California Privacy Policy for Applicants and Employees

Effective Date: January 1, 2023

New American Funding ("NAF," "we," "our," or "us") respects the privacy of our applicants' and employees' personal information.

Pursuant to the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 ("CCPA"), we are required to provide California employees and job applicants with a privacy policy that contains a comprehensive description of our online and offline practices regarding our collection, use, sale, sharing, and retention of their personal information as well as a description of the rights they have regarding their personal information. This Privacy Policy provides the information the CCPA requires as well as other useful information regarding our collection and use of personal information.

Please review this Privacy Policy carefully. From time to time, we may change this Privacy Policy. If we do, we will post an amended version on this webpage and on our Company Policies page in ADP. You also may receive a copy by contacting us as described in the "**How to Contact Us**" section below.

This Privacy Policy covers the following topics:

1. Scope of Privacy Policy

When This Policy Applies

This Privacy Policy is intended solely for, and is applicable only to, current and former California employees. Where relevant, it also applies to job applicants, interns, agency workers, contractors, consultants, directors, and other individuals whose information we collect in connection with providing employment. For ease of reference, this Privacy Policy generally refers to employee data, but this does not indicate in any way that an individual is our employee.

When This Policy Does Not Apply

This Privacy Policy does not apply to individuals who are not California residents.

This Privacy Policy also does not apply to our collection and use of your personal information in a consumer or business-to-business capacity. For more information on our collection and use of your personal information in that capacity, please see our online privacy policy available at www.newamericanfunding.com.

2. Notice at Collection of Personal Information

Personal Information We Collect

The CCPA defines "personal information" to mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident or household. Personal information does not include publicly available, deidentified, or aggregated information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this Privacy Policy, we will refer to this information as "Personal Information."

We or our service providers currently collect and, in the 12 months prior to the Effective Date of this Privacy Policy, have collected the below categories of Personal Information from employees or applicants.

From Employees:

- Identifiers (name, alias, email address, postal address, Social Security number, driver's license number, other types of state identification card numbers such as California ID Cards, emergency contact information, passport number, Internet Protocol address, online identifiers, other similar identifiers)
- Unique personal identifiers (employee number, unique pseudonym, or user alias; cookies, beacons, pixel tags, mobile ad identifiers, or other similar technology; telephone numbers or other forms of persistent or probabilistic identifiers that can be used to identify a particular employee or device)
- Telephone numbers
- Signature
- Physical characteristics or description
- Bank account number

- Corporate card number
- Account log-in, financial account, debit card, or credit card number for corporate account in combination with any required security or access code, password, or credentials allowing access to an account
- Other financial information, such as bank account information for direct deposit
- Internet or other electronic network activity information (browsing history; search history; and information regarding an individual's interaction with a website, application or advertisement)
- Geolocation data
- Medical information
- Insurance policy number or subscriber identification number
- Any unique identifier used by health insurer to identify employee
- Education information
- Professional or employment-related information (including employment history)
- Biometric information (fingerprint; voice recordings from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted; keystroke patterns or rhythms; keystroke patterns or rhythms; and sleep, health, or exercise data that contain identifying information)
- Characteristics of protected classifications under California or federal law (date of birth; age (40 and older); gender identity/expression; sex/gender (including pregnancy, childbirth, breastfeeding and/or related medical conditions); sexual orientation; racial or ethnic origin; disability (mental and physical, including HIV/AIDS, cancer, and genetic characteristics); genetic information; marital status; citizenship or immigration status; medical condition (genetic characteristics, cancer or a record or history of cancer); military or veteran status; status as a victim of domestic violence, assault, or stalking; and requests for family care leave, for leave for an employee's own serious health condition, or for pregnancy disability leave)
- Video information (CCTV video footage)
- Audio, electronic, visual, or similar information that is linked or reasonably linkable to an employee
- Contents of an employee's mail and email
- Inferences drawn from above information to create a profile about an employee reflecting their preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

From Applicants:

- Identifiers (name, email address, postal address)
- Telephone numbers
- Signature
- Characteristics of protected classifications under California or federal law (date of birth; age (40 and older); sex/gender; racial or ethnic origin; marital status; citizenship or immigration status; military or veteran status)
- Geolocation data
- Education information

- Professional or employment-related information (including employment history)
- Inferences drawn from above information to create a profile about an applicant reflecting their preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

Sources of Personal Information

We collect Personal Information directly from California residents and from recruiters; staffing companies; references; former employers; educational institutions; online providers (such as through LinkedIn and similar providers); government entities; other employees; business partners; payroll providers; benefits providers; medical providers; background checks; company bankers; claims handlers; authentication and single sign-on providers; advertising networks; internet service providers; data analytics providers; operating systems, platforms, or software; social networks; and data brokers. We do not collect all categories of Personal Information from each source.

