

# Comprehensive Real–Time Data Integrity Management In FileMaker Pro and FileMaker Server

By:

Steven H. Blackwell

Platinum Member, FileMaker Business Alliance  
FileMaker 8 Certified Developer  
FileMaker 7 Certified Developer



---

© Copyright 2007, WorldSync, Inc., Berkeley, CA. All rights reserved under both Pan-American and International copyright conventions.

# Comprehensive Real–Time Data Integrity Management In FileMaker Pro and FileMaker Server

---

## ❖Executive Summary

**T**he business owners of databases and their database administrators are faced with multiple, complex challenges and responsibilities in seeking to preserve both the integrity and the availability of their business data. Lulled into a sense of complacency by partial solutions such as backups and Identity and Access Management, *they 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. The need for data restoration, through multiple levels of Undo and Redo, and the reconciliation of multiple versions of current backups with different timestamps and datasets to the actual current work-flow state that has happened since the last backup both present unique challenges. Similarly, fulfillment of regulatory requirements or of corporate security policies about maintaining an authoritative and immutable record of who wrote, edited, or deleted what specific data to a particular row of a table and when that action occurred, presents a totally different set of challenges to the

maintenance of data integrity and data availability.

In the wide variety of database environments designed in FileMaker Pro and deployed by FileMaker Server—ranging from small businesses without IT support, to work groups in large enterprises, to distributed multiple off site office locations, to professional practices governed by a wide range of regulatory practices—meeting the requirements of preserving data integrity and availability can be challenging. But it is also essential both for legal and for business continuity reasons.

This White Paper identifies and explores some of these challenges and offers some prescriptive guidance as how to address them. *It focuses particularly on the difficult issues of deletion management, of backup reconciliation, both roll-back and roll-forward, and of regulatory compliance.* 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 and are expected to remain at significant risk in the future. Both their availability and their integrity 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.

Business owners and IS/IT managers can often be lulled into complacency about managing these risks by the easy lure of partial solutions. Identity and Access Management through Accounts and passwords as well as regularized and automatic backups of data are solutions. *But these solutions are partial answers at best.*

Backups, for one example, 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 writes, edits, and deletes in 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 (Basel II) and Payment Card Industry<sup>1</sup> 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 typically deployed in several different major types of business environments:

- ◆ in the workgroups of large to medium sized organizations,
- ◆ in small businesses at the company-wide level,
- ◆ in professional practices such as physicians' offices or architectural or legal firms,
- ◆ in K-12 and higher education facilities,
- ◆ in trade associations or professional societies, 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

---

<sup>1</sup> Specifically Payment Card Industry Data Security Standard (PCI DSS) v 1.1, Requirement 10, to track and monitor access to cardholder data.

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 of data from a prior backup. While many FileMaker Pro professional 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.

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 must 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 on 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.

Threats to data integrity take many forms. Data can be copied or stolen. Laptops with key data can be damaged or stolen. Drives on servers and workstations can crash, and in some instances, literally burn. Data on those drives are either irretrievably lost or become prohibitively expensive to recover.

**Insiders** remain the principal threat to data confidentiality, integrity, and availability. In a recent survey of IT professionals 34% identified the **careless employee** as the greatest insider threat to

data integrity and availability. The top<sup>2</sup> six insider threats:

Careless employees <sup>3</sup> .....	34%
Negligent employees <sup>4</sup> .....	32%
Temporary employees .....	29%
Disgruntled employees .....	21%
Terminated employees.....	19%
Outside Partners.....	16%

And when the disgruntled employee enters the situation, the instances of sabotage or fraud caused by the intentional, and frequently *undetected*, alteration of data become a significant issue.

Most telling however was this finding from the same study: 31% of organizations surveyed had **no one** designated as being responsible for managing *insider threats*.<sup>5</sup> Not the IT department, not the outsourced IT consultant, not the CFO, not the business owners. No one.

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

<sup>2</sup> Top two threats per each respondent. Totals will therefore exceed 100%.

