

The Next Generation of Fraud Management



Confidential

The recipient of this document agrees that at all times and notwithstanding any other agreement or understanding, it will hold in strict confidence and not disclose the contents of this document to any third party and will use this document for no purpose other than evaluating or pursuing a business relationship with CoreLogic®. No material herein may be reproduced, in whole or in part, by any means without the expressed written consent of CoreLogic. Unauthorized distribution is strictly prohibited.

Table of Contents

Executive Summary	1
Limitations of Current Fraud Prevention Technologies	2
Alerts	2
Reports	2
Workflow	2
An Integrated, Comprehensive Approach to Fraud Prevention	3
Data and Analytics: Targeting Which Loans to Work	3
Policy and Strategy: Determining Optimal Action Steps for the Risky Loans	3
Operational Workflow: Investigating and Evaluating Suspect Loan Applications Efficiently and Effectively	4
Infrastructure Support: Maintaining Standards, Automating Data-Gathering, Reporting on Best Practices	4
Optimizing the Information Processing Flow	5
Input and Output Capabilities	5
Data and Analytics Capabilities	6
Rules Capabilities	7
Workflow Capabilities	8
Providing an Interactive Loan Application Workspace	9
Use Case Example: Correspondent Lending	10
Summary: The Next Generation of Fraud Management	11
About CoreLogic	12

Executive Summary

Today, most fraud prevention efforts take the form of alerts provided in paper-based reports driving manual workflows. This restricts most fraud analysts to a focus on alert clearing, which represents just one component of a comprehensive and effective risk mitigation methodology.

The demands of today's mortgage industry business environment call for a more far-reaching approach to fraud management, one that enables dynamic business intelligence and decision making within the areas of data, analytics, policy, strategy, and operational workflows.

To be most effective within the constantly changing mortgage fraud landscape, a system that supports this holistic approach would need to be easily adaptable by fraud managers, minimizing reliance on information technology (IT) departments. Ideally, this technology environment would also be expandable to support the evolving needs of fraud prevention teams.

Limitations of Current Fraud Prevention Technologies

For the past decade, mortgage fraud prevention teams have had access to technology solutions that provide them with data, analytics, and reporting that can alert them to potentially fraudulent applications. Primarily taking the form of paper-based reports, this business intelligence drives manual workflows that to this day are managed most often by some combination of email, spreadsheets, and “sticky notes.”

Alerts

The alerts delivered by technology vendors, while valuable, tend to be stagnant and challenging to modify or enhance. The typical fraud prevention team in today’s enterprise is forced to rely upon already burdened IT departments for modifications and enhancements, hindering fraud prevention teams in their efforts to respond quickly to changes in the business environment.

In addition, fraud analysts can become narrowly focused on merely “clearing alerts” when they are not equipped with any additional capabilities to more proactively prevent fraud.

Reports

Most fraud prevention technology systems today produce reports with 15 to 25 pages of information on each and every loan. The content within each report remains the same regardless of the degree of risk or the relevance of the information for a given application. These reports currently function as complements to an external, largely manual, and time-consuming workflow.

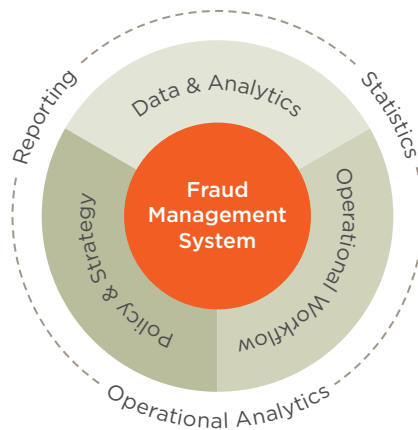
Workflow

While fraud prevention teams are highly skilled and motivated in their efforts, the lack of automation in their analytical technologies leaves most teams highly reliant on manual workflows. Executives and industry regulators pressure these teams to encode and enforce best practices, yet it’s difficult to build repeatable and reproducible best practices that can be followed on a consistent basis for every loan application.

The workflows that have been designed and implemented can’t be easily modified to suit different types of risk cases, and the addition of optimization features such as predictive scoring can be disruptive to a team’s established procedures.

An Integrated, Comprehensive Approach to Fraud Prevention

Given the way most fraud prevention teams work today, the optimal next-generation fraud prevention environment would harmonize data, analytics, policy, strategy, and operational workflows within an integrated, web-based platform. The ideal platform would provide an intelligent, adaptable environment for fraud analysts, equipping them with the right information and specific actions needed to make informed risk management decisions for each application flagged as high risk.