Purposes for Collection

We currently collect and have collected the above categories of Personal Information for all purposes of offering and providing employment, including to:

- Process payroll;
- Enable recruiting services;
- Request you complete applications and forms associated with your employment or prospective employment;
- Consider you for potential employment, including to evaluate your qualifications and eligibility for employment;
- Process security clearances;
- Request you acknowledge your agreement to certain company policies;
- Administer and maintain benefits, including group health insurance, retirement accounts, employee compensation, and employee leave;
- Manage your job-related performance and quality assurance;
- Establish training and/or development requirements;
- Comply with federal and state law;
- Engage in other legitimate business purposes reasonably required for our day-to-day operations such as accounting, financial reporting, and business planning;
- Facilitate remote work arrangements;
- Perform background checks and drug testing;
- Verify your ability to work in this country;
- Identify you as a veteran;
- Perform diversity and inclusion initiatives, including data analysis, development, and deployment;
- Perform company audits;
- Administer our wellness program;
- Contact individuals for emergency purposes;
- Track time and attendance at work;

- Manage workers' compensation claims;
- Arrange business travel;
- Investigate and handle disciplinary actions or termination;
- Detect lost/stolen equipment, fraud, or other types of wrongdoing;
- Grant and monitor your access to secure company facilities and files;
- Engage in corporate transactions requiring review of employee records and information, such as for filing required licensing reports;
- Review web traffic and events, monitor for virus attacks and web content, and determine bandwidth consumption;
- Maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance;
- Maintain commercial licenses for enterprise applications and platforms;
- Prevent the spread of illness and administer programs during a pandemic (e.g., COVID-19);
- Perform call monitoring and surveillance (e.g., CCTV); and
- Enforce our legal rights.

We also use your Personal Information for the purposes described in our Employee Handbook; ADA Service Animal Policy; Call Recording Policy; ID Badge and Security Policy; Injury Illness Prevention Program; Mandatory Pin Enforcement Policy; Technology Use, Privacy Policy, and PIN Enforcement policy; Biometric Information Privacy Policy and Consent Form; Company Device Policy; Remote Worker Policy; and the Handheld Device Acknowledgement and Consent Form.

3. Disclosure of Personal Information

The following tables identify the categories of Personal Information that we disclosed for a business purpose in the 12 months preceding the Effective Date of this Privacy Policy and, for each category, categories of recipients to whom we disclosed Personal Information.

Employees

Categories of Personal Information	**Categories of Recipients**
Personal identifiers - Identifiers (name, alias, email address, postal address, Social Security number, driver's license number, other types of state identification card numbers such as California ID Cards, emergency contact information, passport number); employee number, unique pseudonym, or user alias; telephone numbers; signature; physical characteristics or description; bank account number; corporate card number; account log-in, financial account, debit	Human resource information systems; operating systems and platforms; customer relationship management systems; background check service providers; government or law enforcement entities; applicant and recruiter software and providers; payroll/tax providers; expense management service providers; enterprise travel providers; data analytics providers; company bankers; authentication and single sign-on providers; security providers; mobile device management providers; accountants; lawyers; benefits providers; social networks; company

