U.S. Small Business Administration
409 3rd Street, S.W.
Washington, DC 20416

Office of Disaster Assistance

Disaster Credit Management System 2.0

Privacy Impact Assessment

January 29, 2021
v1.3 (03/18/2021)

System Owner
Michael Yeager
Acting, Director , DCMS Operations Center
Office of Disaster Assistance
Michael.Yeager@sba.gov

Reviewing Official
Keith A. Bluestein
Senior Agency Official for Privacy
Chief Information Officer
Office of the Chief Information Officer
PrivacyOfficer@sba.gov

This is a Controlled Unclassified Document

I. System Description/General Information

SBA provides disaster assistance through its Office of Disaster Assistance (ODA), which coordinates low-interest, long-term loans for damage caused by a declared disaster. The Disaster Credit Management System (DCMS 2.0) was developed to support the mission of the ODA in being used to process loan applications and determinations for the small business disaster loan program.

The DCMS 2.0 information system supports ODA in all disaster loan operations beginning with processing of disaster declaration information until final disbursement of funds. DCMS 2.0 focuses on the processing of loan applications based on eligible disaster damage, credit/repayment worthiness, repayment, statutory interest rate, character and eligibility as defined in the Small Business Act and 13 CFR 120.110.

In March 2020, as the Coronavirus (COVID-19) pandemic began spreading across the United States, the SBA ODA made the official decision to exercise an existing contract relationship with RER Solutions Incorporated, Rocket Mortgage and its subsidiary company Rapid Finance (referred to in this document as RER-Rocket Loans-Rapid Finance) to process Economic Injury Disaster Loans (EIDL) and advances. As a result of this decision, RER-Rocket Loans-Rapid Finance's loan origination system became the primary source system for these loans and advances to handle the tremendous load of disaster applications being submitted as a result of the Coronavirus Aid, Relief, and Economic Security (CARES) Act passed by Congress for the American public.

RER-Rocket Loans-Rapid Finance has been tasked to intake all COVID-19 related EIDL applications and process them for decision. Disaster survivors applying for an EIDL in relation to the COVID-19 disaster declaration will utilize the SBA website, www.sba.gov/disaster, to find the appropriate disaster declaration for the disaster survivor's state of business or residence. From there, a link will redirect the survivor to an RER-Rocket Loans-Rapid Finance website to register for an account and begin the EIDL application process.

The RER-Rocket Loans-Rapid Finance system is outside the boundary of DCMS 2.0. The RER-Rocket Loans-Rapid Finance loan origination system is a non-federal system that is processing information in support of the SBA ODA to assist in handling the loan applications intake for the COVID-19 economic pandemic.

The DCMS 2.0 system contains information about individual members of the public and excludes employees. The Personally Identifiable Information (PII) necessary for approving loans to disaster survivors. PII of disaster survivors is used for loan application processing, credit history evaluation and loan disbursement. DCMS 2.0 contains the following types of PII of disaster survivors:

name, date of birth, Social Security Number (SSN), address, telephone number(s), citizenship or immigration status, financial account numbers, income, assets, expenses, credit history, tax return history, tax identification number, email address, Employer Identification Number (EIN), FEMA registration number, insurance policy number, loan numbers, handwritten signatures, marital status, household size, and closest relative's information (name/address).

This PII information along with property and disaster damage is collected, added to the system and utilized in making disaster loan application decisions. These applications are filed by small businesses, homeowners, and non-profit corporation disaster survivors. The data is collected via an OMB approved form, referenced as OMB No. 3245-0017, Expiration: 08/31/2021, and via a public-facing web-based interface, referenced as the Electronic Loan Application (ELA) service on the Disaster Loan Assistance Portal (DLAP). For business owners, a similar form is utilized to collect PII for the business via an OMB approved form, referenced as OMB No. 3245-0018, Expiration: 07/31/2021, as well as the public-facing web-based application ELA, accessible from DLAP.

The legal authority authorizing the purchase or development of DCMS 2.0 is 15 U.S.C. § 634(b)(6), 44 U.S.C. § 3101, Section 7(b)(1) and Section 7(b)(2).

II. System Data

The categories of individuals covered in the system are members of the general public who were disaster survivors that have applied for disaster loans which includes small business and homeowners. The information is collected directly from disaster survivors that apply for disaster loans, through the Disaster Loan Application Portal (DlAP), from Federal Emergency Management Agency (FEMA), the Internal Revenue Service (IRS), from commercial vendors of credit-related information, the National Flood Insurance Program (NFIP) and RER Solutions Inc. in partnership with Rocket Loans and its subsidiary Rapid Finance (referred to in this document as RER-Rocket Loans-Rapid Finance).

Information is collected from several sources: Directly from the disaster survivor that apply for disaster loans via DLAP, from FEMA by way of electronic referral resulting from the applicant applying for disaster assistance through FEMA, the IRS, from commercial vendors of credit-related information, NFIP and RER-Rocket Loans-Rapid Finance.