The three areas shown in the diagram above represent areas that naturally overlap in the everyday work of fraud prevention teams. Data and analytics, policy and strategy, and operational workflow are interactive and interdependent elements; reporting, statistics gathering, and operational analytics support and inform each of these elements.

Data and Analytics: Targeting Which Loans to Work

Lenders process thousands of loan applications on an ongoing basis, each carrying a unique risk profile. Sophisticated analytics deployed on differentiated data sources give lenders the ability to target the loans that have the highest risk. Determining “which” loans to work is a lender-specific decision that may need to change from month to month (or from loan program to loan program), not something that can be determined by a static (or hard to modify) set of rules.

Risk prevention teams should have access to scoring and optimized alerting for each individual loan file, which is possible when a technology environment has the ability to easily and rapidly deploy new data sources and new analytics, including:

- ▶ Rules
- ▶ Scorecards
- ▶ Pattern-recognition models.

Policy and Strategy: Determining Optimal Action Steps for the Risky Loans

Once lenders have identified the population of loans that most need attention, they need the ability to prioritize them and to determine the optimal action steps needed for each. The fraud manager’s ability to create strategies that combine scores and alerts along with action steps for the analysts that are specific to each lender’s best practices help ensure that the optimal group of loans is worked in the optimal way in every instance. Determining “which” action steps to perform at the individual loan level is a lender-specific decision that may need to change from month to month (or from loan program to loan program), not something that can be determined by a static (or hard to modify) set of rules.

Operational Workflow: Investigating and Evaluating Suspect Loan Applications Efficiently and Effectively

In order to meet best practices standards, fraud prevention must be repeatable and reproducible, meaning that:

- ▶ Each associate will perform the same set of actions for a specific risk situation — time after time — as directed by the system and the lender-supplied best practices.
- ▶ Two different associates would each work the same risky loan in the same, lender-specified way.

In order to ensure that fraud analysts can investigate and evaluate suspect loan files with ultimate efficiency and efficacy, a next-generation fraud prevention solution should integrate with the lender's existing servicing platforms and other internal and external systems. This integration should combine with task level consistency in methodology and information gathering.

Infrastructure Support: Maintaining Standards, Automating Data-Gathering, Reporting on Best Practices

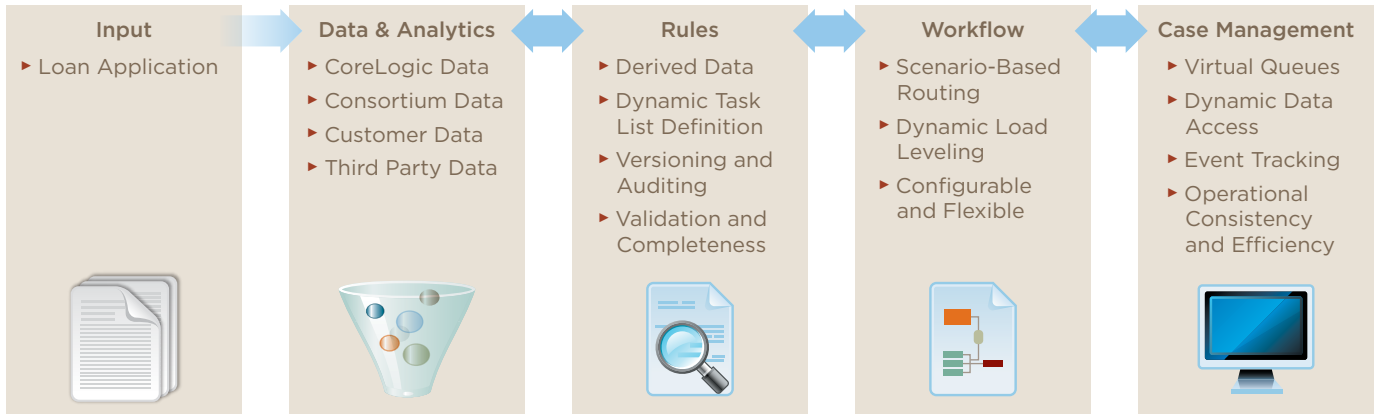
All appropriate data, including loan, case, and task level information, should be exportable in industry standard formats in order to drive external report-generation systems. A next-generation solution would enable the creation and ongoing enhancement of a repository of best-practices reports.