card, or credit card number for corporate account in combination with any required security or access code, password, or credentials allowing access to an account; other financial information, such as bank account information for direct deposit; biometric information (fingerprint; voice recordings; sleep, health, or exercise data that contain identifying information)	insurers; consultants and other professional advisors
Medical and insurance information - Medical information, insurance policy number or subscriber identification number, any unique identifier used by health insurer to identify employee	Benefits providers; company insurers
Education, employment history, and related information	Applicant and recruiter software and providers; background check service providers; benefits providers; lawyers
Characteristics of protected classifications under California or federal law - Date of birth; age (40 and older); gender identity/expression; sex/gender (including pregnancy, childbirth, breastfeeding and/or related medical conditions); sexual orientation; racial or ethnic origin; disability; genetic information; marital status; citizenship or immigration status; medical condition; military or veteran status; status as a victim of domestic violence, assault, or stalking; and requests for family care leave, for leave for an employee's own serious health condition, or for pregnancy disability leave)	Human resource information systems; operating systems and platforms; customer relationship management systems; government or law enforcement entities; applicant and recruiter software and providers; benefits providers; company insurers; background check service providers; authentication and single sign-on providers; security providers; lawyers
Other information - Video information (CCTV video footage); audio, electronic, visual, or similar information that is linked or reasonably linkable to an employee; contents of an employee's mail and email; inferences drawn from above information to create a profile about an employee reflecting their preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes	Operating systems and platforms; government or law enforcement entities; authentication and single sign-on providers; security providers; lawyers

Applicants

Categories of Personal Information	**Categories of Recipients**
Personal identifiers - Identifiers (name, alias, email address, postal address, Social Security number, driver's license number, other types of state identification card numbers such as California ID Cards, emergency contact information, passport number); telephone numbers; signature	Human resource information systems; operating systems and platforms; customer relationship management systems; background check service providers; government or law enforcement entities; applicant and recruiter software and providers; lawyers
Education, employment history, and related information	Human resource information systems; operating systems and platforms; applicant and recruiter software and providers; background check service providers; lawyers
Characteristics of protected classifications under California or federal law - Date of birth; age (40 and older); sex/gender; citizenship or immigration status; military or veteran status	Human resource information systems; operating systems and platforms; applicant and recruiter software; background check service providers; lawyers

We disclosed Personal Information to the above categories of recipients for the following business or commercial purposes:

- Process payroll;
- Enable recruiting services;
- Request you complete applications and forms associated with your employment or prospective employment;
- Consider you for potential employment, including to evaluate your qualifications and eligibility for employment;
- Process security clearances;
- Request you acknowledge your agreement to certain company policies;
- Administer and maintain benefits, including group health insurance, retirement accounts, employee compensation, and employee leave;
- Manage your job-related performance and quality assurance;
- Establish training and/or development requirements;
- Comply with federal and state law;
- Engage in other legitimate business purposes reasonably required for our day-to-day operations such as accounting, financial reporting, and business planning;
- Facilitate remote work arrangements;
- Perform background checks and drug testing;
- Verify your ability to work in this country;

- Identify you as a veteran;
- Perform diversity and inclusion initiatives, including data analysis, development, and deployment;
- Perform company audits;
- Administer our wellness program;
- Contact individuals for emergency purposes;
- Track time and attendance at work;
- Manage workers' compensation claims;
- Arrange business travel;
- Investigate and handle disciplinary actions or termination;
- Detect lost/stolen equipment, fraud, or other types of wrongdoing;
- Grant and monitor your access to secure company facilities and files;
- Engage in corporate transactions requiring review of employee records and information, such as for filing required licensing reports;
- Review web traffic and events, monitor for virus attacks and web content, and determine bandwidth consumption;
- Maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance;
- Maintain commercial licenses for enterprise applications and platforms;
- Prevent the spread of illness and administer programs during a pandemic (e.g., COVID-19);
- Perform call monitoring and surveillance (e.g., CCTV); and
- Enforce our legal rights.

We have not sold or shared Personal Information in the twelve (12) months preceding the Effective Date of this Privacy Policy. We do not knowingly collect, sell, or share the Personal Information of individuals under 16 years of age. We do not use Sensitive Personal Information for purposes other than those allowed by the CCPA and its regulations.

4. Retention of Personal Information

We retain your Personal Information for as long as necessary to fulfill the purposes for which we collect it, such as to provide you with services you have requested, and for the purpose of satisfying any legal, accounting, contractual, or reporting requirements that apply to us. Please refer to our Record Retention Policy or contact us as described in the "**How to Contact Us**" section below for more information on our employee data retention schedule.

