

California Consumer Privacy Act ("CCPA") Notice/Notice at Collection

California Consumer Privacy Act ("CCPA") Notice/Notice at Collection

Last Updated: August 19, 2026.¹

Your privacy is important to us. This California Consumer Privacy Act ("CCPA") Notice/Notice at Collection ("CCPA Notice" or "Notice") explains how National Bank Holdings Corporation ("NBHC") collects, uses and shares personal information relating to California residents, as required by the California Consumer Privacy Act of 2018 (CCPA), and as amended by the California Privacy Rights Act of 2020 (together, the "CCPA"). This Notice is our notice at collection and privacy policy under the CCPA. Please save, print or download (downloading a printable copy of this notice requires Adobe Reader) a copy for your records.

This Notice applies to NBHC and its subsidiary banks, NBH Bank, and 2UniFi Bank, and affiliates, including 2UniFi, LLC, (collectively and each separately, "NBHC," "we," or "us"). Please note that NBH Bank operates under the following division and brand names: Bank Midwest, Community Banks of Colorado, Vista Bank, Bank of Jackson Hole, Bank Midwest Mortgage, Community Banks Mortgage, Bank of Jackson Hole Mortgage, Bank of Jackson Hole Trust & Wealth, and Vista Private Client. This Notice does not apply to NBHC affiliates unless such affiliate links to this policy.

Introduction

The specific information NBHC collects, uses and shares may vary depending on how you interact with us and your relationship with us. Under CCPA, "personal information" is information that identifies, relates to, or could reasonably be linked, directly or indirectly, to a California resident. This may include things like your name, contact details, account information, online identifiers or geolocation data and certain categories of personal information that constitutes "sensitive personal information," such as government IDs, financial account details, or demographic information. The CCPA,

¹ Effective 7/31/2026, Bank of Jackson Hole Trust changed its name to 2UniFi Bank. The name change does not affect this Notice or how we collect, use, or share your information.

however, does not apply to certain information, including information subject to the Gramm-Leach-Bliley Act (GLBA), which is covered by our [Consumer Privacy Notice](#). For example, if you are a California resident and apply for or obtain our financial products or services for personal, family, or household purposes, that information is covered by our [Consumer Privacy Notice](#) and not this Notice.

Collection, Use and Disclosure of Personal Information

The following charts provide specifics about NBHC's practices related to the collection, use and selling or sharing of personal information. Please note that we may also collect and disclose personal information for other purposes at your direction or with your consent.

General Personal Information

Categories of personal information collected and disclosed	Purpose for collection	Purpose for disclosure
A. Identifiers For example, name or alias, address, online identifier, IP address, email address, account name, SSN, driver's license number, passport number, or other similar identifiers.	• Provide and support products and services • Manage customer relationships and accounts • Identify and handle risks • Detect and prevent fraud and financial crimes • Manage hiring, benefits, performance, and staffing • Comply with legal, regulatory and policy requirements • Promote products and services	Same as collection.

	• Deliver services for other businesses or organizations • Improve internal operations • Enhance customer interactions and service channels		
B. Personal information categories from Cal. Civ. Code § 1798.80(e) For example, identifiers listed above, signature, physical characteristics or description, phone number, state ID number, insurance policy number, bank account number, education, employment, employment history, credit, or debit card numbers, or any other financial, medical or health insurance information.	• Provide and support products and services • Manage customer relationships and accounts • Identify and handle risks • Detect and prevent fraud and financial crimes • Manage hiring, benefits, performance, and staffing • Comply with legal, regulatory and policy requirements • Promote products and services • Deliver services for other businesses or organizations • Improve internal operations	Same as collection.	

	Enhance customer interactions and service channels		
C. Characteristics of CA or federal protected classifications For example, race, religion, national origin, age (40 and over), gender, sexual orientation, medical condition, ancestry, pregnancy (including childbirth, breastfeeding, and/or related medical conditions), familial status, disability, veteran status, or genetic information.	- Provide and support products and services - Manage customer relationships and accounts - Identify and handle risks - Detect and prevent fraud and financial crimes - Manage hiring, benefits, performance, and staffing - Comply with legal, regulatory and policy requirements - Promote products and services - Deliver services for other businesses or organizations - Improve internal operations - Enhance customer interactions and service channels	Same as collection.	
D. Commercial information	Provide and support products and services	Same as collection.	

