The Dime Bank

Security Tips

THE DIME BANK

Debit Card Fraud Information

In order to securely process your transactions please use your PIN, especially in high risk retailers such as supermarkets, pharmacies, and discount & variety stores. Also, check your accounts regularly to monitor activity.

Below are a few commonly asked questions and answers:

Why do I have to use my PIN when I never had to in the past?
Due to the changing fraud environment, your PIN is the safest and most secure means of processing transactions. Criminals do not usually get access to PIN numbers during a breach.

What if I do not know my PIN?
Bank employees do not have access to your PIN but we can order you a PIN reminder at no cost to you, which will take approximately one week. We can also rush order you a new PIN from our PIN provider. The vendor's fee for this service is $15. The PIN will be conveyed to you by an Electronic Banking representative in about an hour's time.

What if I'm having trouble using my PIN?
Please call Electronic Banking for further assistance at **570-253-1970.**

I am nervous about all of the breaches occurring. Can I get a new card?
Yes, we can order you a new card immediately. You will receive it in the mail in about a week.

Can I keep my old card open while a new card is ordered?
We would prefer that if your card may have been compromised, that the card be deleted in order to safeguard your money.

Is the use of the PIN requirement permanent?
Yes, for the foreseeable future. Your PIN is an additional layer of security and fraud trends indicate PINs are not included as part of stolen information.

What else can I do to protect my money?
Check your accounts regularly to monitor activity. Report unauthorized activity immediately by calling **570-253-1970** or your local branch and cancel your card. After hours you can cancel your card by dialing 1-866-342-5693 (**1-866-DIAL-MY-D***ime*)**, option 5**.

Back to menu

Beware of Unsolicited Phone Calls

Here at The Dime Bank we have extensive policies, procedures and software in place to identify cases of fraud or identity theft.

Beware of unsolicited phone calls from unusual phone numbers regarding your accounts. If you receive a phone call asking you for account information, Internet banking information, or debit card information, do not respond, this may be a scam. When unsure, please hang up and contact your local branch office. If you have responded and provided any information, please contact your local branch or The Dime Bank's corporate office at 570-253-1970 or toll free at 888-4MY-DIME (888-469-3463).

The Internet is an inexpensive way for criminals to attempt to scam individuals into revealing confidential information, such as credit card numbers, bank account data, social security numbers, and driver's license numbers, as well as deceiving computer users into clicking on links or attachments that compromise the security of their computer. There are constant reports of customers and non-customers receiving fraudulent emails or phone calls requesting account and/or debit card information, including PINs, passwords, phone numbers and email addresses.

Back to menu

ARE YOU A SAFE INTERNET USER?

YOU MAY BE AT RISK IF YOU ANSWER YES TO ANY OF THE FOLLOWING QUESTIONS:

- Do you visit websites by clicking on links within an email?
- Do you reply to emails from companies or persons you are not familiar with?
- Have you received packages to hold or ship to someone you met on the Internet?
- Have you been asked to cash checks and wire funds to an employer you met online?
- Would you cash checks or money orders received through an online transaction without first confirming their legitimacy?
- Would you provide your personal/banking information as a result of an email notification?

DON'T BE AN INTERNET CRIME VICTIM!
For more information and to test your online practices visit:
www.LooksTooGoodToBeTrue.com*

TO REPORT AN ONLINE CRIME VISIT:
WWW.IC3.GOV*

REMEMBER; NEVER give out any of your personal financial information such as account numbers, PIN numbers, expiration dates, etc. to an unsolicited phone call, fax, email, or letter.

Back to menu

*This website is not affiliated with The Dime Bank.

Information Security - Account Hijacking

The Dime Bank will never request sensitive information from ANYONE via email.

We want to keep you informed of some scams that are currently active on the Internet that effect your privacy and your account information.

According to the FDIC account hijacking is presently the fastest growing form of identity theft. Account hijacking is the unauthorized access and misuse of existing bank account information, primarily through "Phishing" attacks. A classic Phishing attack involves a deceptive email purporting to be from a legitimate financial institution, which typically tells a customer that there is some sort of problem with the customer's account. The email usually includes a hyperlink to a "spoofed," or fake, website that looks exactly like the site of a legitimate financial institution with which the consumer does business.

