensitive information. For customers, this included Social Security, driver's license, and credit card numbers. For employees, this included payroll and bank account information. Fortunately, DealerBuilt addressed this quickly with its dealers. It is one of the few DMS systems that allows a dealership to control where their data is sent, and that does not charge the dealers for access to their own data.

However, this is a lesson of exposure for all dealers. The mistakes of third-party vendors can create major consumer and employee legal issues, costing the dealership time, money, and reputation – identifying the affected customers and employees, notifying them, responding to their complaints and addressing the legal fallout.

Resulting identity theft or fraud that harms the affected parties could result in expensive litigation against the dealership in several ways. The close example, if DealerBuilt violates this settlement, it must pay $42,350 per violation. Allegedly 69,283 customers were affected (not counting employees), so that penalty in retrospect could theoretically be nearly $3 billion.

Let's break that down a bit from the dealership's perspective. Suppose that your dealership sells 200 new and used vehicles per month over one year, which would, in turn, mean 200 separate transactions where you take secure information from the customer. This figure doesn't necessarily take into account the unknown number of dead deals where customer information is collected, but there was no final deal. And it does not take into account the number of employees affected by the breach. Pursuant to the FTC's settlement agreement, and the penalty above, a failure to properly handle your data would theoretically be upwards of $100 million for the year for that one dealership alone (separate from the third-party vendor). Also, that's just the statutory penalty, not monetary (out of pocket) or punitive damages.

Fortunately, the FTC was rational and neither of these theoretical, staggering numbers will become reality.

But, it is a hammer that they can put over your head to force a settlement. The lesson is this: third-party vendors can create chaos for you.

> As an aside, another example of third-parties creating dealership significant legal liability is an FTC action against a Washington, D.C. based dealership for advertising violations that were promoted by a California third-party marketing company. The FTC alleged that the dealership group (but not the third-party marketing company who did it) "mailed more than 21,000 fake 'urgent recall' notices to consumers in 2015 and 2017, to lure them to visit dealerships." Just

another angle of third-party vendor liability for inattentive stores.

[Source: https://www.ftc.gov/news-events/press-releases/2018/10/washington-dc-area-car-dealerships-marketing-firm-settle.]

In its creative style of writing, the FTC starts off its blog post about the action against DealerBuilt with:

> *"The domino principle. The ripple effect. The butterfly phenomenon. Apply the analogy of your choice to describe what happens when one software developer's allegedly lax security practices result in the breach of confidential customer information maintained by multiple businesses that use the software. If of the consequences your business is a service provider – or if your company uses third-party service providers to help manage your data – a proposed FTC settlement merits your attention.*
>
> …
>
> *Many third-party service providers sell industry-specific data management software to consumer-facing businesses."*

This issue is pervasive with third-party vendors. And this is going to be highlighted by the upcoming California Consumer Privacy Act. Because you collect and store customer information on a daily basis, you should heed the above warning.

Besides alleging that DealerBuilt failed to employ reasonable security measures, in violation of the FTC Act for unfair practices, the FTC points out in its second allegation that DealerBuilt meets the definition of a "financial institution." That triggers the duty to comply with the federal Gramm-Leach-Bliley Act's (GLBA) Safeguards Rule.

Hopefully, you all have a Red Flags and Safeguards book at your dealership and an employee who is responsible for overseeing compliance because you are also considered a "financial institution" under GLBA.

Among other things, this requires you to develop, implement, and maintain a written information security program; to identify reasonably foreseeable risks to the security, confidentiality, and integrity of customer information; and to implement basic safeguards and regularly test their effectiveness.

The FTC's proposed administrative complaint provides some lessons from the DealerBuilt case. Some of its transgressions:

- Stored information in clear text, without any access controls or authentication protections like passwords or tokens. Data transmitted between dealerships and DealerBuilt's backup database was in clear text, too.
- Didn't have a written information security policy in place.
- Didn't provide reasonable data security training for employees or contractors.
- Didn't assess risks to the sensitive data on its network by conducting periodic risk assessments or performing vulnerability and penetration testing.
- Didn't use readily available security measures to monitor – among other things – unauthorized attempts to transfer sensitive information.
- Didn't put reasonable data access controls in place – for example, systems to limit inbound connections to known IP addresses or require authentication to access backup databases.
- Didn't have a reasonable process to select, install, and secure devices with access

to personal information.

You can read the full article published by the FTC here. Again, it is unfortunate that this occurred to DealerBuilt and its dealers because DealerBuilt is known to be a dealer friendly DMS provider. But ultimately, you are the retailer and employer, and you are responsible for your customers' and your employees' sensitive information. It is irresponsible to trust this data to any third-party vendor who cannot provide you with the appropriate compliance assurances.

You should hold your third-party vendors to the same standards as you hold yourself.

We'll finish with the direct guidance provided by the FTC to other businesses, which we do not disagree with.

- ***Train and supervise your employees to be security-centric****.* *Designating someone to be in charge of security at your business is a start, but it doesn't mean you then get to pretend that vulnerabilities don't exist. Companies that handle consumers' sensitive personal information have a responsibility to consider security all along the way. Conduct staff training appropriate to the nature of your business and update it to reflect current risks and threats. What's more, make sure someone is supervising the supervisors whose decisions have a big impact on security at your company.*

- ***Exercise care when installing devices with network access****.* *Like sticking a finger in a socket, adding certain devices to your system runs the risk of inflicting a substantial shock. Think through the security implications and make sure any device is properly installed.*

- ***GLB coverage is broad****.* *The phrase "financial institution" may conjure up images of passbooks, tellers, and pens chained to tables, but that's not how the Gramm-Leach-Bliley Rules define the term. Consider whether your business could be a financial institution subject to the GLB Safeguards Rule.*

- ***If your company uses third-party software or providers, build security into your contracts****.* *Even if another company's conduct is implicated in a breach, your customers' information could be at risk and they'll want to know what you did to protect them. As the FTC's publication Start with Security suggests, when entrusting data to third-party service providers, spell out your security expectations, monitor what they're doing on your behalf, and follow websites that report on known vulnerabilities.*

- ***Service providers are accountable for protecting the personal data they collect and store****.* *Even if your operations are behind the scenes, you still may be liable for violations of the law. If you handle sensitive consumer data on behalf of other companies, security should be front and center.*

Questions?
If you have any questions regarding this issue, or any other situation that may arise in your sales or service departments, hotline clients are invited to contact us at (800) 785-2880 (then press "4" for hotline) or hotline@autoadvisory.com.

For More Information, Contact Us:

(800) 785-2880

questions@autoadvisory.com