

**Effective Date: March 18, 2024**

**Updated: March 18, 2024**

*PLEASE CAREFULLY READ THE POLICY BEFORE USING THE SITE. BY ACCESSING OR USING THE SITE, YOU AGREE TO THE POLICY. THE POLICY MAY CHANGE FROM TIME TO TIME. YOUR CONTINUED USE OF THE SITE AFTER WE MAKE CHANGES TO THE POLICY IS YOUR CONSENT TO THOSE CHANGES. CHECK THE POLICY REGULARLY FOR UPDATES.*

Platinum Bank and its affiliates (“we,” “our,” or “us”) respect your privacy and is committed to transparency regarding how we handle your information. This Digital Privacy Policy (the “Policy”) explains how we collect, use, and disclose your information. The Policy applies to any website, mobile application, or other digital service that we own and control (the “Site”) unless a different privacy policy is posted relating to a particular Site that you access. As you read this Policy, please note that software, hosting, and other technology functions on the Site may be provided by entities that process your information on our behalf and based on our instructions (“Service Providers”). We require our Service Providers to handle your data in compliance with applicable law and this Policy.

By using our Site, you consent to the collection, use, and sharing of your information subject to and consistent with this Policy, applicable laws and regulations, and other communication from us that you may have received based on your relationship with us.

## PROTECTING CHILDREN’S PRIVACY ONLINE

The Site is not intended for individuals under the age of thirteen. If you are under the age of thirteen, do not provide Personal Information through the Site. We do not knowingly collect information from children under thirteen. Visit the Federal Trade Commission website for more information about the Children’s Online Privacy Protection Act (COPPA).

## INFORMATION COLLECTION ON THE SITE

When you visit our Site, the types of user data or information about you we obtain about you depends on how you interact with us and our products and services. If you have a financial product or service with us, we will use and share any information that we collect from or about you in accordance with our Privacy Notice, which offers you certain choices with respect to the use and sharing of your personal information. We do not sell (meaning disclosing, disseminating, making available, transferring, or otherwise communicating to a third party for monetary consideration) user data or information about you. We collect user data and information about you and share such information with our Service Providers only for business purposes, such as:

- Auditing, compliance, and examination
- Ensure security and integrity of the Site
- Fraud prevention
- Debugging to identify and repair errors that impair functionality of the Site
- Short-term, transient use, as part of your current interaction with the Site
- Performing services for you that you request
- Communicating with you, including answering your questions
- Advertising and marketing our services to you
- Internal research for technological development and demonstration
- Activities to verify or maintain the quality or safety of the Site and to improve, upgrade, or enhance the Site
- Complying with and enforcing applicable legal requirements, relevant industry standards, contractual obligations, and our policies

## RETENTION PERIOD

We will only retain your personal information for the period reasonably necessary to fulfill the purposes outlined in this Policy unless a longer retention period is required by law, including federal or state banking law regarding records retention.

Information We Collect:

## PERSONAL INFORMATION

When you visit or use the Site, we may collect personal information from or about you including your name, email address, mailing address, telephone and/or cellphone number(s), account numbers, limited location information, username, and password. We may also collect payment card information, tax identification numbers, driver’s license numbers (or comparable), or other information you choose to share with us when you provide such information while using our Site and where we believe such information is reasonably required for ordinary business purposes.



If you grant permission to use access photos, media, or other files stored on your device we, through our Service Provider Jack Henry, will use that information to add an image to a transaction, to attach a document to chat, and add a photo to your profile. If you grant permission to use a camera, we will use it when taking a picture to add an image to a transaction or to capture images of a check that is being deposited or to add a photo to your profile.

#### DIGITAL CHAT OR TEXT MESSAGES WITH OUR EMPLOYEES

Your session on the Site will be recorded and monitored to collect data and manage any digital chats or communications by text message that you may have with our employees. To do this, we may utilize screen sharing technology, which can allow us to help you navigate through the site and find information in real time, making it easier for you to interact with us through the Site. Any text messages between you and our employees will be collected to ensure our employees' compliance with applicable legal requirements and our policies.

#### USAGE AND OTHER INFORMATION

In addition to the personal information described above, we may collect certain information about your use of the Site. For example, you can browse our website without telling us who you are. However, our Site automatically collects and stores: 1) the name of the domain and host from which you access the Internet; 2) the Internet protocol (IP) address of the computer you are using; 3) the browser software you use and your operating system; 4) the date and time you access our Site; and 5) and the Internet address of the site from which you linked directly to our Site. If you are accessing the Site on a mobile device, the Site may collect persistent device identifiers (for example, IMEI, IMSI, or SIM Serial number). Your persistent device identifiers will not be linked to other personal and sensitive user data or resettable device identifiers except for the purposes of: 1) telephony linked to a SIM identity (for example, WiFi calling linked to a carrier account); and 2) enterprise device management apps using device owner mode.