The email then typically instructs the recipient to click on the included hyperlink, go to the financial institution website, and log in using the customer's user name and password in order to "fix" the problem. In reality, the spoofed website is simply collecting customer user names and passwords in order to highjack accounts.

Never respond to an email asking you to verify bank account information or click on links in an email message, even if it looks like it is from The Dime Bank. Forward it to us and then delete it. The Dime Bank will never request sensitive information from ANYONE via email. If you have any questions about the legitimacy of an email that looks to be from The Dime Bank, please contact your local branch. If you receive a call, don't provide any information, ask for their phone number, hang up and call us immediately at 570-253-1970 or toll free at 1-888-4MY-DIME (1-888-469-3463).

Please help us safeguard your information. We're here to help you in any way we can.

Back to menu

What to Do If Your Identity is Stolen

Identity theft happens when someone steals your personal information and uses it without your permission. It is a serious crime that can wreak havoc with your finances, credit history, and reputation – and it can take time, money, and patience to resolve. The Federal Trade Commission (FTC), the nation's consumer protection agency, prepared this guide to help you repair the damage that identity theft can cause, and reduce the risk of identity theft happening to you.

Adults can monitor their own credit reports every few months to see if someone has misused their information, and order a fraud alert or freeze on their credit files to stymie further misuse. But most parents and guardians don't expect their youngster to have a credit file, and as a result, rarely request a child's credit report, let alone review it for accuracy. A thief who steals a child's information may use it for many years before the crime is discovered. The victim may learn about the theft years later, when applying for a loan, apartment, or job. The Federal Trade Commission (FTC), the nation's consumer protection agency, prepared this guide to help you safeguard your child's identity.

Back to menu

Tips to Deter Scams

- Throw away any offer that asks you to pay for a prize or a gift. If it's free or a gift, you shouldn't have to pay for it. Free is free.

- Resist the urge to enter foreign lotteries. It's illegal to play a foreign lottery through the mail or the telephone, and most foreign lottery solicitations are phony.

- Know who you are dealing with, and never wire money to strangers.

- If you're selling something, don't accept a check for more than the selling price, no matter how tempting the offer or how convincing the story. Ask the buyer to write the check for the correct amount. If the buyer refuses to send the correct amount, return the check. Don't send the merchandise.

- As a seller, suggest an alternative way for the buyer to pay, like an escrow service or online payment service. There may be a charge for an escrow service. If the buyer insists on using a particular escrow or online payment service you've never heard of, check it out. Visit its website, and read its terms of agreement and privacy policy. Call the customer service line. If there isn't one — or if you call and can't get answers about the service's reliability — don't use the service. To learn more about escrow services and online payment systems, visit www.ftc.gov/onlineshopping*.

- If you accept payment by check, ask for a check drawn on a local bank, or a bank with a local branch. That way, you can make a personal visit to make sure the check is valid. If that's not possible, call the bank where the check was purchased, and ask if it is valid. Get the bank's phone number from directory assistance or an Internet site that you know and trust, not from the check or from the person who gave you the check.

- If the buyer insists that you wire back funds, end the transaction immediately. Legitimate buyers don't pressure you to send money by wire transfer services. In addition, you have little recourse if there is a problem with a wire transaction.

- Resist any pressure to "act now." If the buyer's offer is good now, it should be good after the check clears.

- Do not respond to emails that warn of consequences unless you validate your information immediately. Contact the company to confirm the validity of the email.

- Check your credit card and bank account statements regularly, look for unauthorized transactions.

- When submitting financial information online, look for the padlock or key icon at the bottom of the Internet browser.

Back to menu

*This website is not affiliated with The Dime Bank.

Skimming

What is ATM skimming?

Skimming is a high-tech crime in which a criminal electronically steals or skims the cardholder's personal financial information during routine ATM transactions. Skimmers fit a portable electronic card reader right over the ATM's card reader slot, to capture the card information. They install mini cameras in the ceiling above the ATM or on the walls or in literature racks beside the ATM to capture the customer's PIN keystrokes. Those two streams of data are then transmitted through wireless blue-tooth technology to the criminals just around the corner in a coffee shop or in their car downloading all the data or they're stored and recorded in the devices themselves. The average cardholder has no knowledge that the skimming device is there because it does not interfere with the operation of the ATM.

