

The Red Flag Rules

Here is a quick overview of the new rules from Mike Goodman, an attorney with the Washington, D.C., office of Hudson Cook, in an interview with Jennifer Reed, Editor at SubPrime News about a year ago:

“A red flag is a pattern, practice or specific activity that indicates the possible existences of identity theft...sales of vehicles financed through a retail installment sales contract are covered by this rule...the red flags rule requires financial institutions and creditors to develop and implement an Identity Theft Prevention program. The term ‘creditor’ covers both dealers and finance companies. Dealers (even those who immediately assign all their paper to third-party finance companies) are covered because the rule applies to the opening of a covered account. Finance companies are covered because the rule applies to the maintaining of a covered account. The red flags rule is accompanied by guidelines intended to promote compliance. These guidelines address how to identify relevant [of 26] red flags; where to look to learn about emerging red flags; typical scenarios where identity theft is especially likely to occur; how to detect the existence of red flags in the course of a covered entity's business; what steps to take to prevent or mitigate identity theft when a red flag is detected; and how to update the program to keep it current,” Goodman said.

Looks like a lot of new curriculum, procedures and training is required to work toward some form of compliance effort. Not to mention the legal policies, forms and trainings that must be developed. During the comments period of the Red Flags legislation, NIADA’s General Counsel stated the “burdens that would be imposed on motor vehicle dealers in complying with the proposed Red Flag Rules are being vastly underestimated.”

In a Ward’s article last year Michael Benoit, Partner at Hudson Cook LLP outlined the steps to comply with the FTC’s Red Flag Rules:

“Auto dealers who engage in financing activities are required to establish an Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft. Your program must consist of six components:

1. Identify relevant “red flags” (patterns, practices or activities that indicate the possibility of identity theft) relevant to the credit origination process
2. Detect and evaluate these “red flags” in connection with individual customer transactions
3. Respond to the “red flags” you detect in an appropriate way to prevent identity theft
4. Ensure your program is updated periodically to reflect changes in risk to customers from your experiences and new identity theft activity
5. Policy generation and reporting capabilities with annual audits
6. Employee training for those involved in the origination of new accounts

This new rule is involved and complicated but completely manageable with the right personnel and the right technology to assist in becoming compliant. So, do yourself a favor – carefully vet new technologies with your compliance counsel. While certain parts of the Rule lend themselves to technological solutions, other parts may require some good old fashioned subjective thinking. Be sure you know which parts are which, and you'll keep the regulatory wildfires to a minimum.”

Here are 12 content items associated with a “good faith” compliance effort that the F&I legal experts at Hudson Cook, LLP, have outlined. A “Red Flags” Toolkit should include the following:

1. Red Flags Program Overview Training
2. Red Flags Risk Assessment
3. Identity Theft “Red Flags” Policy for Employees
4. “Red Flags” Program Policy
5. Reference Sample Red Flags Policies and Procedures
6. Training (Online or on-site)
7. Red Flag Detection Checklist
8. Dealership Red Flags and Responses
9. Customer Identification Workflow
10. Customer Identification Checklist
11. Identity Theft Incident Report Form
12. Annual Red Flags Audit Form

For more information please visit: www.compli.com or contact Jamie Apt via phone: 214.417.8385 or email at: jamie.apt@compli.com