



## Mobilizing Financial Data with Secure USB Flash Drives

to Protect Customer Privacy and Security

## WITH MILLIONS OF USB FLASH DRIVES IN USE,

digital data is constantly on the move. Flash drives let private users easily store, transport and share their photos, videos and text files. But in the financial world, these very same benefits that enable employees to work effectively outside the office pose risks of the loss, theft or misuse of unprotected, confidential data.

The SanDisk® Cruzer® Enterprise USB flash drive with Central Management & Control (CMC) Server Software provides users with unparalleled safety and security in storing and managing sensitive information.



## Combating Data Loss

Today's headlines recount the grim realities of various financial institutions and private organizations losing data or having their data compromised. The following examples show how bad the consequences can be. In March 2008, it was reported that a stolen drive exposed the financial records of 1 million customers of a regional bank in the southeast U.S.<sup>1</sup> This is dwarfed by previously reported multi-million customer account breaches, such as the 40 million credit cards exposed by CardSystems, Inc.<sup>2</sup> The extremely devastating consequences of data compromise and security breaches are no less severe with smaller but more frequent data losses. Research of data breaches by the Ponemon Institute has established that, on average, a single loss of just 30,000 customers' personally identifiable information costs an organization nearly \$6 million in internal investigation, customer notification and regulatory compliance expenses<sup>3</sup>.

## Satisfying Industry Requirements

Data is more mobile than ever before, with high capacity USB flash drives a key enabler of data mobility and, in turn, worker productivity. However, providing assurance that financial institutions comply with regulations for protecting customer information has become exponentially more difficult.

Many financial institutions report literally hundreds of regulations, which involve information security to some degree. Some regulations specifically mandate encryption for customer information. Other regulations are less proscriptive, and require risk assessments of sensitive data and the establishment of compensating controls that must be regularly tested. With regard to mobile devices such as USB flash drives, the emerging best practice is to mandate pervasive encryption as the most cost-effective way to satisfy regulations and mitigate risks of data breaches.

The challenge that financial institutions are facing to secure sensitive data can become daunting when taking into account how much information is transported on personal storage devices. The majority of personal storage devices are neither built to keep data completely secure nor to give financial organizations the control they need to audit files being copied or deleted from various networks. Rather than be forced to undergo time consuming data classification exercises in all cases, it is apparent from the recent policies mentioned above that encryption of data is the best choice for mobile devices.

## The Total SanDisk Solution: Central Control, Increased Protection

SanDisk Cruzer Enterprise USB flash drive with SanDisk Central Management & Control (CMC) software is designed to meet the requirements to comply with industry regulations such as the Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley (SOX) for the secure storage of sensitive information.

CMC is an innovative client-server software solution that utilizes the unique hardware and embedded software capabilities of Cruzer Enterprise USB flash drives. The CMC device agent resides on the USB flash drive, enabling corporate IT departments to centrally manage company-issued Cruzer Enterprise USB flash drives locally and remotely, within and outside the corporate environment.

CMC provides many functions that include constant monitoring, auditing and tracking. Depending on an organization's particular needs, these functions can incorporate various parameters set for various levels of restrictions and monitoring.

Attaining centralized deployment and provisioning is another feature with tremendous benefits. Management can obtain centralized updates and configurations of all drive parameters, remote password administration and remote deactivation of lost or stolen drives through implementation of optional SanDisk CMC software.

Central Management & Control (CMC) software:

- Manages the complete lifecycle of company issued USB drives
- Protects against unauthorized use of sensitive company data
- Protects against possible regulatory compliance failure and associated damages caused by data breaches due to lost or stolen USB drives
- Supports regulatory compliance by tracking and auditing activity, as well as demonstrating the use of strict encryption measures

### Obtaining Best of Breed Security Standards

The combination of Cruzer Enterprise USB drives and CMC software enables the financial institutions to:

- **Provide mobile data assurance for today's e-Discovery challenges.** The revised Federal Rules for Civil Procedure gave digital information the same legal standing as paper-based information. SanDisk's Cruzer Enterprise provides tamper indication features and robust encryption, assuring the integrity of your data.

- **Assert regulatory compliance at every endpoint** Financial Services are responsible for compliance with GLBA, PCI/DSS and typically SOX as well. The regulations require the secure storage of sensitive information, no matter where it resides. SanDisk's Cruzer Enterprise maintains continuous, robust AES encryption to guarantee compliance with today's regulations as well as tomorrow's.

