



CUSTOMER INFORMATION SECURITY

Your account information is important to us. **HARFORD BANK will never call, text, or email you requesting personal information** such as your online banking password, debit card PIN number, card expiration date or CVV code on your card(s).

Please protect your information:

1. **NEVER** answer questions from any unsolicited phone call, text or email requesting information, even if it looks or sounds legitimate. Criminals are adept at making text and emails look official and spoofing caller ID, so the caller appears authentic.
2. **NEVER** give out your online banking log-in credentials, card information or other personal information to people contacting you unexpectedly.
3. HARFORD BANK will not contact you to change your PIN.

If you voluntarily provide your sensitive information to anyone who is not an authorized card user on your account, **you may be responsible for the transactions and you may not get your money back.** Call HARFORD BANK at 410-272-5000 if you suspect that someone tried to obtain information about your HARFORD BANK accounts or cards.

TOOLS TO HELP PROTECT YOU FROM IDENTITY THEFT

Alerts

Alerts are an email or text alert feature available through Online Banking. Sign up to receive alerts when you have a low balance, an overdrawn account, and more. This is a great tool to monitor the activity in your accounts and detect unauthorized transactions.

Secure Email

HARFORD BANK will never ask you to send confidential information to us by unsecured email.

You should refrain from sending any confidential or personal information, such as your user ID, password, account number, or Social Security Number by unsecured email to HARFORD BANK.

If you are requested to send confidential information to HARFORD BANK, you will be asked to use the HARFORD BANK Online Banking Message Center or you may request to have a secure email sent to you, to which you can respond with the information requested. Alternatively, you may request a fax number or visit one of our branches.

FRAUD AND IDENTITY THEFT

If you have been a victim of fraud or identity theft, reference the information below for helpful tips and resources to report fraud, rebuild your finances and protect your accounts and personal information from future threats.

- **Contact your local law enforcement agency** to file a police report. Be sure to request a copy of the report to show proof of the crime, if needed.
- **Contact the three credit reporting agencies** to place a fraud alert and/or credit freeze; obtain/review a copy of your credit report(s):
 - Equifax 888-378-4329 equifax.com
 - Experian 888-397-3742 experian.com
 - TransUnion 833-395-6938 transunion.com
- **Contact ChexSystems** to place a security alert on your consumer file.
 - Call Consumer Relations at 800-887-7652 or visit www.chexsystems.com.
- **Notify Social Security Administration** if your Social Security number was compromised.
 - Call the SSA Fraud Hotline at 800-269-0271.
- **Notify your local Motor Vehicle Administration (MVA)** if your driver's license has been lost or stolen.
- **Contact the Federal Trade Commission (FTC)** to file an identity theft complaint.
 - Call the ID Theft Hotline at 877-438-4338 or visit <https://www.identitytheft.gov/#/>.
- **Get a free annual credit report** from the three major credit reporting agencies and continued monitoring of your credit reports by visiting www.AnnualCreditReport.com.