Online & Digital Customer Privacy Policy Notice

Commitment to Privacy

First Dakota National Bank established this policy to protect the confidentiality of our customers' financial records and the relationship between us and our customers. First Dakota understands the responsibility financial institutions have with safeguarding their customers' sensitive information.

The Online & Digital Customer Privacy Policy describes how we manage personal information when customers interact with us online through our website, digital banking applications, and social media sites. Customers may interact with us using their computer, mobile phone, or tablet.

We recognize the reasonable expectation of privacy for all our customers and the importance of protecting that privacy. As a result, the following Online & Digital Customer Privacy Policy has been implemented by First Dakota National Bank, here and after collectively referred to as "we/our/us."

How We Manage Customer Information

We want customers to understand and be comfortable with our privacy policies. We realize and respect its importance as an issue and will respond to any request for information regarding our privacy policies and procedures.

We will only collect and retain pertinent information allowed by law. We will not collect or retain unnecessary information. We do not share customers' non-public information.

We have established procedures to ensure that a customer's financial information is accurate, current, and complete in accordance with reasonable commercial standards. We will respond in a timely manner to requests to correct inaccurate information.

We limit employee access to personally identifiable information to those with a business reason for knowing such information. We educate our employees so they understand the importance of confidentiality and customer privacy. We will also take disciplinary measures to enforce employee privacy responsibilities.

We have placed restrictions on how customer account information can be disclosed. We will not reveal specific information about customer accounts or other personally identifiable data to unaffiliated third parties unless:

- A legitimate business purpose has been established.
- The information is exchanged with a reputable information-reporting agency.
- The information is provided to help complete a customer-initiated transaction, and the customer has authorized the information to be released.
- The disclosure is required by/or allowed by law (i.e., subpoena, investigation of fraudulent activity, etc.).

When personal customer information is provided to a third party, we expect the third party to adhere to similar privacy principles that provide for the safekeeping of confidential information.

The Types of Information We Collect

We do gather data regarding visits to our website, including domain name, pages visited, length of user session, etc., to evaluate the usefulness of our site. We only collect personal information when customers provide it by applying for our services or our career opportunities. When consumers are simply visiting our website, we do not collect any personal data about them.

Personal Information Collected

We collect information when consumers use our online or digital banking applications. When they enroll in online banking or download our app, we require them to create a username and password. We will gather personal information such as their name, email address, phone number, and account number. They will be asked security questions. Once a customer's online/digital banking profile is created, we will retain the information necessary to allow them to use our online service or digital banking services, such as their account number, IP address, and mobile phone number.

When consumers apply for a new account online, we will collect and retain personal information, including their name, address, phone number, Social Security Number, date of birth, email address, and other credit verification information.

- We do not store any information entered into the application during data entry. Our application process will time out after ten (10) minutes of inactivity. When an application has been inactive for more than ten (10) minutes, the consumer will need to start the application over from the beginning.

We may also collect information when they use our website or digital banking app, such as the Internet Provider (IP) address of their device (computer, mobile phone, or tablet), the type of operating system/browser they use, the areas of our website/app they use, and links clicked.

When using our digital banking app after permission is granted, we will use the customer's:

- Biometrics (fingerprint or face ID) to securely enable functionality.
- Mobile device camera to capture their profile picture, check images (mobile deposit), receipts, and other transaction images.
- Geographical location to provide them with the closest branch or ATM location.

Non-Personal Information Collected

We may use various website analytics tools and technologies, such as Google Analytics, regarding activities on our site that require storage of web session data. The overall aim of these tools is to aid in making our website easy to use, proactively identify and correct error conditions, and provide more relevant advertising and content to customers. These tools and technologies are also used to assist website visitors who report problems with the use of our site. Stored web session data is used in accordance with this privacy policy. For more information on how Google uses data

- Visit http://www.google.com/policies/privacy/partners/. When users click the link, they will be leaving First Dakota's website. Any products or services accessed through this link are not provided, endorsed, or guaranteed by First Dakota. Users

are advised that First Dakota's privacy policy does not apply to the linked website, and they should consult the privacy disclosures on the third-party site for further information.