- **Protect sensitive data with federal information processing standards.** Our highly secure Cruzer Enterprise flash drive is also available in a FIPS Edition with FIPS 140-2 Level 2 certification. This new level of USB drive protection meets the standards and guidelines of federal computer systems set by the National Institute of Standards and Technology

### Encryption That Ensures the Ultimate Protection

SanDisk Cruzer Enterprise USB flash drive uses powerful, hardware-based 256-bit AES encryption, the most secure block cipher encryption standard to date, complex password protection and a lock-down mechanism when a set number of incorrect password attempts is exceeded to ensure that data on lost or stolen drives cannot be hacked into. These security features protect sensitive data even when it needs to be transferred to different computers or workstations.



### Increasing Productivity

Financial organizations do not want to be forced to choose between mobility, ease of use, productivity and security. Complex mobile encryption that is not embraced by users decreases security and hinders worker efficiency. The SanDisk Cruzer Enterprise USB flash drive increases overall enterprise data security by providing centrally managed, secure mobile storage that is transparent to the end user. In this way, both productivity and security remain at high levels.

### Privacy Monitoring Throughout the System

The Cruzer Enterprise USB flash drive, when managed by CMC software, is designed to store confidential enterprise-related information securely while auditing, tracking and backing up all data. It maintains a full audit trail of files read, written or deleted from the drives. Protection this thorough is essential not only to meet legal requirements but to provide financial enterprises with the ultimate protection.

In addition, circumventing reliance on the user through mandatory 100% data encryption of all files on the drive helps prevent human error. The Cruzer Enterprise flash drive also enables business continuity through seamless backup of drive content and the ability to restore or recreate data on lost or stolen drives through central backup.

By incorporating security software that cannot be modified or deleted the Cruzer Enterprise flash drive affords tremendous safeguards. It also supports usage policies that allow for a restricted operating environment to prevent drives from operating on unauthorized PCs.

# Mobilizing Financial Data with Secure USB Flash Drives

to Protect Customer Privacy and Security

## Key Mandates to Protect Data in the Financial Industry

**Gramm-Leach-Bliley Act (GLBA)** requires identification and audited protection of all Non-Public Personal Information (NPPI) belonging to customers. The FFIEC IT Examination Handbook, used by banking auditors, calls for use of encryption to “mitigate the risk of disclosure or alteration of sensitive information”.

**Sarbanes-Oxley Section 404** requires attestation of documented controls for all financial systems.

**Payment Card Industry / Data Security Standards (PCI/DSS)** requires encryption of credit card data. (Ver 1.1, Section 3)

**Various breach notification laws such as California SB-1386** require costly notification of data breaches related to lost or stolen data storage devices, with a common exception made for encrypted information.

<sup>1</sup> Computer World, “Programmer who stole drive containing 1 million bank records gets 42 months,” Jaikumar Vijayan, March 26, 2008  
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9072198>

<sup>2</sup> InfoWorld, “Lawsuit filed over CardSystems data breach”, Robert McMillan, June 28, 2005  
[http://www.infoworld.com/article/05/06/28/HNdatabreachsuit\\_1.html](http://www.infoworld.com/article/05/06/28/HNdatabreachsuit_1.html)

<sup>3</sup> Price Waterhouse Coopers, “Quarterly in law,” Feb 2008, p. 3,  
[http://www.pwc.co.uk/pdf/quarter\\_in\\_law.pdf](http://www.pwc.co.uk/pdf/quarter_in_law.pdf)

SanDisk and the SanDisk logo are trademarks of SanDisk Corporation, registered in the United States and other countries. TrustedFlash is a trademark of SanDisk Corporation. microSD and SD are trademarks. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).

© 2008 SanDisk Corporation. All rights reserved. 80-11-01605 Rev. 2.0, March 2008

## Solution Highlights

- Manages the complete lifecycle of company issued USB flash drives
- Protects against unauthorized use of sensitive company data
- Avoids the regulatory and market repercussions caused by data breaches due to lost or stolen USB flash drives
- Adheres to regulatory compliance by tracking and auditing activity, as well as demonstrating that strict encryption measures are in place

## How to Contact Us

**SanDisk Corporation**  
Corporate Headquarters  
601 McCarthy Blvd.  
Milpitas, CA 95035

For more information, please go to  
[www.sandisk.com/enterprise](http://www.sandisk.com/enterprise)  
or e-mail [enterprise@sandisk.com](mailto:enterprise@sandisk.com)

**SanDisk**