What do ATM skimmers do with the data they collect?

The thieves use the information they have gathered to manufacture counterfeit cards, make purchases and withdraw funds from your accounts. Often skimmers will wait a period of time before using the data they've collected.

When does skimming happen?

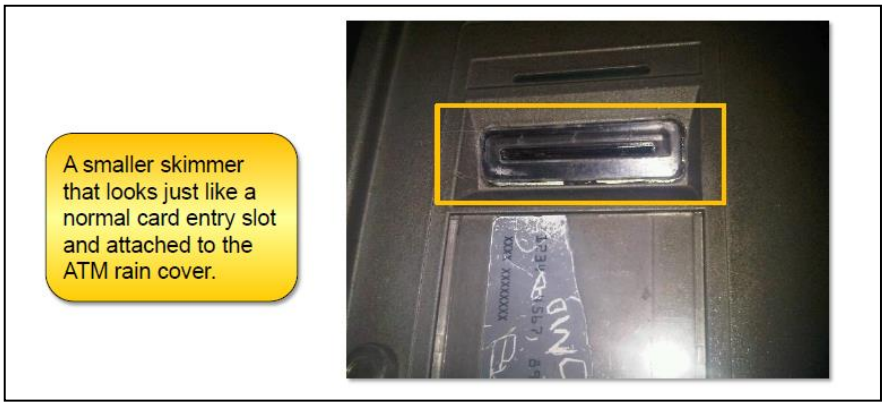
Skimming usually happens at peak transaction times, such as lunch hour or after work. Since there are legitimate uses for many of the devices used to read or skim credit and debit cards, paying attention to where you use your credit and debit cards can also help prevent fraud. Examples of skimming instances include:

- A collusive store employee completes a valid sale, and then captures a second (unauthorized) swipe covertly on a portable device before returning the card to the cardholder.
- A skimming device is added to the front of an ATM or gas pump and captures the credit card information as the consumer attempts to use the machine.
- A skimming device is added inside an ATM or gas pump and captures information during a valid transaction. In many cases a covert camera is also set up to capture the card holder’s personal identification (PIN) number.

To help protect against skimming/fraud:

- Check devices prior to inserting your card.
- Ensure your card is swiped only once at a register or into a hand held device.
- Conceal your PIN as you enter it into an ATM or credit card reader.

Skimming Devices



How can you reduce the risk?

- Use secure ATM machines under video surveillance or inside of a bank lobby. They're less likely to be tampered with.
- Pay careful attention to what the card reader and keypad normally look like on the ATMs you use most frequently.
- Inspect the ATM and all areas of its fascia for unusual or non-standard appearance. Don't use an ATM if the card reader appears to be added on, fits poorly, or is loose. Some thieves place a fake box over the card slot that reads and records account and PIN numbers.
- Call the customer service number on the ATM immediately if a machine appears suspicious or if it does not function properly.
- Always use your hand to shield your PIN when entering it so that if criminals have installed a surveillance camera, they won't be able to see your secret code.
- Experts suggest "re-pinning" your credit and debit cards every six months. Just go to your local Dime Bank ATM and choose "Other" from the main menu. Then choose the Pin Change option.
- When it's time for a new credit or debit card, you can ask for a fresh card number. This will stop the cycle of theft, if your old card has already been compromised.
- Thieves often install skimmers inside gas pump credit card slots. To thwart them, pay inside or pay with cash.

Thieves Target Gas Pumps to Skim Credit, Debit Cards

The crime of skimming has now also taken a worrying turn by targeting gas station pumps, which are far easier to tamper with than ATMs and more difficult to detect. Posing as maintenance techs, the crooks actually open up the gas pump card readers and insert their skimming devices inside. Most gas stations apparently use the same master key codes on their pumps, making them easy prey for the scammers. Unlike the ATM skimming version of the crime where a sharp eye could spot that the machine has been tampered with, users, including the pump attendants, may be totally unaware of this skimming and scanning.

Like regular ATM skimmers, the devices read the magnetic strip from the cards, while a hidden camera picks up the keypad clicks for debit card PINs.