We may employ cookies (i.e., small text files) that our website may send to a user's browser for storage on their hard drive, and later processes may check for the presence of such cookies. We may use such cookies to make use of our site easier by saving their status and preferences upon visits to our website. We may also employ cookies, web beacons, or site instrumentation to monitor the behavior of visitors to our site and activity on our site, such as the number of visitors to our website.

- Most browsers are initially set to accept cookies, but users may be able to change the setting in their browser to refuse cookies or to alert them when cookies are being sent.

Third-party service providers may place and administer cookies and web beacons via our website or check for the presence of our cookies on a user's device. Such third parties may collect the user's anonymized information and perform website analytics as described in this privacy policy. We and/or such third parties may also use the reports created by such third parties based upon web analytics data or other similar data collected from visitors to our site in connection with providing users with more relevant advertising and content on our site and sites across the Internet. When users want to opt out of Google's use of cookies or device identifiers, they can manage their settings on the Google Ad Settings page. When users want to opt out of third-party cookies and device identifiers, they can manage their settings at the Network Advertising Initiative opt-out page.

We do not respond to "do not track" signals. Some web browsers send "do not track" signals to the websites and other online services with which the browser communicates. No standard governs what, if any, a website should do when receiving these signals. If and when a standard is established, we may revise our policy on responding to the "do not track" signals.

How We Use Personal Information

We use the information collected to:

- Provide customers with online and digital banking access.
- Maintain and improve our online and digital banking services.
- Process customer requests, transactions, applications, inquiries, and messages.
- Report to credit bureaus.
- Allow customers to apply for services such as accounts and prequalify for mortgage loans.
- Provide customers with information and required documents they require and for customer service purposes.
- Identify customers as legitimate users in our system.
- Prevent fraud and security risks and enhance the security of customers' accounts.
- Communicate with customers.
- Comply with laws, regulations, and court orders.
- Offer customers our products, services, and marketing messages. Customers may opt-out of receiving marketing messages from us by following the opt-out processes described in the messages.

Links To Other Sites

Our website may include links to other external third-party sites. These links are offered as a courtesy and convenience to our customers. We do not control third-party sites. We are not an agent for these third parties, nor do we endorse or guarantee their products. We make no representation or warranty regarding the accuracy of the information contained in the external third-party sites. The security and privacy policies of the third-party site may be different from our policies. We recommend customers thoroughly read third-party privacy and security policies.

How We Share Information

We share customer information with our credit card company, which is our joint marketing partner. First Dakota does not have affiliates, and we do not share customer information with non-affiliates to market to them. For additional information, see the First Dakota Privacy Policy issued at account opening.

How We Protect Personal Information

To protect customers' personal information from unauthorized access and use, we implement reasonable technical and physical measures to safeguard the information we retain in compliance with our information security program. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure, and we cannot ensure or warrant the security. Our digital banking app setting options include the ability to remove a customer profile and remove its data. When a customer believes their data has been compromised, they should contact us immediately.

Our third-party providers are required to keep customer information confidential and secure. In the event of a data breach, we will provide customers with timely notification as required by laws and regulations.

Data Retention

We retain customer information based on our retention policy in accordance with applicable state laws and federal regulations.

Children's Privacy Online

Our website and digital banking services are not directed to children under the age of thirteen. First Dakota does not allow children under the age of thirteen to open accounts online without an adult as a joint owner. We do not knowingly collect or use personal information from children under thirteen from our website without obtaining verifiable consent from their parents or legal guardians. Should a child whom we know to be under the age of thirteen send personal information to us, we will only use that information to respond directly to that child, seek parental/legal guardian consent, or provide parental/legal guardian notice. We are not responsible for the data collection and use practices of nonaffiliated third parties to which our websites may link.

Online/Digital Banking App Privacy Policy Updates

This policy is subject to occasional revisions. The date of the updated policy will show in the last revision date at the top of the policy. We will notify customers of material changes to the

policy by posting the notice on our website, digital banking, and messages. The policy changes will be effective thirty (30) calendar days following the change notice.

Contacting Us

Customers can visit one of our First Dakota locations, call us toll-free at 800-486-4712, send us a secure message in digital banking, or visit www.firstdakota.com.