City of Bowie
Police Department
15901 Excalibur Road
Bowie, MD 20716

John K. Nesky
Chief of Police

CREDIT CARD FRAUD PREVENTION AND MONITORING

Review all bank and credit card statements each month, preferably daily or at least once a week. Watch for charges for less than a dollar or two from unfamiliar companies or individuals. Thieves who are planning to purchase a block of stolen credit card numbers often first test to check that the accounts haven't been canceled by aware customers by sending a small charge through, sometimes for only a few pennies. If the first charge succeeds, they'll buy the stolen data and make a much larger charge or purchase. They're guessing -- often correctly -- that most cardholders won't notice such a tiny charge. In addition, many of the fraud alerts you can set on your accounts aren't triggered by small dollar amounts.

Public wireless networks should not be used to access bank accounts or credit card information. Public wireless networks should not be used to access bank accounts or credit card information. Do not log into accounts and do not conduct sensitive transactions, such as shopping or banking, while using public Wi-Fi networks. Disable the "automatically connect to Wi-Fi" setting on your device.

If you suspect you have fallen victim to fraud, report it immediately to your bank. Federal law says you are only liable for $50 in fraudulent charges if you tell your bank within two business days of learning about them. Be sure to complete the necessary paperwork, such as signing an Affidavit. The bank only puts the money back in your account, as a "temporary credit." This temporary credit is made permanent only when you complete the affidavit that is sent to you and you send it back and the bank receives it. To decrease the wait time you may want to visit your local bank branch for assistance.

If you suspect you've fallen victim to identity theft, file a 90-day fraud alert. If you are worried that your personal information -- credit card or otherwise -- may have been compromised, contact one of the major credit bureaus (Equifax, TransUnion and Experian) and request an initial 90-day **fraud alert** for your credit report files with each bureau. The alert grants you a free credit report from each bureau and instructs potential creditors to contact you directly before opening any new lines of credit in your name, decreasing the risk of unauthorized credit activity. Then, if after reviewing your credit reports you discover fraudulent activity, consider taking the alert a step further and **freeze your credit** while you dispute the illegitimacies. However, unlike a free fraud alert, a credit freeze costs about $30 and locks your credit report, preventing all access to new lines of credit.

Use credit cards. There are plenty of reasons to like debit cards more than credit, and credit cards aren't for everyone, but when it comes to fraud protection, there's no contest. Credit cards are safer. Just be sure you pay that card off on time and in full every month.

Check your bank statement often. You check Facebook or Instagram or email several times a day, right? Mix in one visit to check your bank count online every day – or at least once or twice a week. It will just take a moment, and it can help you discover problems as soon as possible.

Find out your bank's debit card liability policy. Will your bank replace fraudulently acquired funds within 24 to 48 hours of you reporting the problem, or will it make you wait until the investigation is complete? If it's the latter, consider opening a second, unconnected account with some "in case of emergency" money to cover you if disaster strikes.

###

April 2015