

**Product-Specific FAQ for Reynolds and Reynolds Customers
Regarding the FTC Safeguards Rule under the Gramm-Leach-Bliley Law**

This information includes our own representations and opinions and is not intended as legal advice.

Q: How do Reynolds DMS solutions “comply” with the Safeguards Rule?

Reynolds’ products are “compliance-compatible” or “compliance-supportive.” There is no one-size-fits-all recipe for privacy compliance, and a given product cannot, by itself, make compliance happen. The Safeguards Rule says that its compliance requirements are flexible, depending on individual characteristics of a business and the resources it has to comply.

Q: What ERA features help with privacy compliance obligations (the July 1, 2001 Privacy Rule)?

In response to the GLB/FTC Privacy Rule, Reynolds implemented the following changes:

- Added an Opt-Out flag to the ERA NameFile (customer master file).
- Modified eActivate queries to allow a test of the Opt-Out flag when extracting personal information about the dealership’s customers.
- Informed all ERA customers that they should contact us to modify any Custom Reports they used to extract personal information about the dealership’s customers to add a test for the Opt-Out flag.
- Similar changes were made to the Reynolds Generations Series Suite applications.

Q: What ERA features help with safeguarding compliance obligations?

ERA includes the following safeguards-related functionality:

- Limit access to specific executables and files by user (such as files containing social security number and other personal information).
ERA security maintenance functions, the 0973 screen, permits a dealer’s administrator to completely block a user’s access to the “General” screens in the Customer File.
- Log users off of an ERA terminal after a specific time
- Require users to change passwords periodically
- Identify duplicate user logons from multiple terminals
- Restrict dial-in access from selected users
- View reports summarizing current status of user permission

- Log user activity

For more details, see the *ERA2 System Director's Manual*, Chapt. 8, "Maintain User Security."

The Reynolds Generations Series Suite offers similar capabilities.

Q. Can I produce a report of who accessed consumer data?

- Activate a function that creates a user history record.
 - Access the 6230 program, SECURITY SPECIFICATIONS to do this.
 - *Note:* Just as with online audit logs, this function may affect "bandwidth" and storage resources, depending on the individual client's DMS platform.
- Create an EXECUTABLE HISTORY REPORT by running job 6240.
 - This specification activates the data-gathering function in the system.
 - You can print the history for the specified number of days. You can specify an interval between 1 and 60 days. The default setting is 14 days.
- The Executable History Report offers the following sort fields: User ID; Executable Number; Port Number; Date/Time; Store; and Area.

Q. Can I restrict third-party 6910 access (via password security) to only allow execution of a pre-defined report?

- The "Restrict Report Access" function limits the user to viewing a specified report. The user cannot modify the report, create a new report, or view a different report.
- In Maintain User Security (6210), if the "Restrict User Access" parameter is set to "Y", the user will not be able to view any reports.
 - For the user to view a report, the user must be granted access to the report in the Report Generator / Letterwriter Security.
 - Once the user has been granted access to a report, the user will then only be able to view the report on screen, print the report, or print the specifications for the report.

- The user cannot create/modify/delete any reports from the system. The user is basically limited to “view only” access to the specified reports themselves.
- Reports and files can be password-protected. If a file is password protected, the user cannot set up a report for the protected file.

Q. How does Reynolds’ ERA3 solutions with Consumer Reach help accomplish safeguards?

- Combined with an appropriately configured firewall, Reynolds’ ERA3 solution with the Consumer Reach gateway server provides an enhanced level of security to protect the confidentiality of consumer data from potential Internet threats.

For Web data (HTTP) that is in transit to or from your location, Consumer Reach protects the data with Secured Sockets Layer (“HTTPS” or “SSL”) encryption.

Note: To maintain these safeguards, Consumer Reach must be properly configured. The effectiveness of Consumer Reach safeguards may be partly or completely disabled if you connect your ERA3 server directly to the Internet.

Q. How does Reynolds’ Managed Access solution help accomplish safeguards?

Reynolds’ Managed Access solutions provide a security foundation to support enhanced data safeguards. Some examples of this include firewall solutions and Intrusion Detection Systems (IDS).

A key component in any Internet security solution is a correctly configured firewall that provides a robust rule set that enables business transactions but blocks potential internal and external threats. A misconfigured firewall can allow these threats (for example, unauthorized individuals, worms, or Trojans) potential access to data.

Reynolds Managed Access solutions are based on industry firewall best practices. Trained network engineers configure and support the solution to protect against emerging threats.