Fraud prevention teams need a better, simplified way of gathering statistics on utilization, productivity, costs, efficiency, and effectiveness of their customized rules, alerts, scores, and hard won strategies. The automation of data gathering for contribution to the Mortgage Fraud Consortium would also prove to be of significant benefit to these teams and their lending organizations.

Optimizing the Information Processing Flow

The next generation of fraud prevention technologies would streamline and largely automate the process of applying each lender's business intelligence, rules, workflow, and case-management best practices to all loan application input.

BASIC NEXT GENERATION FLOW



Input and Output Capabilities

A true next-generation technology solution should make straightforward the process of mapping from a variety of lender and industry specific data formats into a single, consistent internal "business object" model. These formats should include MISMO, standard GSE layouts (FNMA, FHLMC, etc.), standard industry layouts (LoanSafe® from CoreLogic®), and customer supplied layouts.

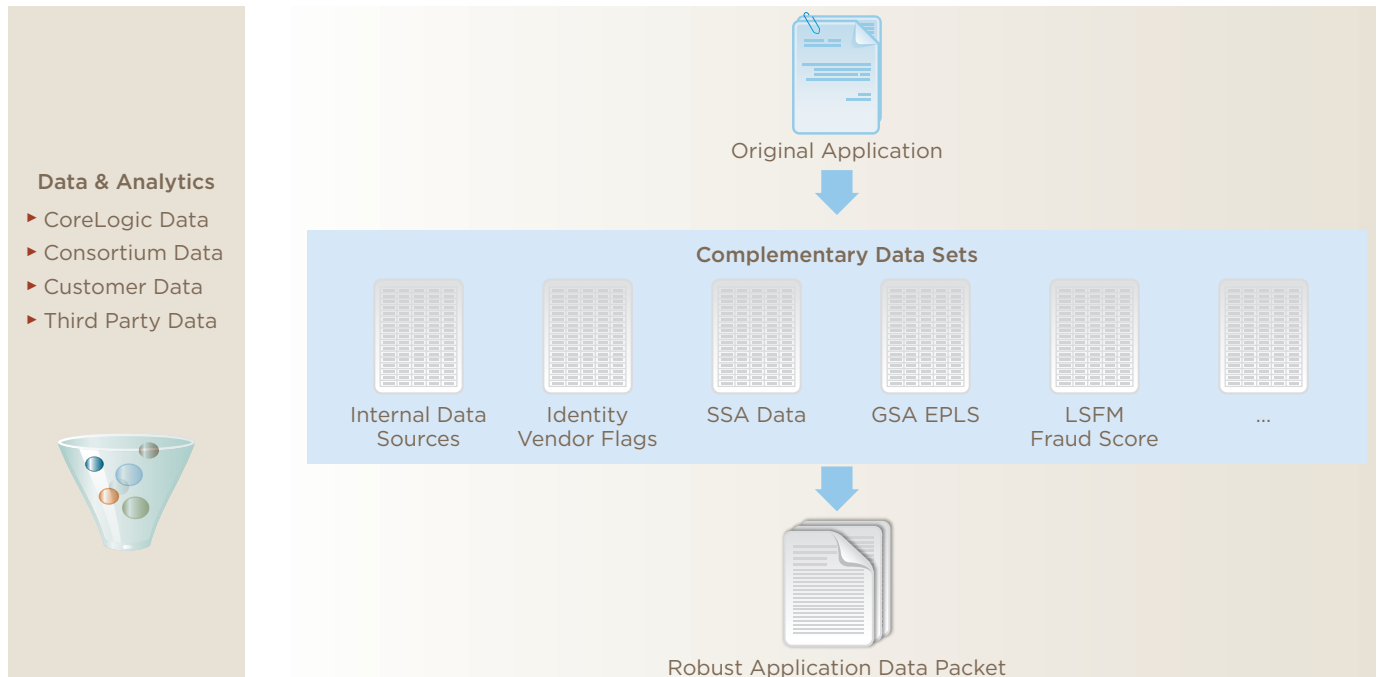
Validation, transformation, mapping, and default values should all be capable of being accomplished "on the fly" and transparently to external users and systems.

For aging and clean-up processes, the solution should ensure that removal and archiving is performed automatically, based on user rules, including time triggers such as aging, and external triggers such as "loan withdrawn," "loan funded," "loan declined," etc.