#### COOKIES, WEB BEACONS, AND OTHER TRACKING TECHNOLOGIES

We and our Service Providers collect information about your activity on the Site using tracking technologies, including:

- **Cookies.** Cookies are small amounts of data a website can send to your web browser. Cookies allow us to collect information such as the type of browser you are using, the amount of time you spend using the Site, other websites, or applications you visit, and the preferences you have set up for your accounts. We use this information to personalize your experience, enhance security, facilitate navigation, display material more efficiently, recognize the device that you are using to access the Site, and understand how the Site is used. While each device and each browser is different, many web browsers allow you to adjust your browser settings to decline or delete cookies. Doing so may degrade your experience with our Site. Please note that you will need to manage your cookie settings for each device and browser that you use.
- **Pixel tags, web beacons, clear GIFs and other similar technologies.** These technologies are typically one-pixel, transparent images located on a webpage or in an email or other message. We may use these or similar technologies on the Sites and in some of our digital communications (such as email or other marketing messages). Such technologies may also be used when you are served advertisements or you otherwise interact with advertisements outside of our Site. These technologies help us recognize users, assess traffic patterns, and measure Site or marketing campaign engagement. We may use these technologies to bring together information we collect about you, but we never sell this information.
- **Location tracking on mobile devices.** Certain applications on mobile devices may transmit information to us about your location. For example, this could include your physical location when you search for a nearby ATM using your mobile device. We may use that information to improve the products and services we provide to you as well as improving our services generally in your area.
- **Advertising Service Providers.** We use advertising Service Providers to place advertisements for our services on websites not affiliated with us, and to help us determine which of our advertisements are most likely to be of interest to you using non-personal behavioral information. Advertisements placed by these Service Providers may use tracking technologies that allow monitoring of your responsiveness to such advertisements. We restrict Service Providers by agreements with us from collecting information about you on our behalf for purposes other than assisting us with our advertising efforts.

#### YOUR CONSENT TO CELLPHONE AND WIRELESS DEVICE CONTACT

By providing us with a telephone number for a cellphone or other wireless device, you are expressly consenting to receiving communications, including marketing communications, from us. Those communications include but are not limited to: 1) prerecorded or artificial voice message calls; 2) text messages; 3) calls made by an automatic telephone dialing system. This express consent applies to each such telephone number that you provide to us now or in the future and permits such calls for marketing and non-marketing purposes. Please note that calls and messages may incur access fees from your cellular provider.

To help us verify your identity, you authorize your wireless operator (AT&T, Sprint, T-Mobile, US Cellular, Verizon, or any other branded wireless operator) to use your mobile number, name, address, email, network status, customer type, customer role, billing type, mobile device identifiers (IMSI and IMEI) and other subscriber status details, if available, to allow us to verify your identity, and to compare information you have provided to us with your wireless operator account profile information for the duration of our relationship. See our Privacy Notice for more information on how we treat your data.



**SECURITY AND PROTECTION OF INFORMATION**

To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. No data transmission or storage system can guarantee security. If you have reason to believe that your interaction with the Site is no longer secure, notify us immediately at 651-332-5200.

Please note that information you send to us electronically may not be secure when it is transmitted to us. We recommend that you do not use unsecure channels to communicate sensitive or confidential information to us.

**IDENTITY THEFT AND EXTERNAL AGGREGATION SERVICES**

You are responsible for helping us protect your accounts. Carefully consider the risks before revealing your username, password, or other credentials to any person or third party. By providing your username, password, or other credentials to any person or third party (including an aggregation service) you authorize that person or third party to initiate transfers to or from your account.

Some third-party companies offer aggregation services that allow you to consolidate your financial account information from a variety of sources and view that information at a single online location. For example, an aggregation service might collect and consolidate your checking and savings account balances at your bank, the value of your stocks and bonds in your brokerage account, and your frequent flier mileage information from airlines. In order to do so, the aggregation service may request personal information from you, including identification information, account information, usernames, and passwords, for each individual account.

Please use caution when providing personal information to an aggregation service. By providing your username, password, or other credentials to an aggregation service you authorize that person or third party to initiate transfers to or from your account.

To help us protect your personal information, you must always keep your account information safe. Additional information regarding identity theft and the steps you can take to help protect yourself from fraud can be found on the Federal Trade Commission website.

**WARNING REGARDING LINKED WEBSITES**

The Site may contain links to third-party websites or mobile applications not controlled by us. When you leave the Site, we encourage you to read the privacy policies and terms of use of any such websites or mobile applications that may collect user data or information about you. The privacy policies and terms of any third-party website or mobile application will likely differ from those of the Site. We do not guarantee and are not responsible for the privacy policies or security of these websites and mobile applications, including the accuracy, completeness, or reliability of their information. In addition, we are not responsible for the information collection, use, and disclosure practices (including the data security practices) of other organizations, such as Facebook, Apple, Google, Microsoft or any other app developer or provider, social media platform provider, operating system provider, wireless service provider, or device manufacturer.

