REALPAGE
Outperform

# PRODUCT SPECIFICATIONS FOR ON-SITE FRAUD INVESTIGATION/VERIFICATION

UPDATED: March 5, 2020

These Product Specifications describe the current functionality and certain dependencies of the above-referenced product center (the "Product Center"). Access to and use of the Product Center is governed by an underlying agreement and, as applicable, addendum (collectively, the "Agreement") with RealPage, Inc. and, as applicable, its affiliates (collectively referred to herein as the "Provider" "we" or "us"). Capitalized terms used in these Product Specifications have the meanings provided in the Agreement unless otherwise defined herein.

Subject to the terms of the Agreement, these Product Specifications may be modified at any time. If we modify these Product Specifications, we will post the updated version at http://www.specifications.controls.realpage.com and update the "Updated" date above. We recommend that you review these Product Specifications periodically for any changes. Your continued access to or use of the Product Center will constitute your acceptance of the updated Product Specifications.

## 1. AUTHORIZED USERS AND PASSWORD

Provider will provide the licensee under the Agreement ("Licensee") with a user name and password permitting Authorized Users to access the Product Center. Licensee is responsible for the protection and dissemination of such user name and password and for any activities or actions occurring under Licensee's account or log-in credentials—including, without limitation, for any losses or damages resulting from the loss, theft or misuse of or failure to protect any such user name or password. Licensee will permit only Authorized Users to access the Product Center, will ensure that all Authorized Users comply with the terms and conditions set forth in the Agreement and herein, and will not permit any person that ceases to be an Authorized User to continue to use a user name or password.

## 2. OVERVIEW OF ON-SITE FRAUD INVESTIGATION/VERIFICATION

ON-SITE FRAUD INVESTIGATION/VERIFICATION is used in conjunction with Screening to confirm the veracity of applicant stated information regarding rental history, employment status and income. The Verification services are performed by a dedicated On-Site team using phone, email, fax, and other outbound methods to collect and confirm present and historical information often deemed by property management company's (PMC) as critical pieces to predicting future rental performance. On-Site Fraud investigation/verification services typically fall into two primary categories of Standard or Comprehensive.

- **Standard Verification** services consist of a verification of current employment and housing. On-Site collects documentation and contact information from the property as well as the applicant. The verifications will be conducted for three (3) business days before being discontinued. Specifically:

  On-Site makes one phone call/fax attempt daily to references for up to three (3) business days. If information or documentation is missing that is hindering On-Site from moving forward, the Verification representative will post for the needed information and reach out to the applicant, the property or both. On-Site will also make diligent efforts to find the necessary information online if possible. If the information is not received by the second business day, On-Site will again reach out to the property or applicant. If the needed information is not received by the end of the third business day, the verification will be marked "Unable to verify" and closed out.

- **Comprehensive Verification** services consist of verifications of current employment, housing, and a bank account. On-Site collects documentation and contact information from the property as well as the applicant depending on the client's specifications. Verifications will be conducted for five (5) business days before being discontinued.

Note: The ON-SITE FRAUD INVESTIGATION/VERIFICATION Product Center was not designed to store electronic protected health information, as defined by Section 160.103 of the HIPAA Regulations, 45 CFR Parts 160, under the Health Information Portability and Accountability Act Omnibus Final Rule released on January 17, 2013. Users should not use any feature of the ON-SITE FRAUD INVESTIGATION/VERIFICATION Product Center to upload or to store any electronic protected health information.

## 3. DETAILED SPECIFICATIONS FOR ON-SITE FRAUD INVESTIGATION/VERIFICATION

This section outlines the major capabilities of ON-SITE FRAUD INVESTIGATION/VERIFICATION:

### 3.1. Fraud investigation/verification (Standard) - Employment

a. Verifications are verbal, and follow these guidelines:
   (i) Search for the company in the state's Division of Corporations website or select a few websites to ensure it is a legitimate and actively registered company
      1. Required when verifying with paystubs/offer letter as well
   (ii) Verify the phone number provided for the reference to ensure that a land line office number is being called
   (iii) Contact either a direct supervisor of the applicant, the signatory of any documentation received, or the Human Resource/Payroll Department to verbally corroborate the terms of employment

b. ONLY the following may be accepted in lieu of verbal verification:
   (i) If self-employed: applicant's most recently filed Form 1040 tax return
   (ii) If U.S Military: applicant's most recent LES (Leave and Earnings Statement)
   (iii) If a W-2 employee: applicant's two most recent and consecutive pay stubs (require a full month)
   (iv) If employer uses an automated third-party employment verification service (for example, The Work Number, Verify Job System) the applicant must obtain the verification directly from the service and provide it to On-Site
   (v) New Hire: if the applicant has not yet begun employment, we will accept the offer letter if it meets the following requirements:
      1. Must be on company letterhead
      2. Signed by the Employer
      3. Provide position, hire date, and base salary

### 3.2. Fraud investigation/verification (Standard) - Rental

a. Homeowner: If a mortgage is reported on an applicant's rental report, On-Site will verify based on the mortgage. If there is no mortgage on file, the applicant must provide either a current property tax bill or a copy of the deed showing their name and address On-Site is verifying.

b. Renter: Contact the landlord to verify the dates of tenancy, rent amount, payment history, current account standing, and any possible issues (for example, complaints, damages, and bed bugs).

c. Corporate: Same as above, but verify a company's rental history.

