

Privacy Policy

Our Privacy Policy

At St. Kitts-Nevis-Anguilla National Bank LTD., accessible from <https://www.sknanb.com/>, one of our main priorities is the privacy of visitors to our site.

This Privacy Policy document contains our policies regarding the collection, use, and disclosure of personal data when you use our Service and the choices you have associated with that data.

We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy.

If you have additional questions or require more information about our Privacy Policy, do not hesitate to contact us through email at: customerservice@sknanb.com

What is Personal Data

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personal Data may include, but is not limited to:

1. Email address
2. First name and last name
3. Phone number
4. Address, State, Province, ZIP/Postal code, City
5. Cookies and Usage Data

Why We Collect and Use Personal Data

We collect personal data to provide and improve our Service to you.

The purposes include:

1. Developing and providing banking facilities, products or services;
2. Assessing and processing applications, instructions or requests from you;
3. Communicating with you, including providing you with updates on changes to products, services and banking facilities;
4. Managing our infrastructure and business operations and complying with internal policies and procedures;
5. Responding to queries or feedback;
6. Addressing or investigating any complaints, claims or disputes;
7. Verifying your identity for the purposes of providing banking facilities, products or services;

8. Conducting credit checks, screenings or due diligence checks as may be required under applicable law, regulation or directive; and
9. Seeking professional advice, including legal advice.

We may also use personal information for purposes set out in the terms and conditions that govern our relationship with you.

Usage of Personal Data

We may also collect information that your browser sends whenever you visit our Service or when you access the Service by or through a mobile device ("Usage Data").

This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When you access the Service by or through a mobile device, this Usage Data may include information such as the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browser you use, unique device identifiers and other diagnostic data.

Tracking & Cookies Data

We use cookies and similar tracking technologies to track the activity on our Service and hold certain information.

Cookies are files with small amounts of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyze our Service.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

Examples of Cookies we use:

- **Session Cookies** - We use Session Cookies to operate our Service;
- **Preference Cookies** - We use Preference Cookies to remember your preferences and various settings
- **Security Cookies** - We use Security Cookies for security purposes.

We may share your personal data with third parties for the purposes described below.

We may share information with our service providers: We may use third party service providers to process or handle Personal Data on our behalf. These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

We may share information with your joint account holders, representatives, executors and beneficiaries : We share Personal Data with joint account holders or representatives (such as a legal guardian, power of attorney or attorney at law). Joint account holders will each have access to all of the account history and transaction details for the account. We may also share personal information with your (or your joint account holder's) estate representatives where reasonably necessary to administer the estate.

We may share information to meet legal requirements:

This may be:

1. For the purposes of investigating contravention of law or to detect, suppress or prevent fraud;
2. To establish, exercise or defend legal claims;
3. To protect the rights, property and safety of the Bank and others;
4. To courts, law enforcement and regulatory authorities in the jurisdictions in which we or our service providers operate, including to respond to a local or foreign court order, search warrant or other demand or request which we believe to be valid;
5. To comply with the rules of production of a local or foreign court; and
6. To satisfy legal and regulatory requirements that we believe are applicable to us.

We may share information in accordance with your requests or as you otherwise consent

[How We Protect Your Personal Information](#)

SKNANB maintains safeguards for the purpose of securing your personal data including data encryption and firewalls to maintain the security of the information we receive via our website.

The security of your data is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

[Guarding Your Personal Information/Steps that you can take](#)

While security and privacy risks cannot be eliminated, they can be minimized. SKNANB recommends that you take the following precautions:

Proper Use of Passwords

1. Do not under any circumstances share your passwords with anyone, including family members.
2. Never give your password to a third party such as a payment service provider as this places your financial information at risk.
3. Don't use passwords that are obvious like your name, names of family members, your address, date or birth or any other information that might be found in your purse or wallet.
4. Try to avoid passwords that are real words. Choose passwords that are difficult for others to guess. Such passwords may contain a combination of letters, numbers or symbols.
5. Avoid using the same password for several accounts or services. Try to use unique passwords for different web sites and purposes.
6. Change your passwords frequently.
7. If you suspect that someone knows your password, change it immediately. In the meantime, ensure that your information has not been compromised.

Using a Firewall

Your computer may become vulnerable to hackers if it is not properly protected while connected to the Internet. All cable modems, digital subscriber lines (DSL) and dial-up users may be susceptible to Internet hackers.

A personal firewall will help protect your computer while it is connected to the Internet. A firewall creates a barrier between your computer and the rest of the Internet. A firewall can be a hardware device, a software application or a combination of the two. Firewalls can help prevent hacker attacks and block certain types of data from entering your computer or private network. They can also be set up to alert you if anyone tries to access your system.

Security Updates

Be sure to download and install security updates regularly. Alternatively, you may configure your operating system to check for new updates automatically.

Be Wary of Internet Fraud

The most common of these are *email fraud*, *identity theft*, *phishing* and *pharming*.

E-mail fraud

Exercise caution with e-mails that ask for personal information. Never provide your personal passwords, personal identification numbers (PIN), account numbers or log in information for Online Internet Banking. Please note that SKNANB ***will never send you an e-mail asking you to provide these personal details.***

Most importantly, if you think that you are a target of e-mail fraud, do not reply to the e-mail — delete it immediately **without opening it.**

Transfer of Data

Your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

If you are located outside Saint Kitts and Nevis and choose to provide information to us, please note that we transfer the data, including Personal Data, to Saint Kitts and Nevis and process it there.

Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

The Bank will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

We have implemented measures designed to safeguard the personal information in our custody and control against theft, loss and unauthorized access, use, and disclosure.

We restrict access to personal information to employees and authorized service providers who require access to fulfil their job requirements.

We may keep and use information about you in our records for as long as it is needed for the purposes described above, or to otherwise meet our legal obligations, even if you are no longer a customer.

Links to other sites

Our Service may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Changes to this Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Contact Us

If you have any questions about this Privacy Policy, please contact us:

- By email: customerservice@sknanb.com
- By phone number: (869) 465-2204 Ext 1111

Date 10/15/2019