Customer Service: 1-844-966-5622

Online Privacy, Security & Information Gathering Policy

Last Reviewed: January 08, 2025

This outlines the policies relating to privacy, security and information gathering put in place by ZYNLO, a division of PeoplesBank, Holyoke, MA member of the Federal Deposit Insurance Corporation ("FDIC") ("ZYNLO", the "Bank" or "Issuer") on behalf of NYMBUS Inc. ("NYMBUS"), the program partner responsible for managing ZYNLO accounts. "We", "our", and "us" refer to NYMBUS and/or the Bank, our successors, affiliates, or assignees. "You" and "your" refer to the user of the services provided by Bank and NYMBUS.

Privacy

Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

VIEW FULL PRIVACY NOTICE - https://zynlobank.com/file/privacyPolicy

Children's Online Privacy

We do not knowingly collect, use, or maintain any information through our websites from or about children who are under the age of 13 years. If we determine that a child under the age of 13 has provided us with information through one of our websites, we will use this information only to notify his or her parents that the information was received.

NYMBUS and ZYNLO are committed to safeguarding your confidential information and maintaining the security of our online products and services. In addition to this statement, please view our full Privacy Notice, that addresses our general policies for collecting and sharing customer information.

Security

We maintain appropriate physical, electronic and procedural safeguards to protect the security, integrity and privacy of your personal information. Information you submit through the ZYNLO website is encrypted to industry standards. No confidential or personal information should be sent through regular email since those email transmissions may not be secure.

We continually review our security safeguards in order to protect customer information that we gather, transmit and store in connection with our online products and services.

Passwords and Mobile Security

We recommend you safeguard your identity and personal information by using effective password protection and access our services using only secure devices. Without limiting any other provisions herein, you agree that we have no liability or obligation related to (i) your creation of any user ids or passwords used to access our services; or (ii) your use of any mobile or other devices to access our services. Use of third-party devices is solely at your own risk. Please refer to the section, Security - Protect yourself from scams.

Security - Protect yourself from scams

Scammers use several different methods to try and lure you into giving them the personal financial information they require, to commit fraud and theft. These methods include seemingly "official" email messages, phone calls, and even text messages from your banking institutions, stating problems with your account in various ways, to create a sense of legitimacy and urgency for action.

Phishing: the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication, which is typically email.

Vishing: the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward.

Smishing: a form of criminal activity using social engineering techniques similar to phishing. The name is derived from "SMs phISHING". SMS (Short Message Service) is the technology used for text messages on cell phones.

ZYNLO will never ask for any sensitive information from their customers in these ways, and we urge you to be suspicious of any e-mail, text message, or caller, asking you to "verify account information." If you ever have any doubts as to the validity of these communications, please keep the following points in mind:

- Never give out your personal financial information in response to an unsolicited phone call, text, fax or email, no matter how official it may seem.
- Do not respond to email that may warn of dire consequences unless you validate your information immediately. Contact ZYNLO to confirm the email's validity using a telephone number or Web address you know to be genuine.
- Check your bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies to ZYNLO immediately.
- When submitting financial information online, look for the padlock or key icon at the bottom of your Internet browser. Also, many secure Internet addresses, though not all, use "https" to signify that your information is secure during transmission.
- Report suspicious activity to the Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center.
- If you have responded to a fraud message contact ZYNLO immediately so we can protect your account and your identity.

Information Gathering

We obtain information about our clients and website users online when you provide your information to us directly to complete online forms or obtain online services or indirectly as part of the information we collect on our websites. One example of information we collect indirectly is information collected through our internet access logs. When you access our website, your internet address is automatically collected and is placed in our internet access logs. We may also record the URLs of the websites and pages you visit before, during and after your visit to our website, the times and dates of these visits, information about the computer hardware and software you use, and other information that may be available.

We may collect information directly from you in a number of ways, including through the use of cookies. Cookies are small files of information which save and retrieve information about your visit to the website such as how you entered our website, how you navigated through the website, and what information you viewed. The cookies we use identify you merely as a number. We use cookies to record information on customers' visits and use of our websites in order to administer and improve our websites. We do not use cookies to store or transmit any personally identifiable information.

Temporary "session" cookies are also used to facilitate customer navigation within our website. Session cookies are deleted once you close your internet browser. We may also use "persistent" cookies that are retained on your computer after your visit ends so we can identity your preferences and enhance your next visit to our website.

In addition, cookies help us manage and monitor internet traffic from third-party websites to ours and identify which areas of our website are used most often and for how long. We may provide this type of aggregate information to non-affiliated application service providers that compile statistical or other information for us. This feedback and analysis allows us to continually update our website.

We also collect information directly when you voluntarily submit it to us. In addition to our cookies, we may use cookies from advertising partners, transparent GIFs or web beacons to help us gather information about the effectiveness of our advertising. We do not gather personally identifiable information from this use and it does not affect our protection of your information.

You can block cookies by changing the settings on your internet browser or through the use of software programs specifically designed to block cookies. You should be aware that blocking cookies or using certain security software settings may prevent you from logging onto your accounts or limit your online activities. If you employ "do not track" signals while visiting our website, we will not collect information about your visit, nor will any third-party included on our site.

Changes to this Policy

This Online Privacy, Security & Information Gathering Policy is subject to change. Please review it periodically. If changes are made, the effective date at the top of this Policy will be revised. Any changes to this Policy will become effective when posted unless indicated otherwise.