



- Encrypt and secure data across multiple, diverse platforms and endpoints from a single console
- Create automatic audit trails to prove end-to-end data security
- Provide a transparent end-user interface that supports user productivity while keeping data safe

With CREDANT, financial institutions can:

- › **Protect cardholder data** from leaving the organization unprotected on USB flash drives or other forms of removable media.
- › **Provide confidentiality, privacy and auditing** of data residing on any endpoint device.
- › **Protect sensitive data from unwarranted access** to reduce risk of internal breaches.

More than 600 million cards are now in use in the U.S. alone, and in 2008, the top 10 U.S. credit card issuers supported more than \$750 billion in balances. With so much money transacted electronically, cardholder data is under constant threat—from within and outside the organizations that accept credit and debit card payments.

Yet the growing number of remote users of laptops, handhelds, smartphones, USB drives and CD-DVDs has compounded the risk of security breaches, and the reality is that millions of card numbers can be stored on a removable memory device.

Regulations like the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Data Security

Standards (PCI DSS) were established to protect financial and cardholder data. They stipulate that organizations must protect information contained on desktops, laptops, PDAs, USB drives and other devices, and fully ensure that data is protected if mobile devices are lost or stolen. As headlines will attest, unsecured financial and cardholder data that falls into the wrong hands results in steep fines and severely damaged reputations.

Achieve Compliance Without Performance Disruption

Banks, lenders, insurance companies and other financial organizations turn to CREDANT Mobile Guardian (CMG) to secure financial and cardholder data no matter where it resides—and to meet the latest compliance requirements.

CMG fully addresses requirements for:

- › **The Gramm-Leach-Bliley Act (GLBA)**
GLBA requires banks, brokerage companies, insurance companies, and any organization that services consumer loans, transfers money, prepares tax returns or provides financial advice to securely store personal financial information. Non-compliance can lead to civil and criminal penalties,

including fines of up to \$100,000 per violation and imprisonment.

CMG helps organizations achieve GLBA compliance without disruptive changes to operations and support processes by detecting and reporting on devices transparently across the enterprise network. It can also automatically install identity- and role-based security software on mobile devices to:

- › Support multi-factor authentication for users
- › Automatically encrypt all vital information stored on mobile devices
- › Track and maintain mobile device inventories to support internal usage controls
- › Provide detailed audit trails for reporting purposes

› **Payment Card Industry Data Security Standards (PCI-DSS)**

Organizations that process card transactions and businesses that accept cards for payment must meet all 12 requirements for data encryption and end-user access control, activity monitoring and logging outlined in the PCI-DSS. Organizations that fail to comply risk losing the privilege of accepting credit cards—effectively putting them out of business—and can be liable for fraud compensation.

CREDANT's CMG supports PCI-DSS compliance by helping you to:

- › Build and maintain a secure network
- › Protect cardholder data
- › Implement strong access control measures

Why Financial Organizations Turn to CREDANT

CMG is the only enterprise-scale security solution to protect all data with enforced security that follows data across all endpoints. What's more, CMG delivers enforceable and auditable protection that cannot be

disabled by the end-user. With CREDANT, financial organizations can leverage:

- › Comprehensive views and centralized management from a single console
- › Protection in heterogeneous environments, including Mac OS
- › Cohesive integration with numerous third-party technologies

CREDANT Mobile Guardian (CMG) Helps Financial Organizations:

- › Achieve and demonstrate compliance without disrupting performance
- › Safeguard data with little to no increase in administrative burden
- › Maximize operational productivity for routine tasks, such as troubleshooting and data recovery
- › Fully recover encrypted data upon OS corruption, device failure or human error
- › Eliminate the impact to end users by avoiding pre-boot login authentication
- › Support all required platforms and device types using one solution with a single management console

Learn more

With nearly 800 global customers, including some of the world's most demanding financial organizations, CREDANT solutions protect financial and cardholder data no matter where it resides. Download a demonstration of CMG in action at www.credant.com/demo. For more information about CREDANT solutions for financial organizations, email sales@credant.com, or visit www.credant.com.