IDENTITY THEFT: What should you do?

To avoid identity fraud, the FBI recommends that you:
♦ Never throw away ATM receipts, credit statements, credit cards or bank statements in a usable form.
♦ Report unauthorized financial transactions to your bank, credit card company and the police as soon as you detect them.
♦ Review a copy of your credit report at least once each year.
♦ Notify the credit bureau in writing of any questionable entries and follow through until they are explained or removed.

For more tips, visit this FBI site:
http://www.fbi.gov/majcases/fraud/fraudschemes.htm#imperson

For more information about identity theft, visit these websites:
- Equifax: www.equifax.com
- Experian: www.experian.com
- Trans Union: www.transunion.com
- Free credit report: annualcreditreport.com
  (or call 1-877-322-8228)
- FTC’s Do Not Call Registry: www.donotcall.gov
- US Dept. of Justice: www.usdoj.gov/criminal/npftf
- Federal Trade Commission: www.ftc.gov/bcp/edu/microsites/idtheft
- FTC and other federal agencies’ new site: onguardonline.gov
- Identity Theft Resource Center: www.idtheftcenter.org
- Privacy Rights Clearinghouse: www.privacyrights.org
- Office of the Attorney General: www.myfloridalegal.com/identitytheft
- FL Dept. of Agriculture and Consumer Services: 800helpfla.com/identity.html

In the event of an exposure of confidential data, an organization and its employees may be held liable.

Due diligence must be exhibited in protecting data and preserving data security.

For the accompanying PowerPoint presentation, please refer to our website:
http://www.chipola.edu/datacenter/FAQ/index.htm
The hyperlinks within the presentation are operational, so you may visit the websites referenced.

Produced and distributed by:
CHIPOLA COLLEGE INFORMATION SYSTEMS DEPARTMENT
May, 2007
Identity theft is currently the number one consumer complaint to the FTC.

Since January of 2005, more than 100 million records containing sensitive information have been exposed.

Almost half of those security breaches were caused by employees either accidentally or maliciously placing confidential data at risk. (See http://www.idtheftcenter.org.)

Security experts are pushing federal and state legislators for stricter controls. A few states have already passed “identity theft” laws, and there are several pieces of federal legislation being considered.

Until there are stronger and more enforceable laws that are designed to protect you and your confidential data, you will have to rely upon yourself and a few tips from the experts.

PHISHERS and PHARMERS trick you through spoofed e-mails (e-mails that have forged sender addresses or headers) and redirected websites that request your account number, password and other info. These scammers can then gain access to your accounts and financial information.

SKIMMING refers to the process of quickly and temporarily stealing a credit card and running it through a skimmer. A skimmer is a credit card reader that has been re-programmed to steal information off of a card.

PRETEXTING is the illegal act of acquiring a consumer’s personal information under false pretenses. Some methods to acquire this information include phone surveys, electronic sweepstakes, the “Free Credit Report” scam and other e-mail scams, like the “Nigerian” money transfer scam.