5. Your Rights

If you are a California employee, you have the following rights with respect to your Personal Information:

(1) The right to know what Personal Information we have collected about you, including the categories of Personal Information, the categories of sources from which we collected Personal Information, the business or commercial purpose for collecting, selling, or

sharing Personal Information (if applicable), the categories of third parties to whom we disclose Personal Information (if applicable), and the specific pieces of Personal Information we collected about you;

(2) The right to delete Personal Information that we collected from you, subject to certain exceptions;

(3) The right to correct inaccurate Personal Information that we maintain about you;

(4) If we sell or share Personal Information, the right to opt-out of the sale or sharing;

(5) If we use or disclose sensitive Personal Information for purposes other than those allowed by the CCPA and its regulations, the right to limit our use or disclosure; and

(6) The right not to receive discriminatory treatment by us for the exercise of privacy rights conferred by the CCPA.

6. How to Submit a Request to Know, Delete, and/or Correct

You may submit a request to know, delete, and/or correct your Personal Information through our interactive webform available here, by emailing us at CAPrivacyRequest@nafinc.com or by calling us at 1888-840-4722.

If you are submitting a request on behalf of a California employee, please submit the request through one of the designated methods discussed above. After submitting the request, we will require additional information to verify your authority to act on behalf of the California employee.

In addition to the CCPA rights discussed above, California law provides current and former employees with the right to request certain information relating to their employment, such as the right to access their personnel file and payroll records. Because these requests are governed by laws that contain different requirements than the CCPA, we handle such requests separately from CCPA requests. If you would like to make such a request, please contact the People and Culture Department at pac@nafinc.com.

If you would like to update your personal information, such as to notify us of a change of name or address, or if you have questions about your employment, please contact the People and Culture Department at pac@nafinc.com.

7. Our Process for Verifying a Request to Know, Delete, and/or Correct

We will comply with your request upon verification of your identity and, to the extent applicable, the identity of the California employee on whose behalf you are making such request.

Our verification process may differ depending on whether you maintain a password-protected account with us. If you maintain a password-protected account, we may verify your identity through existing authentication practices available through your account. Prior to disclosing or

deleting the Personal Information, we will ask you to re-authenticate yourself with respect to that account.

If you do not maintain a password-protected account, or if you are an account-holder but we suspect fraudulent or malicious activity with your account, we will verify your identity either to a "reasonable degree of certainty" or a "reasonably high degree of certainty" depending on the sensitivity of the Personal Information and the risk of harm to you by unauthorized disclosure, deletion, or correction as applicable.

For requests to access categories of Personal Information and for requests to delete or correct Personal Information that is not sensitive and does not pose a risk of harm by unauthorized deletion or correction, we will verify your identity to a "reasonable degree of certainty" by verifying at least two data points that you previously provided to us and which we have determined to be reliable for the purpose of verifying identities.

For requests to access specific pieces of Personal Information or for requests to delete or correct Personal Information that is sensitive and poses a risk of harm by unauthorized deletion or correction, we will verify your identity to a "reasonably high degree of certainty" by verifying at least three pieces of Personal Information previously provided to us and which we have determined to be reliable for the purpose of verifying identities. In addition, you will be required to submit a signed declaration under penalty of perjury stating that you are the individual whose Personal Information is being requested.

8. Other Relevant Policies, Including Monitoring

When we hire you, we provide you with other policies and procedures that govern your use of our offices, networks, computers, and other devices. We have the right to monitor your use of our offices and electronic resources in accordance with those policies and procedures.

For more information, please read our Employee Handbook; Call Recording Policy; ID Badge and Security Policy; Mandatory Pin Enforcement Policy; Technology Use, Privacy Policy, and PIN Enforcement policy; Biometric Information Privacy Policy and Consent Form; Company Device Policy; Remote Worker Policy; and the Handheld Device Acknowledgement and Consent Form. You can find copies of these policies on our Company Policies page in ADP or by contacting HumanResources@nafinc.com.

9. Accessibility

We are committed to ensuring this Privacy Policy is accessible to individuals with disabilities. If you wish to access this Privacy Policy in an alternative format, please contact us as described below.

10. How to Contact Us

To contact us for questions or concerns about our privacy policies or practices please contact us at CAPrivacyRequest@nafinc.com.