



Update - Identity Theft in the Dealerships

With

Brian Bentz, CPA & Wayne Youngs

Dixon Hughes PLLC

Moderated by

Jerilyn Klein Bier

Editor, DealersEdge Business Briefing

Presented by DealersEdge





Brian Bentz, CPA

Since joining the firm in 1989, Brian has provided exceptional perspective in accounting and advisory services to our dealership clients.

With his entire career dedicated to service dealerships, Brian's experience includes an extensive audit and tax background focused solely on dealerships. That experience, coupled with his continuous hands-on involvement in dealerships, allows him to bring very specific and practical solutions to all his clients.

Brian now provides services for our Dealer Services Group from our Dallas/Ft Worth office. These specialized services include:

- ❑ **Compliance services** – F&I Compliance, Information Security Program development and training, FTC Safeguards Compliance, and Sarbanes-Oxley assistance
- ❑ **Internal Audit** – risk-based program development, modification and service
- ❑ **Due diligence & buy/sells** – pro-forma and operational analysis, agreement document modification, closing assistance
- ❑ **Agreed-upon procedures** – consistent dealership-specific programs including internal control, process testing and dealership operations

Brian is also co-facilitator of the Dixon Hughes CFO Alliance Group, a consortium of CFOs from larger multi-franchised dealerships across the country that meets twice a year to discuss current challenges and the solutions to those issues.

Wayne Youngs

is an Executive Consultant with Dixon Hughes PLLC. Wayne specializes in the automotive industry and has been assisting car dealers with process improvements, data processing cost recovery, and contract negotiations for the past 23 years.



In addition for the past three years, he has also been helping Dealers become Gramm-Leach–Bliley compliant by doing in-depth GLB risk assessments that help dealers meet these new identity security procedures.

He is familiar with billing practices and contracts of major DMS ADP, Reynolds & Reynolds ,Arkona and UCS.

Prior to joining Dixon Hughes 4 years ago, he spent 3 years with his own dealership consulting firm and 16 years with ADP the last 14 years as their Director of Sales in the Southwest.



Gramm-Leach-Bliley Regulation

Prepared and discussed by

Brian Bentz - CPA & Wayne A Youngs

Executive Consultant-Dixon Hughes PLLC



What to Know!

- *How these regulations affect the dealership?*
- *What is their impact?*
- *What are the Dealers risks and exposure?*
- *How can they be used to protect me?*
- *What computer products should be considered to help secure dealership data?*

*Fines of \$11,000 Per Occurrence
FTC.*

*OFAC Fines Start at a Million for 1st
Offence,- to \$10 Million.*

Have I Got You Attention!





FTC Safeguard Rule!

- *21,000 (est.) auto dealer points in US-deemed as financial institutions that are subject FTC regulation.*
- ***All** must comply with the FTC Safeguards Rule.*
- *Safeguards simply states that you will secure the customer records and information. (Both in the front end and back end of the dealership)*
- *And it's a good time to review in house security.*

Industry Look at who must Comply!



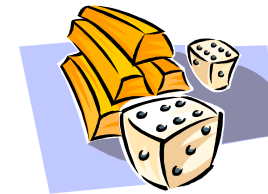
- *Businesses (regardless of size) that are engaged in providing financial products or services to customers (ex. banks, dealerships, etc.).*
- *While it is not only the law in securing customers data, it's good business to review internal document policy.*
- *Poorly secured data can lead to customer identity theft and possible business disruption and loss of consumer confidence.*

Industry – How Dealers Comply!



1.) Designate one or more employees to coordinate the safeguards.

2.) Identify and access the risks to customer information in each area (department) of dealership operations.



How Dealers Comply (Continued)

3.) Design & implement a safeguards program, monitor and test it.

4.) Select appropriate service providers and contract them to implement a written program.

5.) Evaluate and adjust program in light of relevant circumstances as result of monitoring and testing.

6.) Document- it will save you money!



What Areas Are Important to Information Security!

- *Employee management & training.*
- *Information systems*
- *Managing system failures.*



Employee Management & Training?



- *Check references prior to hiring employees with access to client information.*
- *Have every new employee sign an agreement to follow your organizations confidentiality and security standards in handling client information.*
- *Train employees to take basic steps to maintain security and confidentiality of clients information.*
- *Locking rooms and file cabinets where records are kept.*



Employee & Management Training Continued . . .

- *Using password activated screen savers. Make passwords at least 8 characters long.*
- *Change passwords every 30 days and don't tape to computers.*
- *Remind & test employees on organizations policy to keep client information secure.*
- *Limit access to client information to employees that only have business reason to see it.*
- *Impose disciplinary measures for any breaches.*





Information Systems



This includes network and software design , and information processing,storage,transmission,retrieval and disposal.

- *Store records in a secure area, with only authorized employees having access to them.*
- *Store paper records in room or cabinets that are locked when unattended.*
- *Store electronic customer information on a secure sever that is only accessible with a password.*





Information Systems

continued

- *Don't store sensitive customer data on a machine with an internet connection unless monitored, protected and secured.*
- *Maintain secure backup and keep archived data secured.*
- *Provide secure data transmission when you collect or transmit customer information. Credit reports or credit card info.*



Information System Continued

- *Dispose of customer information in a secure manner.*
- *Hire or designate a records retention Manager for disposal of records.*
- *Shred printed or written customer info.*

Information System Continued



- *Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media.*
- *Use over-site and audit procedures to detect improper disclosure or theft of customer information.*
- *Maintain a close inventory of your computers.*



Managing System Failures

Maintain up to date and appropriate program controls by:

- *Proper documentation.*
- *Written contingency plans to address breaches of your physical, administrative and technical safeguards.*
- *Up to date- records*

