

## SOLUTION BRIEF

# Centralized Data Repository Powers Enterprise Analytics

### The Challenges You Face:

- Regulations governing the use and storage of FCRA data are complex
- Data pulled isn't 'model-ready' for use in analytics
- Data isn't maintained in a central archive
- Traditional data warehouses easily become big and clunky, making it difficult to find needed data
- Extracting data is extremely difficult and time-consuming
- Exposure to risk associated with the collection and use of PII data is high

800.367.1800  
sales@dms.net  
www.dms.net

© 2019 Digital Matrix Systems, Inc.

### Introduction

Traditional data warehouses can be cumbersome, and aren't typically optimized for the extraction of data for use in analytics. What Digital Matrix Systems (DMS) provides is quite different. DMS Data Warehouse™ stores data for leading banks and insurers in accordance with regulatory and vendor requirements, and powers enterprise analytics. Necessary data is ready for your statisticians to work with, without requiring extensive clean up or lengthy extraction times. Our capabilities enable you to store data properly, leverage that data in analytics, and reduce exposure to the risk associated with the collection and use of personally identifiable information (PII). Not a replacement for your enterprise warehouse, DMS Data Warehouse™ provides a nimble solution to augment your current data warehouse and support the analytics that drive key business decisions.

### Increase the Value of Your Data

Many of our clients want to store their FCRA data, but don't want to handle the complexities created by the regulations around storage of the data. As a result, clients are increasingly migrating the storage and management of all PII data to DMS, and we can help you manage your compliance with PII and FCRA regulations.

- Clients find value in the way we store the full raw files, not just the attributes used to make decisions. Our solution has the ability to output 'model-ready' data sets.
- Gain actionable business intelligence from your data for many analytic purposes, modeling, regulatory compliance, dispute resolution, and research.
- Gain the ability to utilize the data in the warehouse for model and scorecard builds.
- DMS standardizes and normalizes data to reduce extract-transform-load (ETL) efforts and simplify coding.



## Easily Suppress Sensitive Information

Access restrictions are defined by the client and based on the user's role and job function. User access can be set to only display anonymized information on a consumer, or with full access to the information.

DMS can suppress information that is returned in the credit response. Each client can select the specific data they want suppressed to ensure that they are not receiving any PII or PCI data in the response. Only the data elements the client needs to make a decision on the consumer will be returned. Even though the data in the client response is suppressed, the entire response is written to the DMS Data Warehouse™.

Role-based access control is performed by the client. Users can be setup for an anonymized view which removes any PII and PCI data from the display and the extracts. If a user needs to see the full response they can be setup for a normal view of the response that does not anonymize the data. All data is securely stored on the DMS Data Warehouse™ so no information is loaded to the client systems.

## Go Beyond Data Storage

Combined with your own scores and attributes, data is stored for easy access when you need it. Stored information can be accessed and viewed immediately at the individual report level, or custom queries can return large volumes of information within an optimized data structure using your analytics tools. By analyzing large data samples with custom queries, risk managers can identify trends, create models and scorecards, sharpen business decisions, and track portfolio performance. Clients can extract raw credit reports from the warehouse for analysis, and test new custom scripts, attribute libraries, and scorecards on anonymized production reports. Attributes can be extracted to compare production attribute values to the attribute values of a new script.

**Structure data views based on job role. For example:**

- IT logs in and can pull full reports for exceptions testing and regression
- R&D can do extracts, but they are fully anonymized
- Customer Service can query, but only via the web interface for call center support

## Easily Maintain Compliance and Security

DMS helps lead the fight in data security for our clients. We have a constantly evolving security program that has been established to ensure the integrity of our systems and to protect the data that our clients entrust to us. You can reduce your security burden and rely on our expertise and our suite of security governance policies, risk management controls, and compliance efforts.

By adopting PCI DSS 3.2 standards, DMS is prepared to maintain the highest level of external security for our clients. Machine learning has been adopted in our edge security services to ensure rapid response to new threats. You will be able to leverage our continuous investment in data security and avoid making those costly investments on your own, including security certifications and third party security assessments.