**CROSS-BORDER TRANSFER**

The Site is controlled and operated by us from the United States and is not intended to subject us to the laws or jurisdiction of any country or territory other than that of the United States. We may store and process your personal information in any country where we have facilities or in which we engage Service Providers. By using the Site, you consent to the transfer of your information to countries outside of your country of residence, including the United States, which may have different data privacy and data protection laws than those of your country.

**California Residents**

California law may provide California residents with additional rights regarding their personal information. To learn more about these rights, see our California Privacy Notice.

**Contact Us**

If you have any questions or comments about this Policy, we encourage you to contact us by calling 651-332-5200 or visiting the "Contact Us" page on our website.



Effective Date: March 18, 2024

Updated: March 18, 2024

This disclosure is addressed to California residents only and concerns the practices of Platinum Bank and its affiliates (“we,” “our,” or “us”) that relate to personal information of California residents. It explains what personal information we collect, where we collect it from, what we use it for, who we disclose it to, how long we keep it, the rights California residents may have, and how to exercise them.

We are providing this notice as required by the California Consumer Privacy Act (“CCPA”) of 2018, as amended by the California Privacy Rights Act (“CPRA”) of 2020, also known as Proposition 24, which provides California residents with important privacy rights. We encourage you to visit <https://privacy.ca.gov> to learn more about your rights. Please note that the CCPA, and this disclosure, do not apply to information covered by other federal and state privacy laws, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act.

Under the limited circumstances where we are acting as a business, and your personal information is not otherwise excluded as set forth above, the following information applies as to how we collect, use, share and/or sell your personal information.

### CATEGORIES OF PERSONAL INFORMATION THAT WE COLLECT AND WHY WE COLLECT IT

When you visit our Site, the types of personal information we obtain about you depends on how you interact with us and our products and services. If you have a financial product or service with us, we will use and share any information that we collect from or about you in accordance with our Privacy Notice, which offers you certain choices with respect to the use and sharing of your personal information. We do not sell (meaning disclosing, disseminating, making available, transferring, or otherwise communicating to a third party for monetary consideration) user data or information about you. We collect user data and information about you and share such information with our Service Providers only for business purposes in the categories described below:

CATEGORY	EXAMPLES	PURPOSE FOR COLLECTION
Personal Identifiers	Your full name, any aliases, date of birth, postal address, unique personal identifiers, online identifiers, Internet Protocol (IP) address, persistent device identifiers (IMEI, IMSI, or SIM Serial number), email address, account name, social security number, driver’s license number, passport number, state identification number, citizenship, and immigration status	Communicating with you; Performing services; Marketing our services; Research and development; Quality assurance; Security/Fraud Prevention; To comply with our legal obligations
Personal Records	Your signature, physical characteristics or description, address, telephone number, insurance policy number, education, employment, employment history, bank account number, credit or debit card number, other financial information	Communicating with you; Performing services; Marketing our services; Research and development; Quality assurance; Security/Fraud Prevention; To comply with our legal obligations
Characteristics of protected classes	Characteristics of protected classes or groups under state or federal law, such as sex or marital status	Performing services; Research and development; Quality assurance; Security/Fraud; To comply with our legal obligations
Purchase Information	Your records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies	Performing services; Marketing our services; Research and development; Quality assurance; Security/Fraud Prevention; To comply with our legal obligations
Biometric Information	Your biometric information, such as fingerprints and voiceprints	Performing services; Security/Fraud Prevention



Internet or Online Information	Information regarding your interactions with our websites and applications, computer systems, and devices	Communicating with you; Performing services; Marketing our services; Research and development; Quality assurance; Security/Fraud Prevention; Debugging; To comply with our legal obligations
Geolocation Data	Your device location, IP address when visiting our website, or your physical location when using an ATM	Performing services; Research and development; Quality assurance; Security/Fraud Prevention; Debugging; To comply with our legal obligations
Audio and Visual Information	Audio, electronic, or visual, such as when you call our text us regarding our services	Performing services; Quality assurance; Security/Fraud Prevention; To comply with our legal obligations
Employment Information	Your work history and prior employer information	Performing Services; Marketing our services; Research and development; Quality assurance; Security/Fraud Prevention; To comply with our legal obligations
Education Information	Schools you attended and degrees you have received	Performing services
Inferences	Inferences based on information about an individual to create a summary about, for example, an individual's preferences and characteristics	Performing services; Marketing our services; Research and development; Quality assurance; Security/Fraud Prevention

