

*Ensuring Information, Security
and Regulatory Compliance
Through Encryption*

Helping Banks and Financial Institutions Keep Sensitive Data Safe



To better compete in a global economy, banks and other financial organizations are deploying enterprise applications and mobile technologies — especially laptops — across their organizations. While those technologies improve productivity and lower institutional costs, storing sensitive information off secure networks increases the risk of accidental and/or intentional loss.

Credit card and bank account numbers, tracking data, merger and acquisition activity, consulting, investment advice and other types of financial reporting data for both public and private companies' demands enhanced measures to avoid risk and compliance difficulties. Securing personally identifiable information (PII) is critical because it is a prime target of identity theft, economic espionage and other cyber crimes. In 2010 alone, almost four million financial records were compromised exclusively due to lost or stolen computing devices.¹ That year, U.S. data breaches averaged \$7.2 million each and a whopping \$353 per stolen data record, for the financial sector — a 42% increase over the previous year.²

Protecting themselves from data breaches and cyber attacks is essential for banks and other financial institutions, as well as the services organizations that support them. Growing political, public and industry pressures have strengthened commercial and government requirements to notify breach victims and regulators. Data breach disclosure now often brings negative public reaction, closer government and commercial scrutiny, lawsuits and hefty fines. Four key-related challenges are listed at the right:

Key Banking and Financial Services Data Breach Mitigation Challenges

Government Regulatory Compliance

Institutions must comply with state and federal data protection laws — including the Graham–Leach–Bliley Act (GLBA), the Health Information Portability and Accountability Act (HIPAA) and new state laws in California, Massachusetts and Nevada, mandating such protection.

Commercial Regulatory Compliance

Commercial regulations, especially the Payment Card Industry Data Security Standard (PCI DSS), also carry great weight. Failure to comply with PCI can forbid violators from performing online credit card transactions, which can severely damage revenue generation profitability and customer trust.

IRS and ANSI Encryption Requirements

The IRS requires all financial data on laptops be protected with either full-disk encryption (FDE) or file encryption that meets the Federal Information Processing Standard (FIPS) 140–2.³ The Accredited Standards Committee (ASC) X9, Inc., develops and promotes financial industry standards and requires encryption of Personal Identification Numbers (PINs) for electronic transactions.⁴

Bigger Needs, Smaller Budgets

Increased use of mobile technology has exacerbated the need to secure laptops and other mobile devices but IT budgets remain tight. To meet enterprise-wide needs, financial institutions need protection that would meet government and commercial standards, works across platforms and would have known acquisition, as well as reduced ongoing operational costs. In addition, financial institutions, when called upon, need to provide proof that sensitive information was encrypted in order to avoid public embarrassment, fines and penalties, as well as potential loss of revenue.

Self-Encrypting Drives and Wave's EMBASSY® Software Protect Financial Data

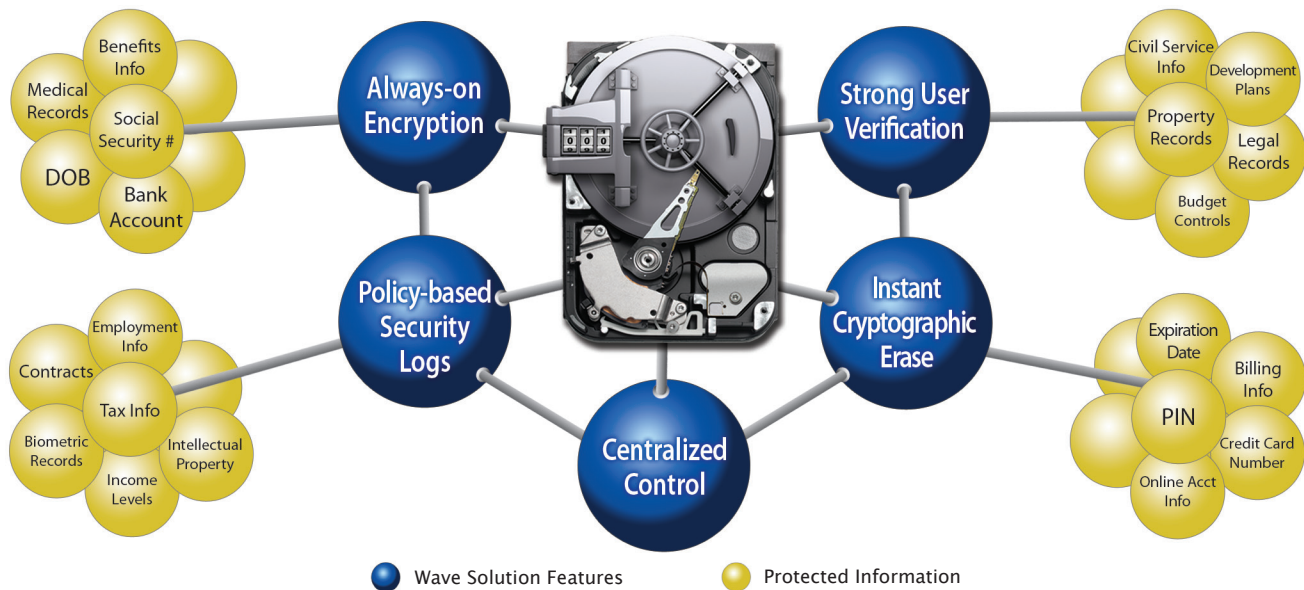
Options abound for protecting sensitive data but experts agree that hardware-based, full-disk encryption in the form of self-encrypting drives is the most secure option for safeguarding all data stored on a computer. For years, the standard choice was software full-disk encryption, but with malware able to hide from the operating system, software applications are unable to detect malware, thus leaving data vulnerable. Furthermore, software-based FDE has exploitable weaknesses, meaning it can't guarantee that lost data is unreadable. These facts leave financial institutions at continued risk of costly and catastrophic breaches.

To overcome these hurdles and comply with regulations, financial institutions are turning to self-encrypting drives (SEDs). These drives offer an alternative hardware-based FDE approach, making them more secure and less expensive to implement and maintain. SEDs house all encryption processes and keys in a protected hardware boundary impervious to traditional software attacks. Further, they cost only marginally more than unencrypted hard drives, need little IT overhead and are completely transparent to end users. SEDs are a proven IT security solution; for instance, Seagate alone has shipped more

than one million SEDs, many of which use Wave's EMBASSY software. Further, given the status of computer equipment manufacturers, Gartner believes that, within five years, all hard disk drives (HDDs) will be shipped pre-loaded with some kind of industry-standard FDE technology.

Wave Systems, a pioneer in hardware-based laptop security, has partnered with leading hard drive manufacturers Hitachi, Samsung and Seagate to provide enterprise security management for their SEDs. Through partnerships with Seagate, Data Management, Inc. and other trusted IT providers, Wave serves a growing number of customers in the banking and financial services industries. Moreover, Wave is the leading ISV for Seagate Momentus Self-Encrypting Drives, the first SEDs to gain FIPS 140-2 certification.

EMBASSY transforms SEDs into a complete managed enterprise encryption solution: one that centrally provisions security policies limits access to only authorized users and — perhaps, most importantly — proves whether or not sensitive information stored on a laptop was encrypted at the time it went missing.



¹ Chronology of Data Breaches, Privacy Rights Clearinghouse, February 2011
² 2010 Annual Study: U.S. Cost of a Data Breach, The Ponemon Institute, March 2011
³ Internal Revenue Service, <http://www.irs.gov/businesses/small/article/0,,id=217110,00.html>
⁴ ASC X9, <http://www.x9.org/about/x9presentation/>