



## **Privacy/Security Statement**

The Receivable Management Services Corporation (herein known as RMS) is dedicated to providing our customers and business partners with products and services that render the entire receivables management process more effective and cost efficient. Furthermore, RMS understands the importance of maintaining the privacy and confidentiality of the information belonging to our customers and their clients, our vendors, business partners, and employees. Through administrative, procedural, physical, and technical controls; management of systems and information access; the use of non-disclosure and non-compete agreements; and other appropriate contractual obligations RMS effectively safeguards information provided to us or generated by us as requested by our customers and required by regulations that apply to us.

### **Information Collection and Use**

Throughout our business process, we receive confidential and proprietary information from our customers about their customers and prospects, and their business models, processes, and procedures for the purposes of understanding their businesses to effectively fulfill our contractual agreements. This information may include information provided on applications or other forms, information about transactions with us or other businesses, and other information that has been legally obtained from public sources such as court filings or tax assessor databases. This personal/business information may include financial information and identifying information such as social security number, taxpayer ID number, D-U-N-S<sup>®</sup> Number, business or personal addresses, account numbers with companies forwarding accounts to us for servicing, and other information.

RMS uses the information it collects in its business processes to support and maintain its business relationships and/or the relationships with those with whom we, RMS, and/or our customers do business. RMS will use personal information to facilitate communications, to complete a business transaction and/or to personalize our communications, specifically lettering programs and email messages. Credit card and Social Security numbers are used for payment processing and/or identification purposes only, and maintained in a secure, PCI-compliant, environment as described under *Security Procedures*.

### **Information Sharing and Disclosure**

RMS complies with our customers' requests to protect their information. RMS does not disclose nonpublic information supplied by, or about, our current or former customers or business partners to anyone, except as permitted by law or authorized by the customer. Through contractual agreements, we agree to protect our customer's information, including information covered under the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm Leach Bliley Act (GLBA). Under HIPAA we protect our customers' Protected Health Information (PHI) and under GLBA we protect our customers' Non-Public Personal Information.

In addition, RMS complies with Fair Debt Collection Practices Act (FDCPA) and all applicable state collection laws concerning the disclosure of information and the processes by which a customer may request that RMS cease

*Working Capital Optimized*



attempts to contact or otherwise communicate with the customer. RMS may disclose your personal information when we are required to do so by law, or in order to comply with a court request or governmental inquiry.

## **Security Procedures**

RMS maintains the following Security Policies and Procedures:

### Administrative Safeguards

1. Security management processes to prevent, detect, contain and correct security violations.
2. Designated Security Official who develops and administers the data security policy.
3. Data Security Department defines, administers and oversees access to electronic information by the workforce.
4. Information Security awareness and training is conducted for all appropriate members of the workforce.
5. Security incident procedures for handling breaches of data security.
6. Contingency Plans for disaster recovery and business continuation.
7. Evaluation of business procedures and associated systems on a periodic basis.
8. Business Associate Agreements are required to be signed by our contractors.

### Physical Safeguards

1. Facility Access Controls limiting building and computer room access.
2. Specific internal application security controls to limit access to data.
3. Secured network and workstation access with individual sign-ons.
4. Physical device and media controls concerning the receipt and removal of hardware/data.

### Technical Safeguards

1. Access controls – security software that denies or permits electronic application or data access.
2. Security audit controls and reporting of electronic information systems.
3. Data integrity managed through programmed application security and audit controls.
4. Person or entity authentication maintained by user sign-on and password.
5. Transmission security governed through network/firewall infrastructure.

## **How RMS uses Cookies**

A cookie is a piece of text that is temporarily stored in a computer hard drive or in a browser's memory. Cookies allow a web site to store information on the machine and to later retrieve it, and are used to facilitate internet sessions. A Web site may set an expiration date for a cookie it delivers. If no expiration date is specified, the cookie is deleted when the user quits the browser. Cookies from RMS or other websites can be managed by resetting the web browser to either notify the user when a cookie is received, thereby allowing the user to accept or reject the cookie at the time it is presented, or by having the user's web browser reject the cookie immediately upon its presentation.

## **Links**

*Working Capital Optimized*



Links to other non-RMS websites are provided solely for user convenience, and access to these websites via the links provided are at the user's risk. RMS does not control these websites and, therefore, cannot guarantee that their Privacy Policies follow the guidelines established here, or that they are in conformance with the privacy guidelines established by the EU Safe Harbor Act.

### **EU Safe Harbor Act**

RMS is registered with the U.S. Department of Commerce's Safe Harbor program, and adheres to the U.S. Safe Harbor principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement as defined by the agency. Individuals who wish to file a complaint or take issue with RMS' compliance to the Safe Harbor Act are request to contact:

### **Contact Information**

If you have any questions or comments concerning RMS' Privacy Policy, please contact our Manager of Compliance; Maryann Cantor at 484-242-6826 or email her at [Maryann.Cantor@rmsna.com](mailto:Maryann.Cantor@rmsna.com).

D-U-N-S<sup>®</sup> Number is a registered trademark of D&B

*Working Capital Optimized*