Data and Analytics Capabilities

A progressive approach to data and analytic flow would result in the production of a robust application data packet after processing of application data through a comprehensive collection of complementary data sets.

BASIC NEXT GENERATION FLOW – Data & Analytics



The next-generation approach should augment the loan object with new data fields – whether calculated or derived – using a user-accessible rule language. These new data fields would be based on:

- ▶ Internal or external database lookup
- ▶ External system-to-system call
- ▶ Results of other rules

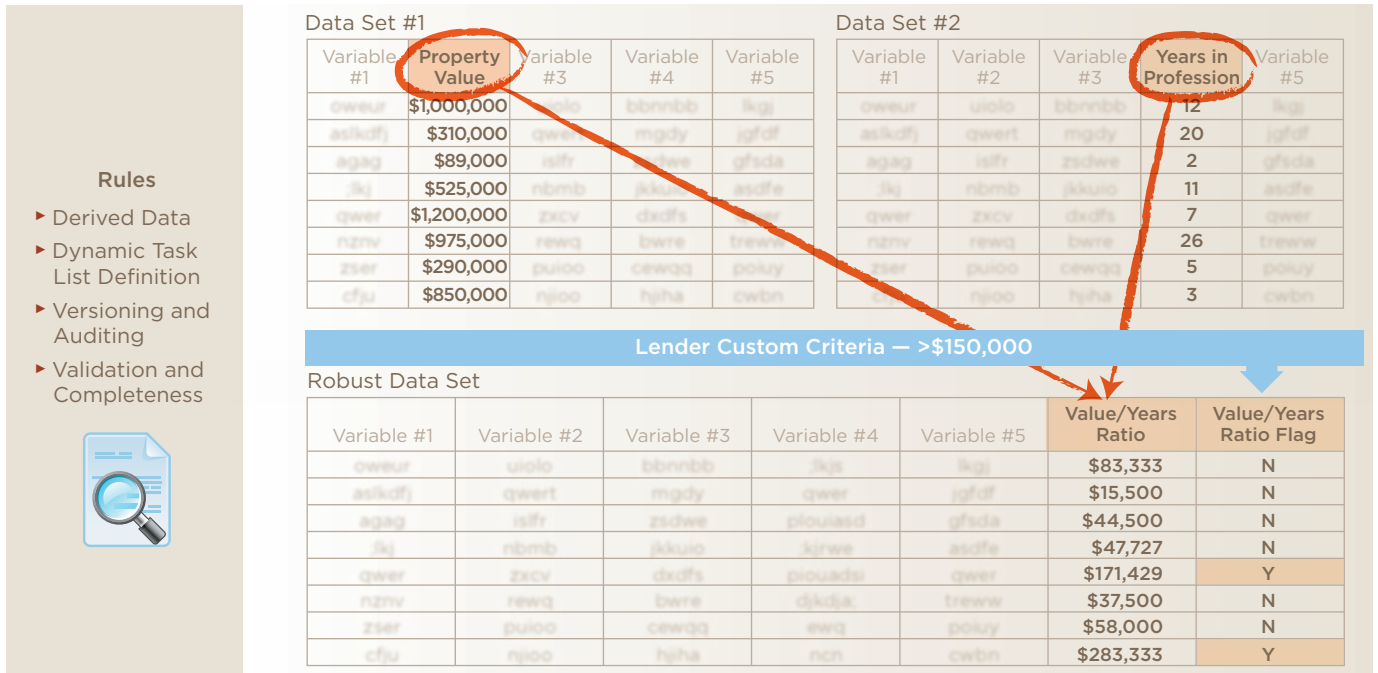
A genuinely robust production caliber rules system would enable consistency and completeness, as well as versioning and auditing scenarios, including:

- ▶ **“What-if”** – the ability to execute new rules and strategies on a speculative basis to understand the effect of implementation without risking harm to production work
- ▶ **“Roll back”** – the ability to restore any rule, group of rules, or strategy to a prior point in time; useful to correct an inappropriate decision or to return to a prior way of working based on changing conditions
- ▶ **“As of”** – the ability to understand how rules and strategies would have behaved at a particular point in the past; useful for back-testing new approaches to fraud prevention on a retrospective basis in combination with the “What-if” feature.

Rules Capabilities

Another critical quality of a new generation of fraud prevention systems is the ability to migrate and update existing alerts and enable the ability to create new alerts that can be modified as needed without reliance on IT.

