



Data Security and Confidentiality Statement

Reverse Market Insight (RMI) takes client confidentiality very seriously, as it underscores our business model and everything we do for clients and the industry at large. The first and most important point in understanding our security measures is in understanding different data sources we utilize in our work – public and private.

Public vs. Non Public Data Sources

Public data sources are those accessible to the general public and clients directly from the provider of the data. A prime industry example of this is HUD's HECM Activity Reports, which are published by HUD on their internet site monthly. RMI provides reporting services and analysis based on this data source that names companies, but at all times this is not disclosing anything that could not be achieved by anyone using public data.

RMI's role with public data sources is to efficiently and effectively organize and analyze the information available in the public domain, utilizing our expertise to distill powerful insights from raw data at a better price than our clients can achieve on their own.

This is very different from RMI's role with non public data, where RMI is an objective intermediary serving as both the secure warehouse for data and a provider of performance analytics and reporting services that highlight trends in the industry. RMI will never share loan level data from the Reverse Mortgage Industry Data Repository for many reasons, but at least one simple reason that you can always trust – our business cannot exist without the confidentiality of our clients and the exclusivity of the Reverse Mortgage Industry Data Repository.

Reverse Mortgage Industry Data Repository Security

There are four main factors that help to ensure our Data Repository is a secure and efficient way to gather industry data and support the development of performance and competitive reporting: 1) Technology, 2) Physical Security, 3) the Data itself, and 4) Report Design Considerations.

1) Technology

RMI uses state of the art technology to protect customer information. From encrypting certain data at the database layer to limiting access to the systems on which the data resides, we practice multiple redundant protection strategies and tactics to keep client data secure.

1. Activity monitoring: proactively ensures that nobody is accessing data that shouldn't be.
2. SSL encryption: we encrypt communications between the data repository and any applications that require access to the information (report development tools, report generation, data uploading, database backups, etc).
3. Field Level Encryption: even though we are using partially redacted fields for sensitive customer information, we are using field level encryption at the database level to further protect our clients' data.

2) Physical Security

The data repository will always be housed in a physically secure environment.

1. Hardware Firewall: We will manage our own physical firewall, ensuring only traffic from trusted locations is allowed access to the system.
2. Tier-One Hosting: Our server(s) will be physically hosted at a managed tier-one hosting facility (such as Rackspace).

3) Limited Data

While RMI is using technology to provide a buffer against any unwanted access to data, we are also taking measures to protect information in the data itself.

1. Redacted and Partially Redacted Fields: RMI is not storing a complete borrower record, only enough to de-duplicate data in the database. First Initial of first name, First 4 characters of last name, Street Number only of physical street address, and no reference at any time to borrower Social Security Numbers.
2. No Contact Information: RMI does not store customer contact information. (phone, email, fax, etc).

4) Report Design

RMI understands that even though we've taken steps to secure and keep confidential the data within our database and network environments, we need to keep our customers' information private when reports are issued as well.

1. Aggregated Data: RMI does not provide loan level data in our reports (loan level data will never be shared with anyone). We aggregate the data and provide meaningful summaries of the trends in the industry - similar to management reporting within your company.
2. Participant Confidentiality: RMI only shows specific companies at the broadest geographic levels of our reports, and only when dealing with market share on a unit and dollar basis. Any time multiple variables are displayed and/or significant market segmentation reporting is utilized, company names are never disclosed and are aggregated in most cases to show only client vs. market comparisons.
3. Rule of Five: RMI will never publish repository data for a market segment where less than 5 participating institutions are represented in the data to prevent any attempted disaggregation or reverse engineering aimed at identifying individual company metrics. We take client confidentiality seriously and this principle ensures that companies will never see their information compromised.

Our report outline displaying these levels of aggregation and confidentiality is available upon request, and we encourage you to inquire if you have any questions regarding confidentiality and privacy in the published format of our reporting services.

In closing, I'd like to reiterate our continued commitment to keeping your information secure and maintaining your trust. Please feel free to contact us at any time for additional information about our security practices and thank you for your time and consideration.

Sincerely,

John K. Lunde
President, Reverse Market Insight

RMI is proud to be the exclusive partner of the National Reverse Mortgage Lenders Association for the Reverse Mortgage Industry Data Repository and all market intelligence services resulting from this important industry initiative.