KEMBA DELTA FEDERAL CREDIT UNION

HOW TO PROTECT YOURSELF, AND YOUR GOOD NAME

Protecting your personal information in perilous times

By Blair Ball

Preventative Steps to Take:

- Do not give out personal information, such as account numbers, debit card numbers or credit card numbers on the phone or over the Internet unless you have initiated the contact.
- Report lost or stolen checks/check, debit cards or credit cards immediately. Examine new checks to be sure none were stolen during shipment and store them in a safe and secure location. Sign all new credit cards immediately and save all credit card receipts and match them against your monthly statements.
- Destroy unused financial paperwork (statements, mailings, marketing) before discarding them. Use a shredder.
- Guard your PIN numbers and treat your receipts with care.
- Make sure your mailbox is secure and promptly remove mail when it has been delivered.
- Review your credit reports at least annually to make sure you have not been a victim.

CREDIT BUREAUS

Equifax:	www.equifax.com	1-800-685-1111
Experian:	www.experian.com	1-888-EXPERIAN (397-3742)
TransUnion:	www.transunion.com	1-800-916-8800

If someone has stolen your identity follow these steps:

1) Contact Kemba Delta FCU to protect your credit union accounts.
If your Kemba Delta FCU Visa credit card or debit card is lost or stolen, call 901-795-9055 or toll free 1-800-725.2622.

2) Contact the fraud department of one of the three major credit bureaus listed above. Tell them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name. At the same time, ask for a copy of your credit reports; credit bureaus must give you a free copy if it is inaccurate due to fraud.

3) Contact the creditors for any accounts that have been tampered with or opened fraudulently. Ask to speak to someone in the security or fraud department, and then be sure to follow up in writing. Credit Services Fraud Assistance Center: 1-800-272-9281

4) File a report with your local police or the police in the community where the identity theft took place. Keep a copy in case your creditors need proof of the crime.

5) Contact the Social Security Fraud Hotline: 1-800-269-0271

6) Contact the FTC Identity Theft Hotline: 1-877-IDTHEFT (438-4338)

7) If the crime involved U.S. Mail, contact the U.S. Postal Inspection Service,
(See federal government phone list or visit the website at www.usps.gov/postalinspectors)

Special Alert - Protect Yourself from "Phishing" Scams

Recently, many Americans have received a series of fraudulent e-mails, which direct recipients to websites where they are asked to verify sensitive personal information. The e-mails claim that the individual's personal information is necessary to assist in the fight against terrorism or for some other purpose supposedly required by law. These e-mails are purportedly sent from several government agencies or include content related to government agencies including the Federal Deposit Insurance Corporation.

The fraudulent e-mails are part of a scam known as phishing. Phishing is the fraudulent scheme of sending an e-mail to a user falsely claiming to be a legitimate company. The email attempts to con you into surrendering private information that could later be used for identity theft. The e-mail directs the user to visit a website where they are asked to update personal information, such as name, account and credit card numbers, passwords, social security numbers and other information. The website, however, is bogus and set up only to steal the user's information.

You can protect yourself from this latest identity theft scam by following these useful tips, which were developed by the Federal Trade Commission:

- If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm you're billing information, do not reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or website address you know to be genuine.
- Avoid emailing personal and financial information. Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company, credit union or bank to confirm your billing address and account balances.
- Report suspicious activity to the FTC. Send the actual spam to uce@ftc.gov.If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site www.ftc.gov/idtheft to learn how to minimize your risk of damage from identity theft.

Links to more Information on ID Theft:

Federal Trade Commission: www.consumer.gov/idtheft/
Secret Service: www.secretservice.gov
Federal Deposit Insurance Corporation: www.fdic.gov/consumers
General Information: http://computer.howstuffworks.com/identity-theft.htm