

SECURITY INFORMATION

At Parallelex Bank Limited, keeping your personal information secure and confidential is a priority. We take appropriate measures to protect the security of your personal information and prevent unauthorized access to same.

Security Tips

- **Use a personal firewall and anti-virus software:** This can prevent unauthorized access and viruses being downloaded onto your PC when you're on the Internet.
- **Pay Attention to your Environment:** Shield and carefully protect your PIN when you are conducting transactions at the Automated Teller Machine (ATM) or when making Point of Sale (POS) transactions at retail stores and agent banking locations.

Only enter credit card and personal information when it involves a transaction you initiated and on Websites you trust.

Always log on to our internet banking service via our website - www.parallexbank.com

Watch out for copycat websites. Don't fall prey to any website that looks similar to Parallelex Bank's website. Check the URL carefully. (<https://www.parallexbank.com>)

- **Check the padlock symbol and site certificate:** Double-click the padlock symbol at the bottom of your browser when you log-in to Parallelex Online Banking to ensure the site certificate belongs to Parallelex Bank Limited. This will ensure you're not being duped into entering your details on a 'fake' site.
- **Always log-out after using Online Banking:** Just select the log-out button and never leave your PC unattended while you're logged in to the service.
- **Keep your personal details secret:** Never write down or reveal your password. Giving away your Internet Banking login, card details, PIN and codes from your token device, gives anyone total access to your account. Parallelex Bank Limited will never ask for any of these details via any form of communication.

Keep your ATM cards safe and do not share your personal identity number (PIN) with anyone. Do not keep any written copy of your PIN with your card. Memorize it.

- **Vishing:** Seeing a phone number or email address you recognize does not mean it is genuine. Always give cold-callers a cold reception

Vishing is a fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce you to reveal personal information, such as bank details and credit card numbers.

- **Be extra wary of emails:** See the scam email section for all the details.

- **Check your accounts regularly:** Check your bank account statements and card transactions regularly to make sure these only reflect transactions you have made. If you see a transaction you cannot explain, report it to the bank.
- **Legitimate Notification:** Subscribe to SMS alerts to be delivered to your cell phone or email, so you can stay updated on your account activity.

Recognizing Fraud

▪ **Scam Emails**

Scam e-mails are “spoofed” emails, and it is the most common avenue of online scams. Email spoofing is a technique that is used to trick you into thinking a message came from a reputable source in order for you to divulge your personal information such as your Bank Verification Number, to carry out fraudulent activities – steal your money.

You may receive emails that look like they come from Parallellex Bank, asking you to disclose your security information.

Please be advised that the Bank will never ask you to disclose your personal or security details by email. If you receive an email asking you to ‘verify your account’, ‘confirm your sign-in details’, or a similarly worded request, it is certainly a scam. These are probably from criminals looking to steal your money.

Usually the links contained in these ‘phishing’ emails will direct you to a fake Internet banking website requiring you to ‘update’ or ‘verify’ your details on the page. Be warned – these can appear to be genuine. Don’t click on these links or provide any of your security details.

If you’re ever in doubt about whether an email is genuine, do not click on its links or open any attachments.

▪ **Phishing Scams**

Phishing is a type of deception designed to obtain and use your personal data for fraudulent purposes. It involves the use of fraudulent email or browser pop-up messages that appear to be from a legitimate source, often using a company name, logo and/or graphic.

A typical phishing scam consists of:

1. An email message stating you need to update or validate your account information.
2. The message suggests a dire consequence, such as your online access expiring or being suspended, if you do not respond.
3. Via a link in the message, it directs you to a Web site that looks legitimate, but is not.

Con artists might send thousands of fraudulent e-mail messages to trick you into divulging personal information, such as your account number, Debit/Credit card numbers, User ID or Password via e-mail or on an illegitimate website created by them so they can commit crimes of a monetary nature or identity theft. It may also be an attempt to deliver and install malicious code (malware) that can harm your computer.

