

Is there a Red Flag on your DMS System?

by : Sandi Jerome

I recently spoke at the Oregon and Idaho Auto Dealer's convention. Paul Metry, NADA's director of Regulatory Affairs gave a presentation about current legal issues including Red Flag. I couldn't help but notice long faces in the audience and dealers were quick to ask me after my technology presentation how they can be prepared for Red Flag. I won't go into the specific requirements of Red Flag since many articles have been written about that, but instead I'll discuss your technology and how Red Flag concerns you. To make it simple, think of Red Flag as a Safeguards Rule with the objective to prevent identity theft. Like the Safeguards Rule, you need to develop a written program and the best place to start is your DMS system and F&I office since your risk will involve three areas: thieves trying to use a stolen identity to purchase a vehicle from you, employees trying to steal from you via identity theft, and thieves trying to get at the identity information you warehouse or transmit of your customers.

Where should you start? That is easy. Your first step is to make sure every employee is using a Windows password and the Windows screensaver with a password. Just go to start, control panel, display, screensaver, and check the box "on resume, password protect." Document the changes you made today, you'll need that later for your written plan. Next move onto your DMS system and find out if you have a server or ASP solution. If you have a server, then you don't have as much concern about the transmission of customer data by your DMS system (except in the F&I process). You still might have customer data being transmitted wirelessly from your service department, used car office or body shop; or you might be an ASP for your other dealerships. The thing to investigate is how each user on your system connects to the server. A simple user report and diagram should get you started in the right direction. You might also provide wireless service in the service lounge, and that needs to be secured along with any devices like hand-held service tablets and credit card processors. Next you need to find out what data is being transmitted from your dealership to third parties. This can be as simple as repair order data being transmitted to your factory and as complicated and risky as credit applications. Again, making a diagram of the process helps. If you do have a server onsite; how is that secured? I once walked up to a service cashier counter and bumped into a blue box at my feet. It was the dealership DMS system! How easy is it for someone to just pick up your server (including employees) and walk out with it? If you are on an ASP then you need to diagram the connection from your dealership, through your ISP, through their ISP and into their service center. Next it is your responsibility to make sure these people and their technology is reliable.

All this might sound like a lot of work, but according to Jason Blair, president of Dealerspan, "This new rule is involved and complicated but completely manageable with the right personnel and the right technology to assist in becoming compliant." His web site offers a free video for you to watch and download of the regulation. Visit www.Dealerspan.com, and they also offer Red Flag services from a "do it yourself" package to a full monitoring security program. I realize that I didn't cover the other two areas, which are preventing someone from using a stolen identity to purchase a vehicle from you and preventing your employees from stealing customer data to create stolen identities. Both of these require extensive employee training and screening more than protecting your technology. And most of the dealerships I've spoken to already have these safeguards in place. I've heard lots of stories of identity theft happening in our industry by these two methods but after hearing what happened recently at Borders, Boston Market, and other retailers, I've been worried about the information moving to and from DMS system servers. Your servers might contain hundreds of thousands of records and it's time to make sure that data is secure before you hear your dealership's name on the six o'clock news as the latest cause of a huge identity theft!

Sandi Jerome is a former controller, CFO, system administrator, F&I, assistant GM, and fixed operations manager with over 20 years experience in the automotive industry. She is the owner of Sandi Jerome Computer Consulting.