

[MEMBER BANK LOGO]

IMPORTANT INFORMATION

Regarding your [ISSUER NAME]
Visa® Check Card ending in: XXXX

Sample A. Sample
123 Any Street
Any Town, SS 12345-6789

You will soon receive a new [ISSUER NAME] Visa Check Card.
It replaces your current [ISSUER NAME] Check Card.

Dear Sample A. Sample,

To protect you and your money, [MEMBER BANK] is constantly monitoring accounts for fraudulent activity. During a recent security review, we identified your Visa check card number as being at risk for unauthorized charges.

Your account security is a top priority for us, so we are taking the proactive step of issuing you a new [ISSUER NAME] Visa check card.

Your new [ISSUER NAME] Visa check card should arrive in the mail in the next 7-10 business days. As soon as you receive it, activate it immediately, then destroy your current card.

Your current card will be deactivated on Month XX, 200X. You may continue to use it until the new one arrives, or you can call 1-8XX-XXX-XXXX to cancel it now.

In the meantime, you can take steps to protect yourself even further by reviewing your monthly checking account statements and monitoring your account online at [www.MemberBank.com]

If you notice anything suspicious, please notify us as soon as possible. You won't have to worry about paying for unauthorized charges because your card is backed by Visa's Zero Liability protection.[†] Just notify us immediately and we'll put money in your account within five business days to cover any funds lost due to fraudulent purchases.

[MEMBER BANK] takes your account security and privacy very seriously, and we apologize for any inconvenience this may cause you. **If you have any questions or concerns, please call us at 1-8XX-XXX-XXXX or visit our website at [www.MemberBank.com]**

Sincerely,

[Member Bank Signer]
[Member Bank Signer Title]

P.S. See the back of this letter for more steps you can take to protect your account.

[†] Covers U.S.-issued cards only. Visa's Zero Liability policy does not apply to ATM transactions or PIN transactions not processed by Visa and certain commercial card transactions. Cardholder must notify issuer promptly of any unauthorized use. *Consult issuer for additional details or visit www.visa.com/security*

You can help protect yourself from fraud.

[MEMBER BANK] and Visa[®] are working closely together to catch any fraudulent behavior and protect your account. There are also some simple things you can do. And remember, your Visa check card is backed by Visa's Zero Liability policy, so even if your card or its number is ever lost or stolen, you won't be responsible for unauthorized charges.

Protect your Personal Identification Number (PIN):

- Never write down your PIN. Memorize it as soon as you get it.
- Do not disclose your PIN to anyone. No one from any financial institution, the police or a merchant should ever ask for your PIN.
- Beware of phishing emails. These are emails that appear to be from your bank or online merchant asking for account information. Do not reply to them or click on any links. Visa, your bank or any other legitimate online merchant will never ask for your PIN or other personal financial information via email.
- At an ATM or PIN pad, enter your PIN discreetly, shielding the keypad with your hand or body.

Follow these steps to spot suspicious activity and protect your account:

1. Review your monthly checking account statements to spot any unauthorized purchases. You can also monitor your account activity online at any time at [www.MemberBank.com]
2. Review your credit reports for accuracy. Call any one of the three credit reporting agencies to receive your free annual credit report.

Equifax[®]
800-525-6285
www.equifax.com

Experian[®]
888-397-3742
www.experian.com

TransUnion[®]
800-680-7289
www.transunion.com

3. If you spot any unauthorized charges, please contact us immediately at 1-8XX-XXX-XXXX.
4. You should also contact the three credit reporting agencies listed above to notify them of any suspected fraud or identity theft.