For example, records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	• Manage customer relationships and accounts • Identify and handle risks • Detect and prevent fraud and financial crimes • Comply with legal, regulatory and policy requirements • Promote products and services • Deliver services for other businesses or organizations • Improve internal operations • Enhance customer interactions and service channels		
E. Biometric information For example, physiological, biological, or behavioral characteristics that can be used to establish individual identity and not limited to imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings.	• Detect and manage risks, including fraud and security using identity verification • Detect and prevent fraud and financial crimes • Improve internal operations	Same as collection. [1]	

F. Internet or other Similar network activity For example, browsing history, search history, and information regarding an individual's interaction with an internet website application, or advertisement.	• Provide and support products and services • Manage customer relationships and accounts • Identify and handle risks • Detect and prevent fraud and financial crimes • Comply with legal, regulatory and policy requirements • Promote products and services • Deliver services for other businesses or organizations • Improve internal operations • Enhance customer interactions and service channels	Same as collection.	
G. Geolocation data For example, information that can be used to determine a person's physical location, such as device location or Internet Protocol (IP) location.	• Provide and support products and services • Manage customer relationships and accounts • Detect and prevent fraud and financial crimes	Same as collection.	

	• Improve internal operations • Enhance customer interactions and service channels		
H. Sensory data or recordings For example, audio, electronic, visual, thermal, olfactory, or similar information that can be linked or associated with a particular individual or household.	• Detect and manage risks, including fraud and security using identity verification • Detect and prevent fraud and financial crimes • Comply with legal, regulatory and policy requirements • Improve internal operations • Enhance customer interactions and service channels	Same as collection.	
I. Professional or employment-related information For example, compensation, evaluations, performance reviews, personnel files, and current and past job history.	• Provide and support products and services • Manage customer relationships and accounts • Identify and handle risks • Detect and prevent fraud and financial crimes	Same as collection.	

	• Manage hiring, benefits, performance, and staffing • Comply with legal, regulatory and policy requirements • Deliver services for other businesses or organizations • Maintain records for continuing education		
J. Education information (defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99)) Education records directly related to a student maintained by an education institution or party acting on its behalf, for example, non-public information that can be used to distinguish or trace an individual's identity in relation to an educational institution either directly or indirectly through linkages with other information.	• Manage hiring, benefits, performance, and staffing • Comply with legal, regulatory, and policy requirements • Maintain records for continuing education	Same as collection.	
K. Profile data	• Manage hiring, benefits, performance, and staffing	Same as collection.	

For example, inferences drawn from personal information to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.			
---	--	--	--

Sensitive Personal Information

Categories of sensitive personal information collected and disclosed	Purpose for collection	Purpose for disclosure	
SSN, driver's license number, state ID number, passport number	• Provide and support products and services • Manage customer relationships and accounts • Identify and handle risks • Detect and prevent fraud and financial crimes • Manage hiring, benefits, performance, and staffing • Comply with legal, regulatory and policy requirements • Deliver services for other businesses or organizations	Same as collection.	
Account login, financial account, debit, or credit card number when provided with any security or	• Provide and support products and services	Same as collection.	

access code, password or credentials allowing access to an account	• Manage customer relationships and accounts • Detect and prevent fraud and financial crimes • Improve internal operations		
Precise geolocation	N/A	N/A	
Racial or ethnic origin, religious or philosophical beliefs, or union membership	• Manage hiring, benefits, performance, and staffing, such as collecting demographic data • Comply with legal, regulatory and policy requirements	Same as collection.	
Contents of an individual's mail, email, and text messages (unless we are the intended recipient)	• Requested in limited circumstances to investigate potential violations of law, regulation, or policy in connection with litigation or threatened litigation	N/A	
Genetic data	N/A	N/A	
Biometric information for the purpose of unique identification	• Detect and manage risks, including fraud and security using identity verification • Detect and prevent fraud and financial crimes	Same as collection.	

		• Improve internal operations	
	Health information	• Provide and support products and services • Manage customer relationships and accounts • Manage employee benefits • Deliver services for other businesses or organizations	Same as collection.
	Information concerning sex life or sexual orientation	• Comply with legal, regulatory and policy requirements • When voluntarily disclosed to manage employment needs such as supporting diversity, equity, and inclusion efforts	Comply with legal, regulatory and policy requirements.

From Whom We Collect Personal Information

The categories of sources from which we collected personal information are:

- Directly from a California resident or the individual's representatives
- Service providers, credit reporting agencies and other similar persons or entities
- Information from our affiliates or subsidiaries
- Website, mobile applications, and social media
- Information from client directed persons, entities, or institutions representing a client/prospect

- Information from corporate clients about individuals associated with the clients (e.g., an employee or board member)
- Outside merchants or business partners such as credit card or lending partnerships or corporate clients
- Public records or publicly available data
- Government entities

What we Sell to Third Parties or Share with Third Parties for Cross-Context Behavioral Advertising and What we Share with Third Parties for Business Purposes

In the past 12 months, we have sold or shared personal information with third parties for cross-context behavioral advertising as disclosed in the table below. We also share personal information for business purposes with the third parties described below. The categories of personal information described in this notice may be shared with a counterparty in relation to evaluating or conducting a merger, acquisition, or divestiture, and may be shared with a third party to facilitate the same.