Tips to Protect Yourself from Phishing

1. Never open any email unless you know the sender. The very act of opening an email can infect your computer with malware. Be sceptical of every email you get, and never click on suspicious links, or download suspicious attachments.
2. Contact your bank immediately and delete the e-mail after reporting it.
3. Check to make sure that your virus definitions and anti-spyware are up-to-date and scan the computer, especially if you accidentally clicked on the link or attachment in the e-mail.

▪ **Credit/Debit Card & PIN**

1. Guard your Credit/Debit Card and Personal Identification Number (PIN) like you guard your cash.
2. Never write your PIN anywhere or send it via email.
3. Prevent others from seeing you enter your PIN at the ATM by using your body to shield their view.
4. Do not accept assistance from others at the ATM facility.
5. Promptly notify Paralex Bank if your Credit/Debit Card is lost, stolen or jammed in the machine. Please call any of the following numbers
 - a. 0700 727 25539
 - b. 0912 180 4317
 - c. 0912 192 1226
 - d. 0912 272 2067

Password Security

Customers gain access to their accounts online by supplying their username and password to the internet banking application for verification and authentication. Passwords are the keys to your personal and account information. Therefore, care must be exercised in constructing passwords. The following are some easy steps that you can take to protect yourself from having your personal information compromised.

DO's	DON'T's
Use at least eight (8) characters	Use names and/or dictionary words
Use both letters and numbers	Use personal information
Use special characters (e.g !, @#&\$)	Write it on a sticky note and paste it on your monitor
Use UPPER and lower case	Keep it in a drawer or write it in your dairy
Use combined or misspelled words	Use the same password for several applications
Guard your fingers when typing	Recycle old passwords
Change password periodically	Send via mail or SMS or disclose it to someone else

Customer's Responsibility

You are the first and best layer of defence in combating online fraud. Learning to properly detect and avoid online scams is the ultimate protection against fraud. Read the tips above to help you spot potential scams.

PRIVACY POLICY FOR THE WEBSITE

YOUR PRIVACY, OUR PRIORITY

Parallex Privacy Policy (“**Privacy Policy**”) provides information on the collection, use, sharing and processing of personal information by Parallex when you use Parallex websites, our services, download documents from us, subscribe for our newsletters, interact with Parallex during in-person meetings, at Parallex sponsored events or events hosted at our premises, and in the context of other marketing and branding activities. This Privacy Policy also explains the choices you have in relation to these processing activities.

In this Privacy Policy, ‘personal information’ or ‘personal data’ means information that relates to an identified individual or to an identifiable individual. For example, this could include among other things your name, address, email address, business contact details, or information gathered through your interactions with us via our websites or at events. Personal information is also referred to as ‘information about you.’

WHAT PERSONAL INFORMATION DO WE COLLECT

Parallex uses the personally identifiable information you provide to communicate with you in response to your enquiries, to provide the services you request, and to manage your account. The types of personal information which we may collect, and process are:

1. Name, contact address, email addresses, and telephone numbers
2. Demographic attributes, when tied to personal information that identifies you
3. Employer, corporate contact details, job title
4. Transactional data, including financial details, your photograph
5. Career history, professional background and other Curriculum Vitae (CV) related information
6. International passport, driving license or any other form of proof of identification
7. Data from surveys and publicly available information, such as social media posts
8. Unique IDs such as your mobile device identifier or cookie ID on your browser
9. IP address and information that may be derived from IP address, such as geographic location
10. Information about a device you use, such as browser, device type, operating system

Parallex Bank will only collect information that is necessary for the provision of its service(s) that you have requested.

HOW WE COLLECT PERSONAL INFORMATION

We collect information about you and any other party whose details you provide to us when you:

1. Register to use our websites and portals
2. Complete online forms
3. Take part in surveys
4. Interact with us using our social media platforms
5. Download information such as publications or participate in any other interactive areas that appear on our website or portals
6. Contact us offline, for example by telephone, SMS, email, post or any other means of communication
7. Access and use any of our websites or portals from your devices (including mobile devices) and applications.

8. Share information with third parties that are entitled to share that information, but in each case as permitted by applicable laws.

