Article from **Dealer Magazine** (http://www.imakenews.com/dealercomm1/e_article000978825.cfm?x=bbH76Mr,b5lQws1G,w)

December 18, 2007

The 31 Red Flags

by Gil Van Over

There have been plenty of articles written about the impending Red Flags Rule since I wrote my September 2006 article warning dealers about the new regulation. This rule is effective in a few weeks (January 1, 2008) and must be implemented within your dealership by November 1, 2008. So, what exactly are these Red Flags?

The feds identified these red flags as potential indicators of identity theft. You should consider addressing these potential indicators when you develop your program. Here is the list. During the next two weeks I will discuss solutions.

Red Flags in Connection With an Account Application or an Existing Account

Information from a Consumer Reporting Agency
1. A fraud or active duty alert is included with a consumer report.
2. A notice of address discrepancy is provided by a consumer reporting agency.
3. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
a. A recent and significant increase in the volume of inquiries.
b. An unusual number of recently established credit relationships.
c. A material change in the use of credit, especially with respect to recently established credit relationships.
d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Documentary Identification
4. Documents provided for identification appear to have been altered.
5. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
6. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.
7. Other information on the identification is not consistent with information that is on file, such as a signature card.

Personal Information
8. Personal information provided is inconsistent when compared against external information sources. For example:
a. The address does not match any address in the consumer report.
b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
9. Personal information provided is internally inconsistent. For example, there is a lack

of correlation between the SSN range and date of birth.
10. Personal information provided is associated with known fraudulent activity. For example:
a. The address on an application is the same as the address provided on a fraudulent application.
b. The phone number on an application is the same as the number provided on a fraudulent application.
11. Personal information provided is of a type commonly associated with fraudulent activity. For example:
a. The address on an application is fictitious, a mail drop, or prison.
b. The phone number is invalid, or is associated with a pager or answering service.
12. The address, SSN, or home or cell phone number provided is the same as that submitted by other persons opening an account or other customers.
13. The person opening the account or the customer fails to provide all required information on an application.
14. Personal information provided is not consistent with information that is on file.
15. The person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Address Changes
16. Shortly following the notice of a change of address for an account, the institution or creditor receives a request for new, additional or replacement checks, convenience checks, cards, or cell phone, or for the addition of authorized users on the account.
17. Mail sent to the customer is returned as undeliverable although transactions continue to be conducted in connection with the customer's account.

Anomalous Use of the Account
18. A new revolving credit account is used in a manner commonly associated with fraud. For example:
a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry).
b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
19. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
a. Nonpayment when there is no history of late or missed payments.
b. A material increase in the use of available credit.
c. A material change in purchasing or spending patterns.
d. A material change in electronic fund transfer patterns in connection with a deposit account.
e. A material change in telephone call patterns in connection with a cellular phone account.
20. An account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

Notice from Customers or Others Regarding Customer Accounts
21. The financial institution or creditor is notified of unauthorized charges in connection with a customer's account.
22. The financial institution or creditor is notified that it has opened a fraudulent account for a person engaged in identity theft.
23. The financial institution or creditor is notified that the customer is not receiving account statements.
24. The financial institution or creditor is notified that its customer has provided information to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent Web site.
25. Electronic messages are returned to mail servers of the financial institution or creditor that it did not originally send, indicating that its customers may have been asked to provide information to a fraudulent Web site that looks very similar, if not identical, to the Web site of the financial institution or creditor.

Other Red Flags
26. The name of an employee of the financial institution or creditor has been added as an authorized user on an account.
27. An employee has accessed or downloaded an unusually large number of customer account records.
28. The financial institution or creditor detects attempts to access a customer's account by unauthorized persons.
29. The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information.
30. There are unusually frequent and large check orders in connection with a customer's account.
31. The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report.

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

Published by Dealer Communications