Federal agencies, FEMA, IRS, and the Department of Justice (DOJ) provide data for use in the system. Tribal, State, or local agencies, which develop grant programs for future disasters, may provide data from time to time, as these programs are developed for specific disasters. Commercial credit bureaus, Dun &

Bradstreet business reports, commercial vendors of reference data (Zip Codes), commercial vendors of flood plain mapping data, insurance companies, and RFR-Rocket Loans-Rapid Finance.

The interconnection between DCMS 2.0 and Rapid Finance is a one-way communication path and will remain in place until all COVID-19 loans have been submitted to DCMS 2.0.

DCMS 2.0 data is verified for accuracy, completeness and current by applicants, originating/collecting systems, agency updates. Data not yet submitted as complete is deleted 45 days after the Application Deadline date. The Disaster Loan Assistance Portal requires registered users to authenticate with an independent service to identify the person applying and a two-factor authentication process for all independent service personnel to sign on to the system.

The data elements captured in the system are captured in DCMS 2.0 data dictionary.

III. Data Attributes

The use of the data is relevant and necessary for the purpose for which the system is being designed. Application loans for disaster are voluntary information provided by the customer via an application form and is required for the loan determination process. The information is based on specific need to evaluate disaster damage, credit worthiness, repayment, statutory interest rate, character and eligibility as defined in the Small Business Act and 13 CFR 120.110.   The system will not drive new data or create previously unavailable data about an individual. No new data will be placed in the individual's record and the system can't make determinations about employees or members of the public that would not be possible without new data.

Data is retrieved and accessed by authorized users with sufficient privileges by agency application number, applicant/recipient name, cross-referenced loan number or borrower's Social Security Number or Employer Identification Number. or FEMA registration number.

Ad-hoc reports can be produced on individuals by authorized ODA staff and managers and on a 'need-to-know' basis. Only authorized ODA staff have access to the applicant reports generated by the DCMS 2.0 information system dated, no reports published on individuals, and "opt-out" options are governed by the collecting Information Technology systems. The system is indexed by the individual firm name or the public DUNS.

IV. Maintenance and Administrative Controls

Data is stored in two of Salesforce's U.S collocated data centers with one acting as production site and the other as the fully redundant disaster recovery site. Security controls are consistent between production site and the fully redundant disaster recovery site.

Data is retained until it is no longer needed for operations or reference. The retention periods and disposition are defined in accordance with the current Standard Operating Procedure (SOP) Records Management Program SOP 041(2), and per SBA Privacy Act Systems of Record Notice, SBA 20.

DCMS 2.0 does not use any technologies in ways that SBA has not previously employed such as: Smart Cards, Caller-ID, or monitoring software.

DCMS 2.0 operates under the Privacy Act System of Records Notice SBA 20 which is currently being modified.

V. Data Access

Authorized agency users, officials, and certified contractors have access to data in the system based upon their specific roles or responsibility, with a need to know. Certified Contractor are those that have been adjudicated and are under a confidentiality agreement and have a Privacy Act clause in their contract, while engaged in system development, modification or maintenance.

User access is determined by the manager and approved by the DCMS Information System security Officer, System Owner, and in the case of a certified contractor, additional approval by the Contracting Officer.

Data is periodically shared with other systems from Federal and State agencies to help expedite disaster recovery processes or compliance with statute. Data is shared with the FEMA Disaster Assistance Improvement Program (DAIP). Agreed upon data elements are transmitted as discrete packets sent over secure interfaces or approved technologies. This use is in accordance with SBA Privacy Act System of Record 20 or Computer Matching Agreement(s) or Data Sharing Agreement(s) and Memorandum of Understanding or Agreement(s) where applicable. To assure proper use of the shared data, procedures and policies are in place for the protection of the shared information which includes, this PIA document, Information Security Agreement, and Memorandum of Understanding along with all supporting System Security Policy procedures. Information System Security Officer, system administrators, and Senior Agency Official for Privacy are responsible for protecting the privacy rights of the public and employees affected by the interface.

VI. Privacy Impact Analysis

There are risks related to disclosure of individuals' privacy. Risks to the type of data, ensure information used as intended, safeguard unauthorized monitoring of privacy data, and protect information shared internal and external. The sensitivity of the DCMS 2.0 data elements increases the risk for inadvertent disclosure which is susceptible to identity theft. Some data provides significant information.

Salesforce provides security controls for safeguarding the handling of PII data in the DCMS 2.0 system.

Privacy risks are mitigated through access control, auditing, secure application design and monitoring, monitoring, limited context regarding disaster loan information and comparable to its' collection; collection in compliance with statutory authority to collect, . encryption of data in transit and at rest; incremental and full backups, data integrity checks, data redundancy, and Contingency Planning. Regarding the relevance of data, time diminishes the risk slightly as much of the information is intended would no longer be current or potentially applicable. Mitigation also through education via Cybersecurity Awareness and Privacy Training.