WHY AND HOW DO WE USE YOUR PERSONAL INFORMATION

All personal information which we collect, and process is justified by lawful processing on the basis that:

1. You have given consent to the processing
2. Processing is necessary for the performance of a contract to which you are a party or take steps to enter a contract
3. Processing is necessary for compliance with a legal obligation to which we are subject
4. Processing is necessary to protect your vital interests or another natural person
5. Processing is necessary for the performance of a task carried out in the public interest

We may use personal information for the following purposes:

1. **To communicate and respond to your requests and enquiries about Parallelex** - If you get in touch with us (such as by completing the registration form on our website, sending an email or by visiting the social media platforms), we process information about you to communicate with you and to respond to your requests or other enquiries. Based upon the personally identifiable information you provide us; we may send you a welcoming email to verify your username and password. Also, in response to your enquiries, Parallelex Bank may communicate with you by email, SMS or telephone.
2. **To administer subscriptions of periodic newsletters**– Parallelex Bank may use a third party to create and distribute various newsletters via e-mail. The third party will collect your name and e-mail address when you click through to their site and sign up for the newsletter. Please review their privacy policy to determine how your information will be used.
3. **To deliver technical and functional management on our sites** - When you choose to register with us (such as to make use of our digital channels), we need to process the personal information provided by you so that we can create and manage a personal account for you. Upon creating your account, we will send you your personal login information. This personal information enables us to administer your account, for example by changing your password for you
4. **To market our services or related services, and to tailor our marketing and brand activities to you or your company's interests** – Parallelex Bank may use information about you to notify you (email or telephone) about new products and services, updates and associated campaigns and promotions (including via newsletters)
5. **To manage the security of our sites, networks and systems**– We may collect site use data for security and operations management to help keep our sites, networks and systems secure, or to investigate and prevent potential fraud, including ad fraud and cyber-attacks and to detect bots
6. **To comply with applicable laws and regulations and to operate our business** - In some cases, we are required to process personal information to comply with applicable laws and regulations. For example, to respond to a request from a regulator or to defend a legal claim. We may also process personal information in the performance and operation of our business, such as to conduct internal audits and investigations or for finance and accounting, archiving and insurance purposes.

7. **To arrange events hosted at our premises** – whether you are either an organiser or an attendee and to control access to our premises.

DATA ANALYTICS

We may use data analytics tools to analyse the information generated and stored during your use of our services to improve our services, provide content tailored to your personal preferences, and to monitor our website's traffic and usage. The other purposes include:

1. Develop and provide new and existing functionality and services.
2. Determine your general location to evaluate how our known clients engage with different parts of our website.

All these tools may be provided by third-party service providers and may include the collection and tracking of certain data and information regarding the characteristics and activities of visitors to our website. We may disclose data, including personal information, to such third-party services providers in order to obtain such services.

You have the right to object to processing based on our legitimate activities but if you object, this may affect our ability to provide certain services and/or solutions for your benefit.

WHO WE SHARE YOUR PERSONAL DATA WITH

Your personal data may be stored in a database that we can access in order to provide you with our services. We may also share your data with third parties (data controllers) who provide data storage facilities to us. The other categories of third parties, in accordance with this Privacy Policy, we may share your information with are:

1. Service providers (for example, IT services) or third parties which process information on our behalf (e.g., internet service and platform providers, payment processing providers and those organisations we engage to help us send communications to you) so that they may help us to provide you with the applications, services and information you have requested or which we believe is of interest to you.
2. Analytics and search engine providers that assist us in the improvement and optimisation of our website.
3. Law enforcement or regulatory agencies, or authorised third parties, in response to a verified request relating to a criminal investigation or alleged illegal activity or any other activity that may expose us and/or the user or any third party to legal risks or liability.
4. Third parties where you have a relationship with that third party, and you have consented to us sending information (for example social media sites or other third-party application providers)
5. National Information Technology Development Agency (NITDA) professional advisors and auditors for the purpose of seeking professional advice or to meet our audit responsibilities
6. Agencies where reporting is mandatory under applicable laws

We may share non-personally identifiable information (e.g. the pages you visit, and which links you click, which ads you see and click on, and the categories of search terms you enter) about the use of our website or portal publicly or with third parties but this will not include information that can be used to identify you.

