

THE KEY



JUNE 2010



**Farmers
STATE BANK**

MEMBER FDIC

Building Your Success

UNLOCKING YOUR
FINANCIAL OPPORTUNITIES

THE SECURITY EDITION

ATM & DEBIT FRAUD

IN THIS ISSUE:

FALCON PROTECTION,
PROTECT YOUR PLASTIC &
FRAUD TERMS YOU SHOULD KNOW

CD RATES:

9-13 Mo. - 1.60%^{APY*}

16-18 Mo. - 1.85%^{APY*}

25-30 Mo. - 2.20%^{APY*}

60-67 Mo. - 3.20%^{APY*}

IRA CD RATES:

36 Mo. - 2.75%^{APY*}

*APY = Annual Percentage Yield. IRA = Individual Retirement Account. Qualified funds only. Substantial penalty for early withdrawal. Rates subject to change daily. \$1,000 minimum opening deposit for 16-18 month, 25-30 month, 36 month and 60-67 month terms. \$2,000 minimum opening deposit for 9-13 month term. 9-13 month CD interest rate 1.59%, 16-18 month CD interest rate 1.84%, 25-30 month CD interest rate 2.19%, 36 month IRA interest rate 2.73%, 60-67 month CD interest rate 3.18%. Interest compounds semi-annually for 16-18 month, 25-30 month, 36 month & 60-67 month CD's and every 3 months for 9-13 month CD. Effective 6/1/2010.

In 2008, 9.9 million people were victims of identity theft, which is a 21 percent increase from 2007. (Javelin Research)

1 in 4 identity theft victims was compromised through the use of their ATM (automated teller machine) and debit card PIN (personal identification number). There are more than 2.7 million PIN compromises annually. (Federal Trade Commission)

Thieves have targeted some stand-alone ATMs or retailer's point-of-sale machines for "skimming" which allows them to reuse this information to make fraudulent transactions. They place a secondary card reader over the valid reader in order to capture the magnetic strip and key pad information.

According to the U.S. Secret Service, more than \$3 billion is lost annually due to skimming, with one-third of that coming from skimming devices placed on ATM's.

70 percent of financial institutions reported an increase in ATM skimming from 2007 to 2008, according to a 2009 study by Actimize, a financial fraud prevention company.

A favorite tactic of purse-snatchers and pickpockets is to call the victim and ask for the PIN number for verification, claiming to be the police or the victim's bank.

Never give your PIN to anyone. Be wary of your surroundings and of other people who may be near you at the ATM.

The government has developed a special Electronic Funds Transfer Association task force to help prevent skimming. At FSB we are also working hard to protect you from these types of scams. Using Fraud Management Software, I-Banking, Mobile Banking and our Photo Check Card you can be sure that your money is protected from fraud.



EQUAL HOUSING
LENDER

MEMBER FDIC

1-877-FSB-1879 • www.FSB1879.com

FALCON PROTECTION

Debit card fraud is an issue that is becoming more and more prevalent. Most scams begin when someone uses your identifying information, such as your name, social security number, or credit card information without your permission.

Farmers State Bank wants you to know about a few of the products that we currently utilize to protect you from fraud. By partnering with Shazam, FSB is able to offer two very useful tools to help prevent debit card fraud: Falcon Fraud Management Software and Case Management protection Software.

Falcon Fraud Manager identifies and reduces fraud risk by detecting potentially fraudulent PIN-based and signature based debit transactions using state of the art neural network technology. Case Management protection works with Falcon Fraud Manager to monitor cases twenty-four hours a day, seven days a week so we can protect your transactions from fraudulent activity.

.....

PROTECT YOUR PLASTIC

Tips to keep your debit card safe and secure:

Tip #1 - Never give your PIN to anyone who does not share your account - not even family members. Do not give your PIN to anyone over the phone. Thieves often steal cards and then call the victims for their PIN, claiming to be law enforcement or the issuing bank.

Tip #2 - If an ATM looks suspicious, (for example, if it has a discolored card reader or an unresponsive keypad) use another machine, it could be a skimming device.

Tip #3 - Check your bank statements often and report unauthorized transactions immediately. Online banking and mobile banking can be helpful because they allow you to view transactions almost immediately, which is not possible if you have to wait for your monthly statement.

Tip #4 - If you have a reason to suspect fraud, check your account balance immediately by utilizing online banking, mobile banking, or telephone banking.

Tip #5 - Keep a record of card numbers, expiration dates and 800 numbers for your banks so you can contact the issuing bank easily in cases of theft.

Tip #6 - Keep your receipts to check against your statement.

Tip #7 - Mark through any blank spaces on debit receipts, including the tip line at restaurants, so the total amount cannot be changed.

Tip #8 - Know your limits. Many issuers limit daily purchases and withdrawals for your protection.

Tip #9 - Be wary of those trying to help you, especially when an ATM “eats” your card. They may be trying to steal your card number and PIN.

Tip #10 - Do not give your PIN to anyone over the phone. Thieves often steal cards and then call the victims for their PIN, claiming to be law enforcement or the issuing bank.





IT'S OUR PRIVILEGE TO SERVE YOU

We know that getting your money from ATMs is important. We also know that it should not cost an arm and a leg to use the ATM you choose. That is why FSB is a member of SHAZAM's Privileged Status® program.

Our membership is an extra benefit of your free Photo Check Card. Just look for the Privileged Status logo at ATMs, and you will not pay a surcharge fee!