3.3. Fraud investigation/verification – Comprehensive

a. On-Site **must** obtain documentation *in addition to* verbal verification unless otherwise specified by the client.

b. Employment:

(i) If self-employed: applicant's two most recently filed Form 1040 tax returns

(ii) If U.S. Military: applicant's most recent Leave and Earnings statement

(iii) If a W-2 employee: applicant's two most recent pay stubs showing year-to-date OR current employment letter (dated within last 60 days, on company letterhead and signed by the Employer)

(iv) If employer uses an automated third-party employment verification service (for example, The Work Number, Verify Job System), the applicant must provide On-Site with the necessary salary key code or personal identification number (PIN) code as well as credit card information for the representative to process the verification

c. Once documentation is received, On-Site proceeds with the following steps:

(i) Search for the company in the state's Division of Corporations website or select few websites to ensure that it is a legitimate and actively registered company

(ii) Verify the phone number provided for the reference to ensure that a land line office number is being called

(iii) Contact either a direct supervisor of the applicant, the signatory of any documentation received, or the Human Resource/Payroll Department to verbally corroborate the terms of employment

(iv) Verify position, hire date, and base salary; verify signing bonuses, annual bonuses, housing allowance and commissions if applicable

(v) If self-employed On-Site will verify the accountant who prepared the tax returns to ensure that they are a licensed and active accountant. On-Site will then verbally verify the information provided on the tax returns with the CPA. (Note: if tax returns are self-prepared, On-Site will obtain authorization from the client's Regional Manager to verify directly off the documents.)

d. Housing:

(i) Homeowner: If a mortgage is reported on an applicant's rental report, On-Site will verify based on the mortgage. If there is no mortgage on file, the applicant must provide either a current property tax bill or a copy of the deed showing their name and address On-Site is verifying.

(ii) Renter: Contact the landlord to verify the dates of tenancy, rent amount, payment history, current account standing, and any possible issues (for example, complaints, damages, bed bugs, and so on)

e. Bank: For bank account verifications, On-Site must obtain a current statement proving the applicant has an open account with no negative activity in which they could use to pay rent

(i) Obtain a current bank statement dated within the last 60 days (checking, savings, or money market account) showing the applicant's name, bank's name, last four digits of the account, and the current balance

(ii) Verify that the current balance is positive and that there have been no overdraft fees or NSF fees during the statement period

## 4. CALIFORNIA CONSUMER PRIVACY ACT OF 2018 ("CCPA") DATA PROCESSING STATEMENT

This CCPA Data Processing Statement applies to "Personal Information" of a "Consumer" as those terms are defined under the CCPA (referred to hereafter as "Personal Data") that RealPage processes in the course of providing services under the Product Center ("Services") governed by the Agreement to Customer.

RealPage understands the terms in this CCPA Data Processing Statement and agrees to comply with them. The terms of this CCPA Data Processing Statement will prevail in connection with the purpose and scope of this CCPA Data Processing Statement over any conflicting terms in the Agreement.

4.1. Customer's Role. The Customer is a for profit entity that determines the purpose and means of processing Personal Data. Customer will provide Personal Data to RealPage solely for the purpose of RealPage performing the Services.

4.2. RealPage's Role. RealPage shall provide the Services and process any Personal Data in accordance with the Agreement. RealPage may not retain, use, or disclose Personal Data for any other purpose other than for providing the Services and in performance of the Agreement.

4.3. Data Processing, Transfers, and Sales. RealPage will process Personal Data only as necessary to perform the Services, and will not, under any circumstances, collect, use, retain, access, share, transfer, or otherwise process Personal Data for any purpose not related to providing such Services. RealPage will refrain from taking any action that would cause any transfers of Personal Data to or from RealPage to qualify as "selling personal information" as that term is defined under the CCPA.

4.4. Sub-Service Providers. Notwithstanding the restrictions in Section 2.3, Customer agrees that RealPage may engage other Service Providers (as defined under the CCPA), to assist in providing the Services to Customer ("Sub-Service Providers"). RealPage carries out appropriate due diligence on each Sub-Service Provider and the arrangement between RealPage and each Sub-Service Provider is governed by a written contract which includes terms substantially equivalent to those set out in this CCPA Data Processing Statement.

4.5. Security. RealPage will use commercially reasonable security procedures that are reasonably designed to maintain an industry-standard level of security, prevent unauthorized access to and/or disclosure of Personal Data.

4.6. Retention. RealPage will retain Personal Data in accordance with Customer instructions, the terms of the Agreement, or any applicable law(s), whichever requirement is controlling under the circumstances. At the termination of this CCPA Data Processing Statement, or upon Customer's written request, RealPage will either destroy or return Personal Data to the Customer, unless legal obligations require storage of the Personal Data.

4.7. Assistance with Consumers' Rights Requests. If RealPage, directly or indirectly, receives a request submitted by a Consumer to exercise a right it has under the CCPA in relation to that Consumer's Personal Data, it will provide a copy of the request to the Customer. The Customer will be responsible for handling and communicating with Consumers in relation to such requests.

4.8. Enforceability. Any provision of this CCPA Data Processing Statement that is prohibited or unenforceable shall be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions hereof. The parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall then incorporate such substitute provision into this CCPA Data Processing Statement.