EAGLE BANK

FRAUD PREVENTION CHECKLIST

How to prevent your financial information from being stolen

- [ ] Store your sensitive documents in a secure location or safe.
- [ ] Never provide passwords, PIN numbers, account numbers, etc., over the phone or via text or email.
- [ ] Never send PINs (personal identification numbers), credit card numbers, passwords, or personal/financial information in a text or email.
- [ ] Sign up for additional safeguards to protect your accounts.
- [ ] Enroll in push notifications for mobile banking transactions.
- [ ] Keep your contact information up to date.
- [ ] Always create difficult-to-guess PIN numbers.
- [ ] Protect your PIN.
- [ ] Be aware of your surroundings when using your cards at the gas station pump or outside ATMs.
- [ ] Utilize an encrypted digital wallet from a secure provider.
- [ ] Go paperless.
- [ ] Shred all documents with PII (personally identifying information) and financial data.
- [ ] Clip or shred old, expired cards.
- [ ] Collect your mail daily and set up mail forwarding/holding when you're away.

How to protect yourself on social media

- [ ] Limit the amount of information you share online. For instance, travel plans.
- [ ] Set your social profile settings to private.
- [ ] Monitor your child's social media accounts and ensure they're private.

How to Avoid Phishing, Smishing, and Vishing Scams

- [ ] Don't open or respond to unsolicited emails or texts from unknown contacts.
- [ ] Never sign into an account using a link in an email or text.
- [ ] Be wary of links and attachments in emails, sponsored content pop-ups, and texts.
- [ ] Become familiar with the short codes used by your financial institutions.
- [ ] Use different emails and usernames/passwords for each financial account.

How To Secure Your Online Data and Mobile Devices

- [ ] Only browse secure online websites.
- [ ] Enable location services and location-based security permissions.
- [ ] Consider upgrading to a VPN (virtual private network).
- [ ] Lock your devices with a passcode, and use biometrics.

- [ ] Don't alter, "jailbreak," or remove carrier restrictions from your devices.
- [ ] Don't store passwords or sensitive PII on your devices.
- [ ] Only download apps and programs from trusted sources.
- [ ] Always perform recommended updates on your devices.
- [ ] Completely "wipe" or clear your devices and perform a factory reset before selling, trading, or discarding them.
- [ ] Never use public or shared WiFi at coffee shops, airports, libraries, etc.
- [ ] Don't pair your device with other public devices (rental cars, hotel rooms, etc.).
- [ ] Always secure your home router with a strong password and WPA2 – or better, WPA – security.
- [ ] Carefully research cloud data providers.

Become a Secure Password Professional

- [ ] Use hard-to-guess passwords.
- [ ] Never use your pet's name, family/friends' names, birthdates, addresses, or other PII.
- [ ] Don't recycle or reuse passwords.
- [ ] Regularly change your passwords.
- [ ] Never share passwords via text, email, or direct messages on social media.
- [ ] Always activate Two-Factor Authentication (2FA).
- [ ] Migrate to a secure password manager, Dashlane for example.