FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Cartus Corporation

(Cartus)

August 2015

Table of Contents

System Overview

The FDIC's Division of Finance (DOF) has procured the services of Cartus to provide employee relocation services including home sales and home purchases, household goods, shipping, move management, and temporary housing. Cartus processes payments pertaining to the relocation of FDIC employees and provides payment information for employees. On a monthly basis, Cartus sends the FDIC an invoice for relocation transactions.

Personally Identifiable Information (PII) - Cartus

Cartus collects and maintains personally identifiable information (PII) about FDIC employees, including full name; social security number (SSN); date of birth (DOB); home address; home telephone number; personal email address; employee identification number (EIN); financial information; vehicle identifiers; employment status, history, or information; and information about the employee's spouse and/or dependents (full name, work phone number, DOB, and financial information).

Purpose & Use of Information - Cartus

The data that Cartus collects and maintains is used to support the FDIC employee relocation program. The PII collected and maintained is used to verify the identity of the relocating individual and is required to allow the vendor to process the employee's relocation, as well as assist the relocating individual with selling his/her current home, as applicable.

Sources of Information - Cartus

All information in Cartus comes directly from the relocating FDIC employee, either from filling out the FDIC Official Notification of Relocation form or from the employee self-registering on the Cartus website or mobile application.

Notice & Consent

Individuals are not provided with an opportunity to "opt out" of providing personal information or consenting only to a particular use of their data in Cartus. The PII elements collected and maintained are required by Cartus for processing the relocation transaction.

Access to Data - Cartus

a. Parties with Access to Data - Cartus

Authorized Cartus employees have access to the PII contained within Cartus in order to confirm the PII with the employee and obtain any additional PII as necessary.

Authorized FDIC DOF employees within the Travel Services Section have access to the data to manage billing information and to reimburse Cartus for relocation expenses.

Cartus shares PII with its subcontractors (Nor-Cal Relocation Services, Select Van & Storage, S&M Moving Systems, Young Moving & Storage Inc., NRT LLC, Title Resource Group, US Inspect, Cartus Home Loans, Oakwood Corporate Housing, and Fidelity) to allow these subcontractors to process the employee relocation transactions.

Appropriate taxing authorities (i.e., Internal Revenue Service) may be provided with the data to allow the Federal, State, and Local Agencies to process the taxes and fees associated with the purchase or sale of the employee's home due to the relocation.

Cartus may share information with third party suppliers (e.g., home inspectors, moving companies) when necessary to support the services they deliver.

Cartus may disclose personal information about customers in cases when it is necessary to identify, contact, or bring legal action against individuals who may be in violation of Cartus' terms or use or terms of service. Additionally, Cartus may disclose to local authorities or access a customer's personal information as required by law to comply with legal subpoenas.

b. Criteria and Procedures for Granting Access

Cartus follows the principle of least privilege when granting access and enforces separation of duties by ensuring incompatible functions are managed by different leadership teams. Roles are evaluated for segregation of duties and access entitlements are handled by access control managers.

Data Sharing

Other Systems that Share or Have Access to Data in the System:

System Name	System Description	Type of Information Processed
N/A	Cartus does not directly interface with FDIC systems.	N/A

Data Accuracy - Cartus

Data is collected directly from individuals, which is generally considered to be the best way to ensure accuracy of the data in a system. Cartus works with FDIC to verify the integrity of the data before, in conjunction with, and after inputting it into the system or using it to support the project. As necessary, an authorized user or administrator of Cartus checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

Data Security - Cartus

Cartus has administrative and technical security controls in place to protect data contained in the system and prevent unauthorized access and use of the data. Cartus follows the principle of least privilege when granting access and enforces separation of duties. User access profiles are reviewed by system owners and scrutinized for conflicting access.

Within FDIC, the Cartus Online Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

Additionally, Cartus is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and the vendor has designated the Cartus Account Manager to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. The vendor must comply with the Monitoring and Incident Response contractual requirement.

System of Records Notice (SORN)

Cartus operates under the FDIC Privacy Act SORN 30-64-0012, *Financial Information Management Records*.

Contact Us

To learn more about the FDIC's Privacy Program, please visit: http://www.fdic.gov/about/privacy/.

If you have a privacy-related question or request, email Privacy@fdic.gov or one of the FDIC Privacy Program Contacts. You may also mail your privacy question or request to the FDIC Privacy Program at the following address: 3501 Fairfax Drive, Arlington, VA 22226.