BASIC NEXT GENERATION FLOW – Rules



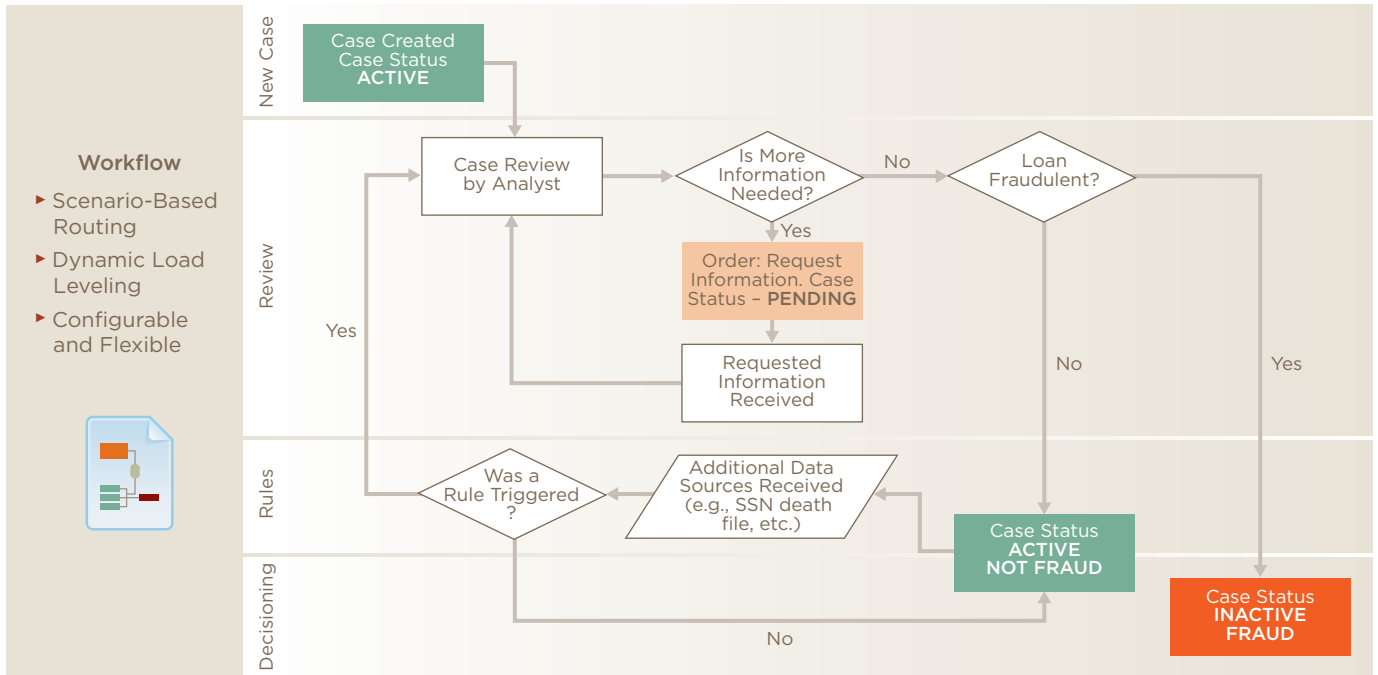
A fully-featured rules environment would include the ability to:

- ▶ Convert each current alert into a manager-accessible rule
- ▶ Empower managers to create new alerts and modify existing alerts
- ▶ Securely and appropriately access internal and third-party data sources.

Workflow Capabilities

Enormous effort is invested by managers in creating the most productive and effective workflows for their analysts. The ideal environment for the creation of workflows would be flexible and configurable, and would include scenario-based routing and dynamic load leveling,

BASIC NEXT GENERATION FLOW – Workflow



The optimal environment would make it possible to establish a workflow that:

- ▶ Determines which loans need to be reviewed
- ▶ Shows which actions are required for each reviewable loan
- ▶ Offer a user-definable fraud case workflow with required actions at each step
- ▶ Delivers trigger based surveillance of loans based on criteria specified by the manager:
 - ◆ External events (e.g., the arrival of an updated data source)
 - ◆ Internal events (e.g., time based or rule based triggers)
- ▶ Keeps loans eligible for reconsideration for fraud review until removed under control of a manager- or lender-specified rules.

