

DATA INTEGRITY AND AVAILABILITY MANAGEMENT
FOR FILEMAKER PRO DATABASES AND FILEMAKER SERVER
IN BUSINESS CRITICAL ENVIRONMENTS



—Executive Summary—

Business owners with large amounts of mission-critical information stored in FileMaker Pro databases are faced with multiple, complex challenges and responsibilities in seeking to preserve both the integrity and the availability of their business data. Their IT managers and database administrators as well as their developers must constantly focus on this key item as well.

Lulled into a sense of complacency by partial solutions such as backups, *they all come to realize only after a significant data loss that restoration of critical data is a major undertaking and responsibility they have overlooked.* Preservation of data integrity and preservation of data availability, along with preservation of data confidentiality, are the three core elements of any professionally designed security program.

The challenges to meeting these requirements take unexpected routes much of the time. Administrators frequently need to restore data through multiple levels of Undo and Redo. They must also reconcile multiple versions of past backups with different timestamps and datasets to the actual current work-flow state that has happened *since the last backup.* Both such requirements present unique challenges.

FileMaker Pro databases deployed by FileMaker Server are increasingly being used to support the business-critical operations of work groups in large enterprises, of distributed multiple off-site office locations, and of entire organizations as well. These files are often complex and large in the multi Gigabyte range. Often individual tables can contain millions of records. Such systems are increasingly moving into the domain of what was once thought of as “Big Iron” systems, *but frequently they employ none of the protections traditionally found with such “Big Iron” systems.*

FileMaker Pro developers are—for the most part—unacquainted with these types of features, and in some instances, even with the need for their use. Preserving data integrity and availability for such critical systems can be challenging. But it is also essential for business continuity reasons.

This White Paper identifies and explores some of these challenges and offers some prescriptive guidance as to how to address them. *It focuses particularly on the*

difficult issues of deletion management and of backup reconciliation, using both roll-back and roll forward. This White Paper also examines what are some key threats to data integrity and availability generally, and specifically within the FileMaker environment.

—OVERVIEW OF PROBLEMS ENCOUNTERED—

Business critical data are at risk of loss or compromise and are expected to remain at significant risk in the future. Both the availability and the integrity of these data are threatened by a variety of agents. *Availability*, as the term implies, means that the data actually exist in the tables and files where they are supposed to be and that they are not inadvertently or purposefully deleted in unauthorized fashions. *Integrity*, as the term implies, means that the data are trustworthy, that they conform to the business rules the database should enforce, and that owners of the data can rely on their not having been altered in unauthorized fashions, even by authorized users of the database system. It also means that the data present are the data that are *supposed* to be present, and not some other data.

Business owners and IS/IT managers can often be lulled into complacency about managing these risks by the easy lure of partial solutions. Regularized and automatic backup of data is one such solution. *But these solutions are partial answers at best.*

Backups must be *reliable*, *available*, *protected*, and *current*. And they must actually function to *restore*

data in the event of damage or loss. Yet many organizations fail to test their backups for restorative capability, and they discover only after an incident occurs, that carefully run backups cannot restore data.

Records that are deleted, either accidentally by authorized users or maliciously by disgruntled ones, frequently are lost forever, particularly if they are not covered in any pre-existing backups. Other times, data can be transposed or written that are incorrect, even though they pass various validation tests. These data must be rolled back to assure data integrity.

Authoritative and immutable logs of creates, edits, and deletes in a database system are a frequent requirement both of various regulatory frameworks such as Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley, as well as of European Union Privacy and Payment Card Industry standards. Likewise such logging capabilities are requirements of many corporate security policies, and their presence is an important element for *qualification of a particular software's acceptable use in a corporate environment.*

—The Deployed FileMaker Environment—

FileMaker Pro solutions are increasingly being deployed in several different major types of business environments:

- In the large workgroups of large organizations,
- In medium-sized businesses at the company-wide level,
- In K-12 and higher education facilities, and,
- In distributed, multi-site locations of any of these type entities.

