

You may obtain a free credit report from the Federal Trade Commission (FTC) by calling 1.877.322.8228, or log onto www.annualcreditreport.com and complete a Request Form.

You may also get a Request Form by writing to:
Annual Credit Report Request Service
P.O. Box 105281, Atlanta, GA 30348-5281.

EQUIFAX — www.equifax.com

To report fraud, call: **1.800.685.1111** and write:
P.O. Box 740241, Atlanta, GA 30374-0241

Hearing impaired call **1.800.255.0056** and ask the operator to call the Auto Disclosure Line at **1.800.685.1111** to request a copy of your report.

EXPERIAN — www.experian.com

To report fraud, call: **1.888.EXPERIAN** (1.888.397.3742) and write: P.O. Box 9530, Allen, TX 75013

TDD: **1.800.972.0322**

INNOVIS

To report fraud, call: **1.800.540.2505** and write:
P.O. Box 1373, Columbus, OH 43216-1373

TRANS UNION — www.transunion.com

To report fraud, call: **1.800.916.8800** and write:
Fraud Victim Assistance Division, P.O. Box 6790,
Fullerton, CA 92634

TDD: **1.877.553.7803**

To file a complaint or to get free information on other consumer issues, visit www.ftc.gov or call toll-free 1.877.FTC.HELP (1.877.382.4357).

Here are additional agencies that should be notified in cases of fraud.

- **Local Police Department**
- **U.S. Postal Inspection Service**
See federal government phone list or visit www.usps.gov/postalinspectors
- **U.S. Postal Service:** Local post office
- **Social Security Administration**
- **Fraud Hotline:** 1.800.269.0271

Fraud & Identity Theft

What to do if it happens to you.

Service Unlike Any Other



Greenville Center
302.421.5800
Wilmington Office
302.888.7400
www.christianabank.com





FRAUD ALERT

Scams — We hear about them all the time

- Be suspect of any cashier's check that just shows up in the mail with a "congratulations" letter, or to pay for purchases if it is from someone you don't know.
- Understand that when cashing a personal check, money order, or cashier's check, even though the bank has provided you with the money, you are responsible for the funds until your bank has received the proceeds from the institution which originally issued the check.
- If you do not know the person who issued the check, hold the funds for 30 – 45 days before using them.
- If you believe you are a victim of this type of scam, contact your local or state police.
- If monies have been deposited or withdrawn from a Christiana Bank account in response to any of the above situations, please call us at 302.421.5800.

For more information, visit christianabank.com and click on Consumer Alerts and Education.

CREDIT CARD ALERT

One of the latest credit card phone scams is the caller identifies themselves to be from the Security and Fraud Department of Visa® or MasterCard®, gives you their ID and a toll-free number. They state your account has been flagged because of unusual activity and asks you to verify that you have possession of your card by reading the three-digit security number off the back. That number is what the scammer wants, they already have your account number, and need the other number to make internet purchases. **HANG UP, DO NOT give out your 3-digit security number. File a police report.**

PHISHING SCAMS

Pronounced "fishing" is a term coined by computer hackers, who use email to fish the Internet hoping to hook you into giving them your usernames, passwords and/or credit card information. To check it out, do not use the information provided to you over the phone or in an email. Key in the company's Web address or look up their number in the phone book to confirm the information. Always report phishing by forwarding the email or documenting the phone call to:

- The anti-phishing network at www.antiphishing.com
- The Federal Trade Commission at www.consumer.gov/idtheft
- The Internet Fraud Complaint Center of the FBI at www.ifccfbi.gov

INTERNET SHOPPING

Use caution when purchasing items through the Internet from individuals or companies that you do not know. It is best to register with a secure site to transfer funds to the seller rather than give out your personal information. It is recommended that you shop online using credit cards, however, all Christiana Bank CheckCards (debit cards) are equipped with Verified by Visa. Just logon to christianabank.com for a link to register your card with your personal PIN and to learn more about how this provides extra protection when using your check card for online purchases.

IDENTITY THEFT IS A SERIOUS CRIME

If you suspect that your personal information has been stolen to commit fraud or theft, take action immediately.

In addition, make sure you...

- Follow up all calls in writing.
- Send your letter by certified mail, return receipt requested, so you can document what the company received and when.
- Keep copies for your files.
- Safeguard your Social Security number; never carry it in your wallet, and give it out only when absolutely necessary.
- Be careful about giving out personal information; make sure the person has a legitimate need to know. Your bank will not ask you for this information over the phone.
- Use different passwords for your accounts, and make sure they are hard to guess.
- Shred documents containing account or personal information, including unsolicited pre-approved credit offers and blank "courtesy" checks — don't throw them in the trash.

- Review your monthly statements promptly and carefully to make sure they are accurate.
- Avoid carrying your checkbook or your Social Security card.
- Guard your mail. Deposit outgoing mail at the post office rather than in your mailbox and promptly remove mail from your mailbox.

If you are a victim...

- Act fast — brace yourself. Contact the fraud department of any one of the four major credit bureaus (listed in this brochure) to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all four credit reports will be sent to you free of charge.
- Close your credit card accounts and change the passwords on all your financial accounts.
- File a police report. Credit bureaus won't extend a fraud alert without it.
- Call every creditor that has a bogus account listed in your file and have them close it immediately. Demand copies of all fraudulent applications for credit and billing statements. Creditors don't want to divulge that information — but they will if you request it in writing and enclose a copy of a police report.

REMEMBER

Stolen wallets and checkbooks remain the most frequent sources of ID theft.

Christiana Bank & Trust wants to help you safeguard your identity. If someone, including a person posing as a banker, attempts to obtain personal information from you, use caution.