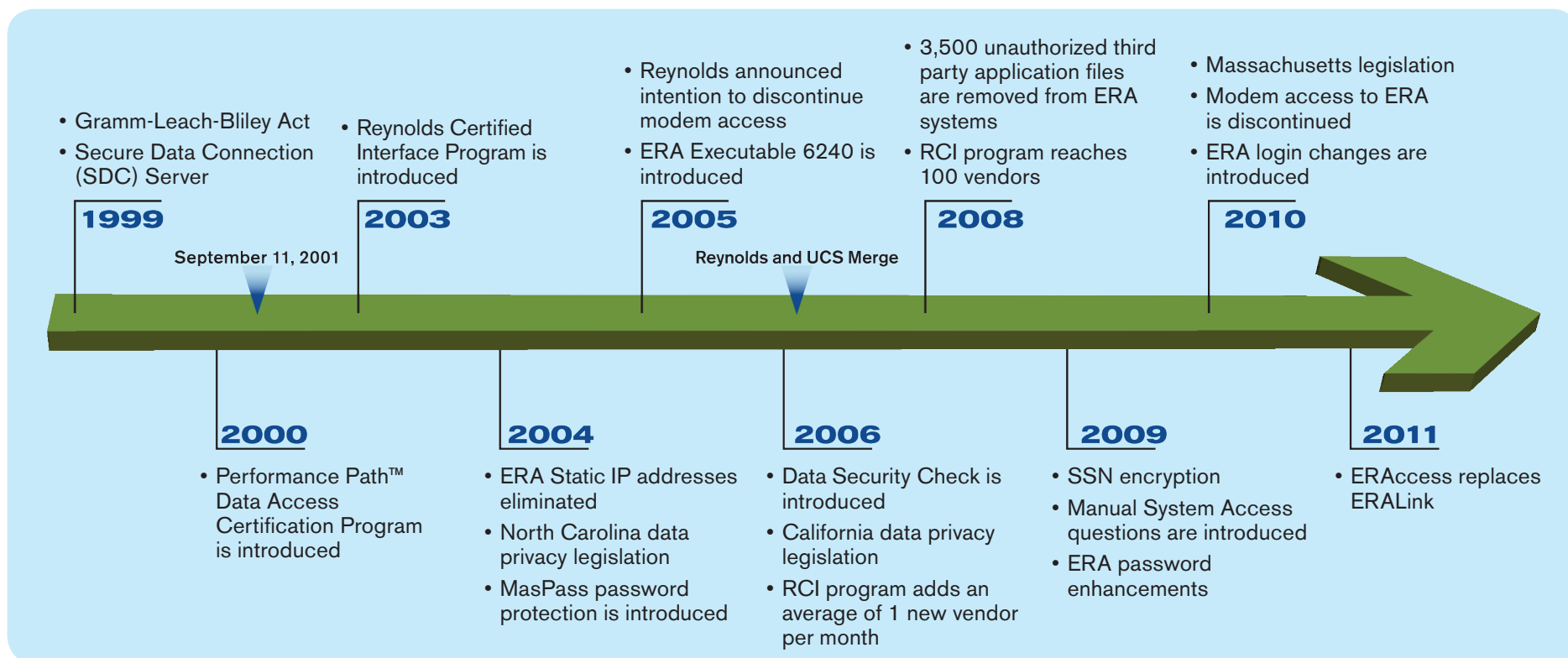


ERA® Data Management Milestones

Dealers, OEMs, and industry vendors all have a stake in protecting consumers' personal information. Reynolds has historically led the way in helping dealerships safely store and move their data as well as stay in step with regulatory requirements.



Reynolds is committed to providing an industry-leading level of data management and security. Enhancements will continue to be made to ERA to maintain the highest levels of data security possible.

Key Points on Noted Milestones

1999

- The Gramm-Leach-Bliley Act increased the requirements to protect personally identifiable information from threats in data security and data integrity.
- With the proliferation of the Internet as a way to move data, encryption of data became critical. The SDC server provided this encryption, and opened the doors for Internet-based applications such as Contact Management.

2000

- Performance Path provided secure integration between third party vendors and the ERA system.

2001

- 9/11 changed the landscape of both physical and data security.

2003

- RCI replaced Performance Path and offered more options to third party vendors to integrate with ERA.

2004

- Eliminating static IP addresses reduced the ERA system's exposure to hackers.
- After ADP is discovered selling dealer data, North Carolina enacted first-of-its-kind legislation to protect dealership data from unauthorized use and sale.
- Master passwords (MasPass) for system access using ROOT, TCL, and MAINT were changed to be unique to each ERA system and were set to change every 7 days.

2005

- At NADA, Reynolds announced intentions to discontinue use of modems in the future because of the security risks associated with modem access to the DMS.
- ERA executable 6240 provided the ability to monitor what screens/executables users are accessing.

2006

- Data Security Check allowed dealers to see what third parties accessed their systems via modems and helped them better monitor their system.
- California legislation required DMS providers to obtain specific authorization to access, modify, or extract dealership data.

2008

- The removal of unauthorized third party application files improved data integrity. Many dealers had no idea that third party vendors – some they weren't even doing business with anymore – were running applications on their system, thus disrupting processes, and potentially removing data.

2009

- Encrypting Social Security numbers is critical to protecting consumer and employee identity. The information was made available for view only by those in the dealership who had a valid business reason to see it.
- Manual System Access questions ensured that Report Generator was not being accessed through automated processes.
- Passwords were required to be changed periodically, providing better security for login credentials.

2010

- Massachusetts(MA) enacted legislation to protect personally identifiable information of MA residents, regardless of whether or not the business storing the information is in MA. The impact was felt across the country due to the possibility of a MA resident doing business with a dealership outside of MA.
- Modem access to ERA is discontinued 5 years after the initial announcement.
- ERA logins cannot be used to login to multiple PCs at the same time, reducing the risk associated with sharing login credentials.

2011

- As of January 1, 2011, ERAccess becomes the only approved terminal emulator for accessing ERA. All other methods including ERALink and third party tools such as ProCom Plus, PowerTerm, WinTerm, Reflections, and others, will no longer work.



MAKING **BUSINESS** BETTER.