Commonwealth of Kentucky
Public Protection Cabinet

Steve Beshear, Governor **Ambrose Wilson IV, Secretary**

FOR IMMEDIATE RELEASE

Contact: Kelly May
502-782-9031 Direct
kelly.may@ky.gov

Consumers Should Use Caution at ATMs, Gas Pumps

DFI's Cybercrime Task Force Warns of Skimmers

FRANKFORT, Ky. (Nov. 16, 2015) – It's a common practice today to use a credit or debit card to purchase gas or withdraw money from an Automated Teller Machine or ATM. But beware; criminals may have installed devices to steal consumer information that results in unauthorized account access.

The Financial Cybercrime Task Force of Kentucky – a work group of the Department of Financial Institutions (DFI) – today issued an alert to state-regulated banks and credit unions urging them to routinely check their ATMs for skimmers, devices that criminals use to collect data from a credit or debit card swipe.

"We're taking a proactive step to ensure community banks and credit unions are aware of the risk and keeping consumers protected," said DFI Commissioner Charles Vice. "However, skimming could happen anywhere a card is swiped – not just ATMs – so it's important for consumers to be aware of the risks."

Card skimming involves the capture of a card's magnetic stripe information, and matching it with the card's PIN number in order to produce a duplicate card. This may occur at gas pumps, ATMs or any other point of sale where a customer uses the card and PIN.

The skimming device is placed on the gas pump, ATM or other point of sale in a way that disguises its presence, but allows it to capture the information on the magnetic stripe of the card and the input of the customer's PIN. The customer inserts the card into the ATM that has been modified with a skimming device, performs a normal transaction and retains the card. The customer leaves unaware that the information on the card has been recorded by a criminal. The captured information is then used to produce counterfeit cards for subsequent fraudulent cash withdrawals. The customer will not become aware of the fact until unauthorized cash withdrawals/transactions are made. Because the skimming devices are very sophisticated, and difficult to detect, multiple cards are compromised.

DFI and its Task Force offer the following tips for Kentucky consumers to protect themselves from skimmers:

- Be careful to protect your card number and PIN when using a credit or debit card at ATMs, gas stations or other points of sale.
- Pull or gently tug on the card reader to make sure nothing comes loose. Also check for scratches around the card slot or adhesive tape or glue residue.
- If the card reader scrapes the card, there may be something inside interfering with the swipe.
- Also check the keypad to make sure there is no false overlay. Cover the keypad with a hand while typing in the PIN in case a camera has been installed.
- If anything looks tampered with or suspicious, avoid that reader and notify the business and local law enforcement immediately.
- Use gas pumps closer to the store or pay inside, and choose ATMs that are less remote.
- Review your statements closely and often for any unusual activity, and report it immediately if it occurs. Use of a victim's card information collected through skimming is identity fraud. Notify the bank or card company immediately to preserve your rights and to prevent additional fraudulent transactions. And notify local law enforcement of potential fraud.
- Review your free credit report from each of the three major credit bureaus at least once a year. Visit www.annualcreditreport.com.

What to know if you're a victim:
If you report it early, you may not be liable for fraudulent transactions. However it may take time to get your money back. And your risk of loss may depend on the type of card and how quickly you report it. The FTC offers advice on reporting credit/debit card fraud and tips to keep your information safe at http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards. If you have unauthorized charges on your account, notify your bank and local law enforcement immediately.

The Financial Cybercrime Task Force of Kentucky is a proactive, internal work group of DFI that focuses on best practice guidance and warnings for the financial services industry. The task force's goal is to identify and address emerging threats in cybercrime and security and to protect the integrity of the Kentucky financial system.

DFI, http://kfi.ky.gov, is an agency in the Public Protection Cabinet. For more than 100 years it has supervised the financial services industry by examining, chartering, licensing and registering various financial institutions, securities firms and professionals operating in Kentucky. DFI's mission is to serve Kentucky residents and protect their financial interests by maintaining a stable financial industry, continuing effective and efficient regulatory oversight, promoting consumer confidence, and encouraging economic opportunities.

###