General Personal Information

Categories of personal information sold to or shared with third parties over the last 12 months	Categories of third parties to whom this category of personal information has been sold or shared for marketing or commercial purposes	Categories of third parties to whom personal information was shared for business purposes (not considered a sale or share under CA law)
A. Identifiers	N/A	• NBHC family companies • Service providers Authorized third parties • Credit reporting agencies • Government and legal entities

B. Personal information categories from Cal. Civ. Code § 1798.80(e)	N/A	• NBHC family companies • Service providers • Authorized third parties • Credit reporting agencies • Government and legal entities
C. Characteristics of CA or federal protected classifications	N/A	• NBHC family companies • Service providers • Authorized third parties • Credit reporting agencies • Government and legal entities
D. Commercial information	• Ad servers, networks, & exchanges • Social media platforms • Online publishers • Data analytics providers • Advertising services platforms	• NBHC family companies • Service providers • Authorized third parties • Credit reporting agencies • Government and legal entities
E. Biometric information	N/A	• NBHC family companies • Service providers
F. Internet or other similar network activity	• Ad servers, networks, & exchanges • Social media platforms • Online publishers • Data analytics providers	• NBHC family companies • Service providers • Authorized third parties

	Advertising services platforms	
G. Geolocation data	N/A	Service providers
H. Sensory data or recordings	N/A	- NBHC family companies - Service providers
I. Professional or employment-related information	N/A	- NBHC family companies - Service providers - Authorized third parties - Credit reporting agencies - Government and legal entities
J. Education information	N/A	N/A
K. Profile data	N/A	N/A

Sensitive Personal Information

Categories of sensitive personal information sold to or shared with third parties over the last 12 months	Categories of third parties to whom this category of personal information has been sold or shared for marketing or commercial purposes	Categories of third parties to whom personal information was shared for business purposes (not considered a sale or share under CA law)
Social Security Number, driver's license, state identification card, or passport number	N/A	- NBHC family companies - Service providers - Authorized third parties

		• Credit reporting agencies • Government and legal entities
Account log-in, financial account, debit card, or credit card number when provided with any required security or access code, password, or credentials allowing access to an account	N/A	• Service providers
Precise geolocation	N/A	N/A
Racial or ethnic origin, religious or philosophical beliefs, or union membership	N/A	• Service providers • Government and legal entities • Legal and compliance reasons
Contents of an individual's mail, email, and text messages (unless we are the intended recipient of the communication)	N/A	N/A
Genetic data	N/A	N/A
Biometric information for the purpose of unique identification	N/A	• NBHC family companies • General business purposes
Health information	N/A	• Service providers • Government and legal entities

Information concerning sex life or sexual orientation	N/A	• Government and legal entities • Legal and compliance reasons
---	-----	---

In the 12 months preceding the date of this Notice, we have not “sold” sensitive personal information subject to the CCPA.

Notice of Right to Opt Out of Sale/Sharing

You may exercise your Right to Opt Out of Sale/Sharing in the following ways:

We do not use tags, cookies, pixels or other tracking technologies on our websites or mobile applications to sell or share your personal information with third parties unless you provide us with your consent first (opt in).	To provide consent or to opt in, click on the cookie icon  that appears in the bottom left corner of our website and select your choices. You can come back here at any point to make changes.
To opt out of other personal information sold to or shared with third parties	1. Submit an Opt Out of Sale or Sharing of Personal Information request through our Privacy Center, or 2. Email your request to privacy@nbhbank.com, or 3. For NBH Bank or 2UniFi Bank call us at 1.866.217.6361 4. For 2UniFi, LLC (“2UFI”) call us at 1.844.988.2UFI (2834)

How We Use Sensitive Personal Information

We only use or disclose sensitive personal Information for the following purposes consistent with CCPA regulations:

- To provide our goods and services as reasonably expected by an average consumer
- To prevent, detect, and investigate security incidents affecting personal information, provided that the use of personal information is necessary and proportionate for this purpose
- To resist malicious, deceptive, fraudulent, or illegal actions against us and prosecuting those responsible for those actions, provided that the use of personal information is necessary and proportionate
- To ensure the physical safety of an individual, provided that the use of personal information is necessary and proportionate for this purpose
- For short-term, transient use, including non-personalized advertising shown as part of an individual's current interaction with us, if we do not build a profile about the individual or alter the individual's experience outside their current interaction with us
- To perform services on behalf of another business (e.g., maintaining accounts, processing orders, or transactions)
- To verify and maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, or improving, upgrading, or enhancing the services or device owned, manufactured, manufactured for, or controlled by us
- For any collection or processing that is not for the purpose of inferring characteristics about you

Retention of Personal Information

NBHC has established product and business-level criteria for retention and disposal according to business requirements, laws, regulations, and applicable industry standards.

