

July 17, 2007

Best practices – Identity theft deterrence

by Gil Van Over

This year's columns have been dedicated to describing this whole thing called compliance. We are now in the process of describing best practices that, if implemented, are designed to help reduce exposure to litigation and regulatory inquiries. Today's topic is Truth in Lending Act (TILA) disclosures.

Background

As you are probably well aware, identity theft is the fastest growing crime in America. From what I understand, the situation is even worse on the continent. Car dealers have long been targets of ID thieves, some internal, some external. Recent headlines from California to Florida highlight this fact. As such, dealers have obligations under the Gramm-Leach-Bliley Act to take appropriate steps to safeguard consumer's personal, non-public information (NPI).



Best Practices

There are a number of best practices a dealer can put into place to help prevent his dealership from being a target for identity thieves.

Re-implement a Safeguards program – Dealers are required to have a Safeguards program in place since May 2003 (See my January 30, 2007 Compliance Corner for the five required components). If you don't have one in place yet, get one up and running. If you do have one in place, test its sufficiency. It may be time to re-implement the program.

Video record the F&I transaction – Identity thieves tend to run once they find out that the transaction is being recorded.

Obtain thumbprints – See point about video recording the F&I transaction.

Common sense and Red Flags – Check your gut. Sometimes things just don't feel right. There are a number of potential red flags that may give you hints that you have an ID thief in front of you. Examples include an out-of-state driver's license, customer agrees to MSRP plus addendum plus every F&I product, brokered deals, consumer arrives in a taxi cab or walks onto the lot from the bus stop, has a driver's license issued the same day, has an expired driver's license, comes in just before you close or wants the vehicle delivered to a parking lot.

Network Vulnerability Assessment – Don't just focus on the paper. The greater risk is in the data in your DMS. Have a Network Vulnerability Assessment conducted to see if an ID thief can hack into your system or if you are able to detect if someone is trying to hack in.

Stop accepting credit apps over the phone – This is a favorite tactic of ID thieves. Here's the scenario: an ID thief finds someone's wallet. The wallet has enough info to steal the person's identity. The thief calls a dealer about fifty miles from the victim's house and tells an eager saleswoman that he wants to buy a car, but doesn't want to drive all the way over if he can't get approved. The saleswoman takes a credit app, runs a bureau and tells the thief that he has great credit and can buy anything he wants. You won't hear from the thief, but may hear from the victim when your inquiry is the first one the victim does not recognize. You are now the victim.

Consider identity verification software – There are a few vendors that can provide identity verification software. This software takes basic info, such as name and address, searches a number of databases and prompts the user to answer some out-of-wallet questions that only the real person will likely know. Having documentation in file that you put someone through this software in the event the identity has been stolen may help to mitigate claims against your dealership.

Identification due diligence – Provide staff training on the adequate review of a consumer's photo identification. Require that a photo ID be obtained before allowing a consumer out on a test drive. Have your state DMV provide training on how to identify phony driver's licenses. And don't make the same mistake as the Texas dealer who gave a car to a 19-year old man posing as a forty-something woman. Also, beware of International driver's licenses and Mexican Matricula Consular ID cards. The documentation to obtain one of these forms of ID is loose or non-existent.

Social Security Number training – This number is a key piece a thief needs to steal someone's identity. The Social Security Administration can provide you with the algorithm that goes into those precious nine digits. The first three digits tell you where the number was assigned. For example, a social starting with 575 was assigned in Hawaii. The second two digits give a clue as to when the number was issued. The last four don't give you a clue about the customer's identity.

Watch credit bureau alerts – Consumers can put alerts into their credit files which alert prospective creditors that their identity may have been compromised. Train your sales manager to look past the bureau score and also check the report for a consumer alert. Follow the instructions in the alert, document your actions on the hard copy of the bureau and sign it.

Validate – Verify the consumer's information on all pieces of documentation such as driver's license, paystub, credit report, credit application, insurance card, checking account, utility bill, etc.

Signatures – Check the consistency of signatures from document to document. An ID thief is probably not used to signing the victim's name and can make mistakes, such as different slant on lettering and misspelling name.

Gil Van Over is the President and founder of gvo3 & Associates, a nationally recognized F&I and Sales compliance consulting firm (www.gvo3.com).

© 2007 by gvo3 Consulting, LLC. All rights reserved.

Published by [Dealer Communications](#)

Copyright © 2007 Horizon Communications Inc.. All rights reserved.

Information in this newsletter is provided by both proprietary and public sources. Dealer Communications makes no claims as to the accuracy of information provided by third party providers.

Powered by [IMN](#)