In some instances these deployments occur in organizations with full, in-house professional IT staff whose support of the FileMaker family of products is just one of many other responsibilities. In other situations, IT support is provided on an out-sourced basis by firms whose familiarity with FileMaker Pro and FileMaker Server is limited at best. In yet other scenarios, there is no professional IT support at all. Yet in each of these instances there are going to be requirements for database backup, for database transaction tracking to help assure data integrity or to meet specific regulatory or security policy requirements, and for reconciliation of backups to *current, real-time* workflow.

In many organizations with professional IS/IT staff and well-defined corporate software policies, authoritative and immutable auditing and transaction tracking as well as roll-back and roll-forward capabilities frequently are *core requirements* for *initial qualification* of a software package for entity-wide use and for *on-going re-qualification* of that

software to remain in use. *The lack of intrinsic tracking and roll-back or roll-forward capabilities in FileMaker Pro and FileMaker Server can disqualify them for use in many environments.*

FileMaker Pro has some indigenous tracking capabilities **at the record level** for creation and modification of records through the auto-enter options of field definitions. FileMaker Server has a robust automated backup capability, one of the principal purposes for its use. However, **field level modification tracking** in FileMaker Pro is cumbersome, and it most times requires either elaborate scripting or an entire series of shadow tracking fields utilizing the auto-enter and replace existing value option, frequently utilizing the Evaluate function as part of its field definition. Moreover, tracking the **before** and **after** values of any edited data element requires even more complex systems. Adding any of these to a table causes extensive overhead in the file, potentially affecting performance.

When data are deleted in FileMaker Pro systems, and particularly when entire records are deleted, retrieving their contents is next to impossible to do short of a manual re-entry or a re-importation from a prior backup. While many professional FileMaker Pro developers take great care and precaution to prevent inadvertent or malicious deletes of records, situations do occur where records can be deleted by accident. Data integrity and data availability in the system both require that these records be able to be restored.

The time between when the action occurs and when it is either noticed or reported to the database administrator can be critical in determining whether and how the data can be retrieved.

Backups of large data-set files with mission-critical business information, particularly with the file verification option enabled, can take significant amounts of time. In many instances this renders the file unavailable, an unacceptable situation in most environments, especially during heavy workflow periods during the day. Moreover, while FileMaker Server produces excellent backups, in an operational environment there is no immediate or facile method to reconcile any given backup to the last known state of the database when an anomalous event *occurs* or when it is *discovered*. When business owners, IS/IT

administrators, or others responsible for maintaining FileMaker Pro databases must restore from the last good backup, they are faced with the challenge of reconciling that backup with actions that have happened in the database *since the backup was written*.

They have the need to be able to perform a *roll-forward* on the backup copy to synchronize its contents with those of the database at the instance of the anomalous occurrence that has necessitated the restoration. If some accident requires the restoration from a backup, any data entered, deleted, or modified since the last backup are lost or desynchronized and their accompanying transactions are not recorded. The lack of this *roll-forward* capability has significant adverse impact on data availability and data integrity.

—Data Integrity Issues—

Unified field level tracking of changes can assist in preserving data integrity and data availability by determining the identity of users who take *authorized* actions within the database system, especially and particularly *editing* and *deleting* records. **Such tracking can monitor the before and the after values of a particular action in a particular field of a particular record. This allows for restoration to the correct state of integrity.** FileMaker Pro does not have the ability to perform this type activity natively. It is just as important to track the actions of *authorized* users as it is to prevent *unauthorized* persons from accessing the databases or to prevent users from promoting or escalating their privileges. In conjunction with strong

Identity and Access management controls, this provides for non-repudiation of user actions.

Simple ignorance of how to use a database system can contribute to data integrity and availability problems. Many systems lack multiple levels of undo or redo for data entry. Careless UI design or careless construction of access privileges for a specific role (or class) of users has frequently led to unexpected data substitution or unexpected data deletion or transposition. When these incidents occur, they frequently cannot easily be reversed, or even reversed at all, even if they are *immediately* recognized.

Roll-backs of systems to a previous, correct data state may be

required when extraneous and incorrect data are entered into the database. When the data meet business rule requirements and other validation options, *but are still incorrect*, roll-backs provide the only viable method, short of some manual re-entry of desired changes into a valid backup, to restore the database system to its correct level of integrity.