Consumer Rights Under the CCPA

If you are a California resident covered by the CCPA, you have the right to:

1. Request we disclose to you free of charge the following information covering the 12 months preceding your request:
2. the categories of personal Information about you that we collected
3. the categories of sources from which personal information was collected
4. the purpose of collecting personal information about you
5. the purpose for sharing personal information about you
6. the categories of third parties to whom we disclosed personal information (including sensitive personal information) about you and the categories of personal information that were disclosed (if applicable) and the purpose for disclosing personal information about you
7. the specific pieces of personal information we collected about you
8. Request we correct inaccurate personal information that we maintain about you
9. Request we delete personal information we collected from you, unless the CCPA recognizes an exception
10. Opt Out from sharing or selling as indicated above in the Section entitled, ["Notice of Right to Opt Out of Sale/Sharing"](#)

Please see the section below entitled, ["How to Exercise Your Rights"](#) for instructions explaining how you can exercise these rights described above.

Requests for specific pieces of personal information will require additional information to verify your identity. Information submitted for verification purposes will only be used to verify the requestor's identity and/or authority to make a request on another's behalf.

For individuals submitting a request on behalf of another person, we may require proof of authorization and verification of identity directly from the person for whom the request is made.

For a company or organization submitting a request on behalf of another person, we may require proof of authorization from the individual, such as a Power of Attorney and verification of identity directly from the person for whom the request is made.

In some instances, we may not be able to honor your request. For example, we will not honor your request if we cannot verify your identity or if we cannot verify that you have the authority to make a request on behalf of another individual. Additionally, we will not honor your request where an exception applies, such as where the disclosure of personal information would adversely affect the rights and freedoms of another California resident or where the personal information that we maintain about you is not subject to the CCPA's access or deletion rights.

We will advise you in our response if we are not able to honor your request. We will not provide Social Security numbers, driver's license numbers or government-issued identification numbers, financial account numbers, unique biometric data, health care or medical identification numbers, account passwords or security questions and answers, or any specific pieces of information if the disclosure presents the possibility of unauthorized access that could result in identity theft or fraud or unreasonable risk to data or systems and network security.

We will process all verified requests within the required 45 days under CCPA. If we need more time (up to an additional 45 days) to process your request, we will provide you with an explanation for the delay.

Opt-Out Preference Signals

NBHC permits California residents to automatically exercise their right to opt out of sale/sharing through opt-out preference signals without having to make individualized opt-out requests. This is a setting in your browser that notifies the websites you visit of your preferences to opt out of selling or sharing your personal information under California law. We treat opt-out preference signals as valid requests to opt out of sale/sharing for the browser.

Non-Discrimination

The submission of any CCPA request will have no impact on the service and/or pricing you receive from us. It will not result in any denial of goods or services, or different prices, rates or quality of goods or services. It will not result in retaliation against an employee, applicant, or independent contractor.

Individuals Under 16 Years of Age

We do not knowingly sell or share personal information, including sensitive personal information, of children under the age of 16.

How to Exercise Your Rights

If you are a California resident, you may submit a request to access, correct, or delete your personal information by:

1. Submitting a [Personal Information Request](#) through the Privacy Center
2. Emailing your request to privacy@nbhbank.com
3. For NBH Bank: Calling us at **1.866.217.6361**
4. For 2UniFi, LLC ("2UFI"): Calling us at **1.844.988.2UFI (2834)**

Please see the section above entitled, ["Notice of Right to Opt Out of Sale/Sharing"](#) for instructions on how you can exercise your rights to opt out of the sale/sharing your personal information.

Keeping Your Information Safe

Protecting your personal information is a top priority. We use a combination of physical, technical, and organizational safeguards designed to protect your data against unauthorized access, loss, misuse, or disclosure—whether it is handled by us directly or by service providers acting on our behalf.

Questions or Concerns

You may contact us with questions or concerns about this Notice and our practices by:

1. Writing to us at:
NBHC Privacy
P.O. Box 410076
Kansas City, MO 64141-0076
2. Emailing us at: privacy@nbhbank.com
3. Visiting our websites at **nbhbank.com** or **2ufi.com**

This California Consumer Privacy Act Notice

We may change or update this Notice from time to time. When we do, we will post the revised Notice on this page with a new “Last Updated” date. You may access this Notice online at our Privacy Center.

[\[1\]](#)About biometric-enabled sign-ons: Your device stores the information it needs to recognize your facial features or fingerprints. NBHC does not have access to the information your device uses to enable facial or fingerprint recognition, nor does NBHC have access to or store your facial image or fingerprint data. Your device’s user information will have additional information regarding its user controls and settings, including its privacy and security controls.