Summer 2005
Volume 3

HOB NEWS ALERT

At Heritage Oaks Bank, we are dedicated to protecting you and your financial future- this includes protection against FRAUD. Because awareness is the best protection, we have issued this HOB News Alert to update you on a variety of current scams.

Skimming

Most cases of counterfeit fraud involve skimming, a process where the genuine data on a card's magnetic stripe is electronically copied onto another card, without the legitimate cardholder's knowledge.

Skimming normally occurs at retail outlets - particularly bars, restaurants and petrol stations - where a corrupt employee skims a customer's card with a small, hand-held electronic device before handing the card back, then sells the information on higher up the criminal ladder where counterfeit cards are made. Criminals then go shopping with a copy of your credit or debit card with cardholders unaware of the fraud until a statement arrives showing purchases they did not make.

Skimming can also occur at ATMs where the damage can be much greater because of the number of accounts and the amount of money that can be quickly accessed.

Two types of skimming devices can be attached to ATM machines: ones that interfere with the ATM operation and ones that do not. The skimmers that interfere with the ATM operation are a bit easier to detect because even though customers insert or swipe their cards, it's not the ATM's card reader so the ATM isn't actually being used and the customer isn't getting any money.
In other skimming cases, the thieves don't interfere with the normal operation of the ATM. The skimmer is placed over the card reader but doesn't block off the reader, and the customer gets money when making a withdrawal.

Don't be a victim!

1.) Guard your cards—treat them the same way you would treat cash.
2.) Keep your PIN safe. Don't give it to anyone.
3.) Watch out for people who try to "help" you at an ATM.
4.) Look at the ATM before using it. If it doesn't look right, don't use it.
5.) If an ATM has any unusual signage, don't use it. NO bank would hang a sign that says, "Swipe your ATM card before inserting it in the card reader" or something to that effect.
6.) If your card is not returned after the transaction or after pressing cancel, immediately contact the institution who issued it.
7.) Check your receipts against your statements carefully. If you find an unfamiliar transaction, contact your bank immediately.
8.) Report suspected fraudulent use of your card account to your bank immediately.
9.) If you discover that your card has been skimmed (or has been lost or stolen) you should inform your bank immediately.

Putting an end to skimming

The Electronic Funds Transfer Association is spearheading a task force to tackle the problem of skimming. It has brought together all segments of the ATM industry to work on solutions. One such solution is Jitter, which varies the speed and reverses the direction of the card intermittently and in a random fashion when a card is entered, making it impossible for the skimming device to read it.

Heritage Oaks Bank will NEVER randomly contact you to request your Social Security number, bank account number, or any other personal financial information.

If you feel you have been the victim of fraud, please contact any bank Financial Service Representative for assistance. You can also contact the Federal Trade Commission to file a complaint or get free information on consumer issues at 1-877-FTC-HELP or www.ftc.gov.

HOB NEWS ALERT *continued*

At Heritage Oaks Bank, we are dedicated to protecting you and your financial future- this includes protection against FRAUD. Because awareness is the best protection, we have issued this HOB News Alert to update you on a variety of current scams.

Visa and MasterCard Scam

A recent scam to be on the watch for...

You may get a telephone call from 'VISA' or from 'MasterCard'. It works like this: The person calling says, 'this is (any name) and I'm calling from the Security and Fraud Department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. Did you purchase (any expensive item), for $497.99 from a marketing company based in (any town)? When you say 'No'. The caller continues with, 'Then we will be issuing a credit to your Account. This is a company we have been watching and the charges range from $297 To $497, just under the $500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (they give you your address), is that correct?' You say, 'Yes'. The caller continues. 'I will be starting a fraud investigation. If you have any questions, you should call the 800 number listed on your card and ask for Security. You will need to refer to this Control number. They then give you a 6-digit number. 'Do you need me to read it again?'

The caller then says he 'needs to verify you are in possession of your card' (this is where the scam takes place as up until now they have requested nothing!). They then ask you to turn your card over. There are 7 numbers; the first 4 are 1234 (or whatever, as they have your number anyway). The next 3 are the security numbers that verify that you are in possession of the card' (these are the numbers they are really after as these are the numbers you use to make internet purchases to prove you have the card). 'Read me the 3 numbers.' When you do he says 'That is correct. I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions? Don't hesitate to call back if you do.' You actually say very little, and they never ask for or tell you the Card number. What the scam wants is the 3-digit number and that once the charge goes through, they keep charging every few days. By the time you get your statement, you think the credit is coming, and then it's harder to actually file a fraud report.

NO bank or credit card issuer will ever ask for any information about your account since they already know everything about it!!!

If this happens to you...

If this happens to you, just hang up, file a police report and notify your credit card issuer immediately.

Heritage Oaks Bank will NEVER randomly contact you to request your Social Security number, bank account number, or any other personal financial information.

If you feel you have been the victim of fraud, please contact any bank Financial Service Representative for assistance. You can also contact the Federal Trade Commission to file a complaint or get free information on consumer issues at 1-877-FTC-HELP or www.ftc.gov.

The tips above were taken from www.bankrate.com/brm/news/atm/20021004a.asp