Case Study: Printer & Personal Systems

ESSINTIAL ENTERPRISE SOLUTIONS

Financial Services Data Security Program Supports FTC Requirements & Improves Customer Satisfaction

The Customer

A multinational financial services corporation headquartered in New York City, the client operates in 42 countries with more than 1,300 offices and 60,000 employees globally.

Since 2009, this client has relied on Essintial℠ for end-user and data security services, now supporting 57,000 desk side personal computers in the U.S. with onsite hardware repair services for both warranty and post-warranty devices.

With a strong focus on data security, the support agreement has led to a data management program providing hard drive shredding services, destruction and disposal.

What	24x7 data management, maintaining data security on 57,000 PCs
Where	Thousands of locations nationwide
Outcome	All FTC requirements met; work ongoing with long-term client

The Challenge

Customary of financial institutions, the financial planning division is responsible for the secure collection and maintenance of customers' personal information including bank and credit card account numbers, income and credit histories and Social Security numbers.

The Federal Trade Commission (FTC) Safeguards Rule requires companies to assess and address risks to customer information of all operational areas, including three areas particularly important to information security:

- Employee management and training
- Information systems
- Detecting and managing system failures

The customer needed a manageable chain of custody for hardware with database information across several organizations and 57,000 PCs. This was not an internally available attribute for this customer, requiring outside assistance to meet FTC requirements.

The Solution

To comply with the FTC Safeguards Rule, Essintial designed and developed a complex data management program and related processes to secure and protect sensitive customer data. These processes and tools help manifest a robust data security vehicle for FTC guideline and covenant compliance. They were also used by Essintial's Managed WorkForce® for

the client's end-user and field repair services through:

- A designated representative coordinating client information security program
- Customer information risk identification and assessment in each relevant area of the operation
- Evaluation of current safeguards' effectiveness for controlling risks
- Design and implementation of a safeguard program, regularly monitored for compliance
- Program flexibility allowing adjustments to support evolving circumstances, such as changes in business or operations, the results of security testing and monitoring, or new FTC requirements

Services Provided

- Nationwide 24x7x365 data management
- Data security for 1,200+ service events annually
- Continuous hard drive shredding services
- Sensitive customer data protection
- Chain of custody for memory resident devices
- Exceed service level objectives
- Mitigate risk by leveraging data security best practices

The Value

Now, with Essintial's streamlined end-user and desktop support programs fully deployed, the client's data security programs meet all FTC requirements, allowing them to focus on internal data security measures and safeguards. The onsite repair and secured hard drive data destruction and disposal processes are efficient, and have alleviated the clients' risk of high cost security breaches.

The Results

This highly efficient program developed by Essintial is regarded as "the small price of insurance" against the potentially high cost of security breaches. Essintial continues to successfully provide hundreds of monthly end-user services to the client while adhering to the strict client and federal data security protection standards implemented. Most importantly, all customer data is held in the highest levels of security and is protected throughout the services lifecycle.