## CATEGORIES OF SOURCES OF PERSONAL INFORMATION

In the past 12 months we have collected personal information about California residents from the following categories of sources:

- Directly from you, when you provide it to us digitally or physically (e.g., where you contact us via email or telephone, or by any other means)
- From our affiliates
- From your employer, when your employer is a client of ours
- From public sources, when you manifestly choose to make it public, including via social media (for example, we may collect information from your social media profiles if you choose to share information publicly)
- From service providers and third parties who provide it to us (for example, our customers, wireless providers, consumer reporting companies, or law enforcement authorities)
- When you visit our websites or mobile applications we may collect certain information about your use of those websites and mobile applications. For example, you can browse our website without telling us who you are. However, our website automatically collects and stores: 1) the name of the domain and host from which you access the Internet; 2) the Internet protocol (IP) address of the computer you are using; 3) the browser software you use and your operating system; 4) the date and time you access our Site; and 5) and the Internet address of the site from which you linked directly to our Site. If you are accessing our website or mobile applications on a mobile device, we may collect persistent device identifiers (for example, IMEI, IMSI, or SIM Serial number). Your persistent device identifiers will not be linked to other personal and sensitive user data or resettable device identifiers except for the purposes of: 1) telephony linked to a SIM identity (for example, WiFi calling linked to a carrier account); and 2) enterprise device management apps using device owner mode.



## DISCLOSURE OF PERSONAL INFORMATION

In the past 12 months we have disclosed the categories of California residents' personal information listed in the table above for the purposes stated in that table to some or all of the following categories of recipients:

- You and, where appropriate, your family, your associates and your representatives
- Our affiliates
- Fraud detection and prevention services providers
- Accountants, auditors, examiners, financial advisors, lawyers and other outside professional advisors, subject to confidentiality and as required or permitted by law
- Service providers
- Consumer reporting agencies
- Governmental, legal, regulatory, or other similar authorities and/or local government agencies, upon request or where required
- Other third parties to comply with legal requirements such as the demands of applicable subpoenas and court orders; to verify or enforce our rights or policies; to address fraud, security or technical issues; to respond to an emergency; or otherwise to protect the rights, property, or security of our customers or third parties
- Other parties, if you specifically direct or expressly consent to us disclosing your personal information to them

## RETENTION PERIOD

We will only retain your personal information for the period reasonably necessary to fulfill the purposes outlined in this disclosure unless a longer retention period is required by law, including federal or state banking law regarding records retention.

## YOUR RIGHTS AND CHOICES

This section describes your CPRA rights and explains how to exercise those rights. Your rights under the CPRA include:

1. Right to Limit the use and disclosure of sensitive personal information collected about you, if applicable.
2. Right to Opt-Out of the sale of your personal information and the sharing of your personal information for cross-context behavioral advertising (for example, targeted advertising).
3. Right to Correct inaccurate personal information that businesses have about you.
4. Right to Know what personal information businesses have collected about you and how they use and share it.
5. Right to Equal treatment and no retaliation following Opt-Out or you exercise of other rights. Businesses cannot discriminate against you for exercising your CCPA rights.
6. Right to Delete personal information businesses have collected from you, if applicable.

## HOW TO EXERCISE YOUR RIGHTS

To exercise your rights to correct, know, and delete described above, please submit a verifiable consumer request to us through one of the following methods:

1. Emailing us at [clientsupport@platinumbankmn.com](mailto:clientsupport@platinumbankmn.com); or
2. Calling us toll free at 888-696-0669

Please note, if applicable and in accordance with Cal. Code Regs. tit. 11, § 7026(d), we do not require a verifiable consumer request, as described below, for a request to opt-out of sale/sharing.

We will respond within 45 days of your verifiable consumer request unless additional time is reasonably necessary to respond to your request. If we need an additional 45 days, we will provide you a notice of extension within the first 45-day period.

Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child, if applicable. To designate an authorized agent, please contact us through one of the methods stated above.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative; and
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us.



**RIGHT TO LIMIT AND RIGHT TO OPT-OUT REQUESTS:**

We do not sell your information to third parties for monetary consideration. Per Cal. Code Regs. tit. 11, § 7027(m), we only share your personal information as commercially necessary and in accordance with this California Privacy Notice. We do not share your information with affiliates for direct marketing to you.

**RIGHT TO KNOW AND DATA PORTABILITY REQUESTS:**

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we disclosed your personal data for a business purpose, a listing identifying the personal information categories that each category of recipient obtained.

**RIGHT TO DELETE REQUESTS:**

You have the right to request that we delete any personal information we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete—and direct our service providers to delete—your personal information from our records, unless an exception applies. We may deny your deletion request if retaining the information is necessary for us or our service providers to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.).
6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
8. Comply with a legal obligation.
9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