Currently, there are thousands of Privileged Status ATMs available to you. You can obtain an updated list of all the locations by clicking the "[Photo Check Card](#)" link on our home page at www.FSB1879.com.



FRAUD TERMS YOU SHOULD KNOW

Phishing - Refers to an e-mail sent to victims to trick them into providing personal information that fraudsters use to perform fraudulent transactions.

Pharming - Refers to fraudulent attempts on the part of attackers to redirect a Web site's traffic to a bogus Web site. Victims end up at the bogus site without any visible indicator of a discrepancy.

Vishing - Is a combination of the words "voice" and "phishing." It is similar to phishing but uses voice or telephone services instead of e-mail. These scams occur when a fraudster poses as someone wanting personal information from the cardholder such as PINs or passwords. There are reports of vishers leaving voice messages requesting a call back to a fraudulent toll-free number where someone can provide his or her personal information. The voice message may identify a specific local financial institution and indicate that personal accounts have been frozen.

Mishing - Is a combination of the words "mobile" and "phishing." Fraudsters may call someone's mobile phone or leave a message asking for personal information such as PINs or passwords, or ask the person they are contacting to provide personal information to verify a purchase. It is especially important to note that using a mobile phone keypad or keyboard to type personal information may provide the fraudster with the ability to record the information given to them.



EQUAL HOUSING
LENDER
MEMBER FDIC



Farmers
STATE BANK

Building Your Success

CLICK



Apply for
an Auto Loan



Apply for a
Mortgage Loan



Apply for
an Account

AT

www.FSB1879.com

FIND YOUR KEYS

I A E E T I N E E T T I V S
 I P D S R F T I I H I T A E
 M I A E S P S A R B T R T P
 T N T H B S U E C R M E I S
 H F D P H I S H I N G A V E
 T A I S T A T E M E N T V D
 G N I H S I M O L S I M U C
 P R O T E C T I O N M A C G
 R M I T C I V E A T R M N T
 N A I I U I M N T F A I O I
 V C S U R S E V E I H T C S
 A S H P I G P D S S P S L G
 E I R A T N P I I I M D A A
 V T G M Y S M V E I Y I F P

KEY WORDS

- ATM
- DEBIT
- FALCON
- FRAUD
- MISHING
- PHARMING
- PHISHING
- PIN
- PRIVILEGE
- PROTECTION
- SCAM
- SECURITY
- STATEMENT
- THIEVES
- VICTIM
- VISHING

BRANCH & ATM LOCATIONS:

Cedar Falls (1 st St & Hudson Rd) 1710 1 st St Ste A (319) 268-1879	Waterloo (Kimball & San Marnan) 1009 Peoples Sq (319) 287-3961
Jesup 1310 6 th St (319) 827-1050	Raymond 300 South 3 rd St (319) 232-3070
Dunkerton 905 Jon Rd (319) 822-2521	Gilbertville 1222 5 th St (319) 296-1410

OTHER ATM LOCATIONS:

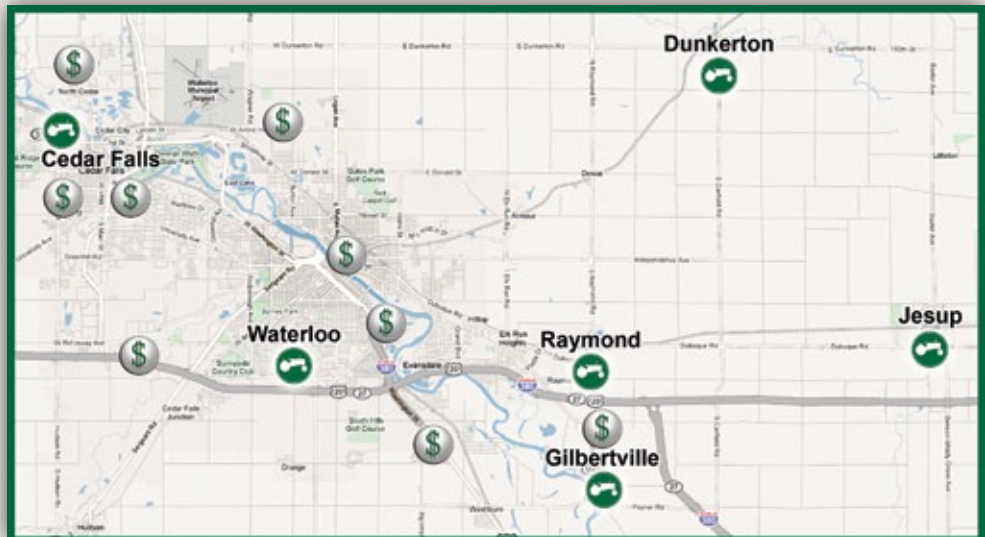
Cedar Falls
 Prime Mart - 2827 Center St
 Tobacco & Liquor - 2328 College St
 Prime Mart - 2323 Main St

Waterloo
 Supervisors Club - 3265 DeWitt Rd
 Omega Cabinets - 1205 Peters Dr
 Court House - 316 E 5th
 Prime Mart - 1008 LaPorte Rd
 Prime Mart - 3535 Marigold Dr

Gilbertville
 Mini Mart - 115 25th Ave

Independence
 Starlight Cinema - 2401 Swan Lake Blvd

BRANCH & ATM LOCATIONS



- BRANCH'S & ATM'S

- FSB ATM'S