WHAT ARE YOUR RIGHTS

In accordance with the Regulation, you may have the following rights in respect of your personal information:

1. **Right to access and/or have your information provided to you** – You have the right to obtain a copy of your personal information and be told how we use your information.
2. **Right to rectify, erase or place restrictions on processing of your information** – You have the right to rectify inaccurate personal information (including the right to have incomplete personal information completed), erase your personal information (in limited circumstances, where it is no longer necessary in relation to the purposes for which it was collected or processed), restrict processing of your personal information (e.g. where the processing is based on our legitimate interests)
3. **Right to transfer your information to another organisation** - You have the right to have any information you provided to us on an automated basis returned to you in a structured, commonly used and machine-readable format, or sent directly to another organisation, where technically feasible
4. **Opt-out of our use of your personal information** - You may withdraw consent you have previously provided for the processing of information about you subject to legal or contractual restrictions.
5. **Opt-out of our processing of your personal information** – You have the right to object to any decisions based on the automated processing of your personal data, including profiling.
6. **Right to lodge a complaint** - You have the right to lodge a complaint with the supervisory authority responsible for data protection matters. In Nigeria, NITDA is the authority responsible for data protection

INFORMATION RETENTION

We maintain personal information not longer than we need to use it in accordance with this Privacy Policy. In some circumstances, we may retain your personal information for longer periods if it is in accordance with regulatory, legal, tax or accounting obligations. The Bank has an established retention procedure it applies to records and information collected and stored. In all cases, where your information is no longer required or you request for deletion, we will ensure it is disposed of in a secure manner.

HOW IS YOUR PERSONAL INFORMATION SECURED?

The security of your personal information is important to us. Parallax Bank therefore takes reasonable precautions to protect your personal information. We generally follow accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it. No method of transmission over the Internet, or method of electronic storage, is 100% secure. However, we have implemented appropriate technical, physical and organisational measures designed to protect personal information against accidental or unlawful destruction, accidental loss, damage, alteration, unauthorised disclosure or access, as well as all other forms of unlawful processing.

WHAT COOKIES AND SIMILAR TECHNOLOGIES DO WE USE ON OUR SITES?

The Privacy Policy covers the use of cookies on the website and does not cover the use of cookies by advertisers. Parallax Bank's third-party partners who provide certain features on the website or display advertising based upon your web browsing activity may use flash cookies to collect and store information. To provide users with the most relevant website content, Parallax may also use embedded pixel technologies to help track site usage. These technologies are used on selected pages for the purposes of identifying unique user visits as opposed to aggregate hits. The site usage information collected by these technologies is associated with cookies and may provide data about site use by registered users of the website. This information is used to evaluate site content, navigability, and composition, as well as page response rates. Any data linking the information gathered by clear gifs (tiny graphics with a unique identifier, similar in function to cookies) to a user's personally identifiable information is used for internal tracking purposes only. Parallax Bank will not disclose or divulge such data linkages outside of Bank. When to use cookies, how you can manage your cookies and details about your consent are provided below.

HOW CAN I MANAGE MY COOKIE PREFERENCES?

By continuing to use our website, you are agreeing that we may place cookies on your computer to analyse the way you use our website. If you are a visitor to our sites, you can use our cookie preferences tool to opt out of cookies.

However, if you do not wish to accept cookies in connection with your use of this website, you must stop using our sites or use your browser settings to block the placing of cookies. If you wish to withdraw your consent at any time, you will need to delete your cookies using your internet browser settings. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies as soon as you visit our site. If you do not wish to receive cookies, you can block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies.

DISPUTE RESOLUTION OR FILING A COMPLAINT

If you have any complaints regarding our compliance with this Privacy Policy, please contact us on 0700 727 25539 OR 0912 180 4317. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information within thirty (30) days in accordance with this Privacy Policy and in accordance with applicable law and regulation.