Providing an Interactive Loan Application Workspace

There can be no question that fraud analysts can be significantly more productive and effective at preventing fraud when they have the right access to the right information at the right time. An interactive workspace designed to provide this information and to present an intelligent, dynamic workflow triggered by lender-specific variables could be the catalyst for expanding from a narrow alert-closing focus to one that is progressively more effective at global risk mitigation.

The next generation of fraud-prevention technologies will present such an **interactive workspace**, where loan, borrower, and collateral information would be readily available within a browser based interface. This workspace could include:

- ▶ Clickable, drill down information on all relevant fields (e.g., Social Security number, address, phone, etc.)
- ▶ Access to a customizable menu of third-party tools (e.g., maps, verifications, reverse lookups, etc.).

An **integrated loan risks screen** could summarize in a single view all risk factors found based on models, rules, and alerts.

An **integrated risk action screen** would outline, for each risk factor, the tasks required of the analyst, then provide a way to disposition each required task, such as:

- ▶ Cleared
- ▶ Pending Response
- ▶ Skipped

Disposition details would also be readily available, including:

- ▶ Confirmed Fraud
- ▶ Pending Response
- ▶ Not Currently Suspicious

Use Case Example: Correspondent Lending

The correspondent lending division of a mortgage company could use rules, workflow, and configuration to:

- ▶ Enforce front-end edits and consistency checking on loans received from correspondents, ensuring:
 - ◆ Loan file completeness (i.e., all required fields present)
 - ◆ Loan quality guidelines met (e.g., “If LTV > 90, then DTI must be < 30”)
 - ◆ Loan accuracy guidelines (i.e., does the loan match the file?)
- ▶ Apply differentiated decision flows for:
 - ◆ Determine whether a loan is reviewable using correspondent specific variables that may not be applicable to other lines of business, using correspondent specific risk information to influence workflow
 - ◆ Route reviewable loans to specific queues that are isolated from loans for other lines of business
 - ◆ Refer the loan into a queue by analyst for lender action
- ▶ Allow access for correspondent lenders to:
 - ◆ Create limited access user credentials that can be distributed to individual lenders to allow them to see only their loans
 - ◆ View and respond to their referred items – allowing the loan to automatically queue back to a fraud analyst for further action.

Summary: The Next Generation of Fraud Management

Many lenders and their risk mitigation teams are motivated to move beyond simply clearing alerts into an integrated, customizable, expandable environment that would offer:

- ▶ The rapid and flexible deployment of:
 - ◆ New data sources
 - ◆ New and/or enhanced predictive analytics (such as models, scorecards, and alerts)
 - ◆ Consortium based best practices (including workflows, alerts, triggers, actions)
- ▶ Client accessible rules for:
 - ◆ The creation, modification, refinement, and tuning of alerts
 - ◆ The implementation of configurable workflow routing and tracking
 - ◆ Consistent Fraud Case Management business practices
- ▶ Configurable Case Management Environment:
 - ◆ Flexible integration with internal and external systems
 - ◆ The presentation of the right information at the right time to optimize analyst productivity and maximize fraud prevention.

About CoreLogic

CoreLogic (NYSE: CLGX) is a leading provider of consumer, financial and property information, analytics and services to business and government. The company combines public, contributory and proprietary data to develop predictive decision analytics and provide business services that bring dynamic insight and transparency to the markets it serves. CoreLogic has built the largest U.S. real estate, mortgage application, fraud, and loan performance databases and is a recognized leading provider of mortgage and automotive credit reporting, property tax, valuation, flood determination, and geospatial analytics and services. More than one million users rely on CoreLogic to assess risk, support underwriting, investment and marketing decisions, prevent fraud, and improve business performance in their daily operations. Formerly the information solutions group of The First American Corporation, CoreLogic began trading under the ticker CLGX on the NYSE on June 2, 2010. The company, headquartered in Santa Ana, Calif., has more than 10,000 employees globally with 2009 revenues of \$2 billion. For more information visit www.corelogic.com.

CoreLogic
4 First American Way
Santa Ana, CA 92707

FOR MORE INFORMATION PLEASE CALL 1-866-774-3282

© 2010 CoreLogic

CORELOGIC and LOANSafe are registered trademarks of CoreLogic
All other trademarks are the property of their respective holders.
Proprietary and confidential. This material may not be reproduced in any form without expressed written permission.

17-NGFM-0910-00



CoreLogic®

corelogic.com