Access privileges as defined in the Privilege Set attached to the active Account can materially assist in preserving data availability and data integrity by, for example, preventing the inadvertent deletion of data. There is no method however, short of merging selected data into a restored backup, for retrieving data deleted by a user *authorized* to take that action. Additionally, field-by-field change history can be cumbersome to maintain.

The wide proliferation of databases and the even wider proliferation of multiple Application Interfaces that can access the data these systems store have opened rather wide the doors by which users can be authorized to access these data and to write, edit, or delete them. When coupled with the dramatically increased business criticality and significance these data assume at all levels of business, both large and small, the need for robust systems to protect these data becomes paramount.

From a regulatory compliance standpoint, companies must frequently demonstrate to independent, outside auditors that they are actively monitoring data changes as well as having evidence of that monitoring.

Assuring effective controls¹ over database activity (creates, writes, changes, deletes) is a key component of data integrity and therefore of Sarbanes-Oxley compliance as well as of other regulatory schemes. *A prescription for failure of such an audit and for an adverse opinion from the auditor is the failure to have a data transaction auditing system in place or the insecure storage and maintenance of the logs such a system generates.*

As a result of Sarbanes-Oxley, or of the HIPAA regulations covering various personally identifiable medical and healthcare information, or of Gramm-Leach-Bliley Act requirements for financial institutions, or of Payment Card Industry requirements for credit card processing, or of Buckley Act requirements for management of student data, many organizations have adopted extensive security policies governing specific steps that must be taken to assure confidentiality, integrity, and availability of digital assets. **Additionally many companies or organizations not covered by various regulatory frameworks have also adopted, as a matter of Best Practices, similar requirements.** In the not-for-profit sector this often includes the business leagues of regulated industries (501c6), educational, literary or scientific professional organizations (501c3), and foundations (501c9) supported by various businesses or industries.

As earlier indicated, many IS/IT managers or business owners succumb to the siren call of "...we have backups..." when contemplating these

¹ Section 404 of Sarbanes-Oxley requires an external auditor's opinions of the effectiveness of these internal controls.

issues. *Backups of business critical data must be reliable, available, protected, current, and restorative.* Many owners and IT managers either do not know how properly to backup FileMaker Pro systems, or they simply do not make such backups. And even when backups are valid, they do not include data changed after the backup and prior to a crash or corruption.

Presently in FileMaker Pro, providing authoritative and immutable logging of data transactions, providing unified field level tracking, enabling multiple re-do's or un-do's, or providing a roll-back or roll-forward capability all entail extensive file overhead with

shadow fields for audit tracking, auto-enter calculations, deletion signatures, and scripts. Additionally, the reliability of such calculations across files that reference one another (*via* file references) is questionable. *It can also be difficult to assure the integrity of the logs themselves, an absolute requirement for forensic purposes.* Business owners, developers, database administrators, and IS/IT Managers can profit by automation and streamlining of these processes both in terms of ease and speed of development and in terms of database deployment management requirements.

•fmDataGuard 2.0™—Meeting these challenges and expanding available tools for business owners, developers, and database administrators.

Enter **fmDataGuard 2.0™** from Berkeley, California, based World Sync, Inc. A specially designed piece of software intended to act in conjunction with FileMaker® Server and FileMaker® Pro, fmDataGuard 2.0 provides core features to business owners, database administrators, developers, and IS/IT managers:

- Complete logging of all changes to rows in data tables, including creates, edits, and deletes, including timestamps and active Account.
- Restoration of individual field and record edits.
- Restoration of deleted records and their data.
- Roll backs of all changes by date range and/or user account.
- Roll forwards of backups to the current active state using a start date and an optional end date.
- Management for backups of larger files and groups of larger files.

Overcomes limitations and restrictions inherent in attempting to use event triggers (script triggers) to perform auditing functions—

- Script triggers are tied to layouts, not the field table, so there is enormous room for inconsistency and lack of triggering altogether across the vast array of files and layouts present in real-world solutions;
- Script triggers do not run on batch operations like import and replace routines;
- Script triggers do not run with Custom Web Publishing and ODBC/JDBC; and,
- Compliance and sound backup strategies do not accept “*usually*” as an approach to logging.

More Information: <http://fmdataguard.com>

This White Paper issued by and under the authority of WorldSync, Inc. developer of fmDataGuard.