<sup>3</sup> Careless employees (aware of security policies but ignores them)

<sup>4</sup> Negligent employees (ignorant or unaware of policies)

<sup>5</sup> Ponemon Institute, LLC. *National Survey of Managing Insider Threats, 2006.*

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 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.

Many companies and organizations operate within the requirements, confines, and restrictions of various regulatory frameworks at national, state, and international levels. Some principal examples include medical practices, financial institutions, mortgage lenders and brokers, K-12 schools, and universities. And most all publicly traded companies are subject to the Sarbanes-Oxley law regarding the integrity of financial data that are reported in their financial audits and other filings. Additionally, the European Union has a wide range of requirements for protection of personally identifiable data and for transmission of such data.

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 controls<sup>6</sup> over database activity (reads, 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 PCI DSS 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**

---

<sup>6</sup> Section 404 of Sarbanes-Oxley requires an external auditor's opinions of the effectiveness of these internal controls.

**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 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.

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™–Meeting these challenges and expanding available tools for business owners, developers, and database administrators**

Enter fmDataGuard from Berkeley, California based WorldSync, Inc. A specially designed piece of middle-ware intended to act in conjunction with FileMaker® Server and FileMaker® Pro, fmDataGuard 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.

fmDataGuard addresses a number of the specific issues raised in this White Paper, including:

◆Helping business owners and managers meet audit log requirements for various regulatory mandates including Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley, as well as European Union Privacy (Basel II) and Payment Card Industry standards.

◆Assisting business owners to maintain the integrity and availability of their critical business data.

◆Assisting IS/IT managers and DBA's to manage reconciliations of backups and roll-backs of any inadvertent data deletions.

◆Enabling FileMaker Pro based business solutions to meet security requirements and to qualify for acceptance in businesses, government agencies, business and professional associations, and educational institutions of all sizes.

◆Assisting FileMaker Pro developers to offer competitive solutions that meet security requirements without the need for extensive scripting or a large number of shadow tables or fields that add to system overhead.

For more information contact:

WorldSync, Inc.  
Jason Erickson, CEO  
510-548-4920 x12

<http://worldsync.com/fmDataGuard>



This White Paper was commissioned by WorldSync, Inc. but was written and prepared independently by Steven H. Blackwell.

### About WORLDSYNC, INC.

Berkeley, California based WorldSync, Inc. is a Platinum Member of the FileMaker Business Alliance and has been providing development and consulting services with the FileMaker family of products for over ten years. The company is the developer of the patented SyncDeK™ process for database management and synchronization across local and wide area networks.

WorldSync's clients include such organization and government agencies as the M. D. Anderson Medical Clinics and the National Aeronautical and Space Administration (NASA).

WorldSync's CEO, Jason Erickson, is a frequent speaker at computer industry events and FileMaker User Groups.

---

### About STEVEN H. BLACKWELL

Steven H. Blackwell is a Platinum Member of the FileMaker Business Solutions Alliance. From December of 1997 to April of 2007, he was a Partner Member of both the Claris Solutions Alliance and the FileMaker Solutions Alliance. He was among the very first class of thirty persons in the world designated as a FileMaker 7 Certified Developer™ by FileMaker, Inc. He also holds the FileMaker 8 Certified Developer™ designation. He is also a FileMaker Certified Trainer™.

He has been developing business management solutions in FileMaker® Pro and its predecessor applications since 1986. In 1998 he was awarded the first FileMaker Excellence Award by FileMaker, Inc. In 2003 he became at the time only the second person ever to receive that award for a second time. In 2000 he was also awarded the "Mad Dog" Recognition Award by FileMaker, Inc. for his efforts to generate positive public information and news coverage about the FileMaker Pro family of products.

He is the author of the definitive volume *FileMaker Security: The Book*, available at [www.filemakersecurity.com](http://www.filemakersecurity.com). He is also the author of, and instructor on, an entire set of videos on FileMaker Security released in June of 2007.