

January 8, 2008

The manual red flags

by Gil Van Over

When last I addressed you, I gave you the list of the 31 red flags the Feds identified as potential indicators of identity theft. Some of these red flags, such as the address change and the anomalous use of the account categories, obviously do not apply to car dealers unless you are running a buy-here, pay-here operation. Other of the red flags will be caught using electronic methods. The remainder of the red flags will have to be observed manually.

The manual red flags which will require manual observation and action include:

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. Documents provided for identification appear to have been altered.
4. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
5. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.
6. Other information on the identification is not consistent with information that is on file, such as a signature card.
7. 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.
8. Personal information provided is internally inconsistent. For example, there is a lack of correlation between the SSN range and date of birth.
9. The person opening the account or the customer fails to provide all required information on an application.
10. Personal information provided is not consistent with information that is on file.
11. 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.
12. The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information.
13. The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report.

Next week I will list the potential red flags which will require an electronic solution. Then I will address potential solutions so that you can get your program up and running.

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).

© 2008 by gvo3 Consulting, LLC. All rights reserved.

Published by [Dealer Communications](#)

Copyright © 2008 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](#)