The stolen information is then transmitted wirelessly to the crooks who use it either for fraudulent purchases or, with debit cards, to manufacture so-called "white-cards" which is blanks onto which the data is loaded so they can be used at ATMs to drain cash from victims' accounts.

It's important to be aware of the skimmers when using cards at the gas pumps. Check your bank statements regularly, if not daily to make sure there are no charges that you didn't make. Sign up for Dime On Line or Mobile Dime so that you have your account information at hand at all times when you are on the go. You can also choose to pay inside, use cash, and avoid pumps that seem to have been tampered with.

If You Have Been a Victim of ATM Skimming

If you think you have used an ATM or a gas pump with a skimmer attached and you believe it has compromised your personal information **contact The Dime Bank immediately at 1-888-4MY-DIME (1-888-469-3463) during our regular business hours. If you need to report your card stolen after banking hours please call our automated telephone system at 1-866-342-5693 (1-866-DIAL-MY D*ime*). You should also contact your local law enforcement office.**

Back to menu

Phishing

Information courtesy of NACHA.org *

What is a phishing scam?

Phishing scams are typically fraudulent emails that appear to come from legitimate entities such as financial institutions, government agencies, or other well-known organizations or companies, which seek to steal personal information that can be used for identity theft or to fraudulently make purchases or access other private accounts

Phishing or fraudulent emails may contain links to phony websites, contain attachments for you to open, or request you to share personal or financial information by using clever or compelling language, such as an urgent need to update your information, decline a payment or communicate with you to ensure the security of your accounts.

Typically, when you open the attachments on visit the phony websites your computer is infected with malicious software that enables the perpetrators to capture your usernames and passwords and ultimately take control of your device without your knowledge.

What to Do?

Do not open suspicious emails or emails from unknown parties. Never respond to or click on any links, attachments, photos, graphics, etc., in an email that you receive from an unknown sender or that is suspicious. If you receive a suspicious email that claims to be from NACHA regarding a payment transaction, forward the email to abuse@nacha.org* and delete it from your system.

If malware is detected or suspected on a computer, consult with a computer security or anti-virus specialist to remove the malicious software. Always use anti-virus, anti-malware, and anti-spamming security software on your system and ensure that all available security patches are installed and remain current.

Fraud & Phishing Resources

NACHA provides this resource area to educate consumers, businesses, financial institutions, and other parties about ways to protect themselves from phishing scams. Phishing scams are typically fraudulent emails that appear to come from legitimate entities such as financial institutions, government agencies, or other well-known organizations or companies, which seek to steal personal information that can be used for identity theft, or to fraudulently make purchases or access other private accounts.

Be Aware That:

- Since 2011, cybercriminals have been using NACHA's name, logo, contact information and product names, such as Direct Deposit via ACH, through phishing email communications and social engineering tactics to gain access to consumer and business computer devices.
- The perpetrators of this criminal activity continue to evolve their tactics and employ sophisticated means to make their fraudulent emails appear legitimate.
- NACHA is one of multiple, reputable organizations including the Federal Reserve, FDIC, IRS, Better Business Bureau, other payment organizations, financial institutions, technology providers, and businesses that have experienced these types of attacks.
- NACHA does not process nor otherwise touch the ACH transactions that flow via the ACH Network nor between financial institutions and their customers.
- NACHA does not send communications of any type to persons or organizations about individual ACH transactions that they originate or receive. If you or your customer has received a communication of this nature that purports to come from NACHA, it is fraudulent.

*This website is not affiliated with The Dime Bank.

- NACHA is the industry trade association that manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data.

- The ACH Network serves as a safe, secure, reliable network for direct consumer, business, and government payments, and annually facilitates billions of payments such as Direct Deposit and Direct Payment via ACH.

- In 2012, NACHA joined with Microsoft Corporation, the Financial Services – Information Sharing and Analysis Center (FS-ISAC), Kyrus Tech, Inc., and financial institution representatives to plan and execute coordinated action to disrupt some of the most notorious cybercrime operations that have been responsible for fueling online fraud and identity theft. This specific action has significantly impacted the cybecriminals' infrastructure and operations and ongoing efforts will continue to help reduce the source of this type of fraudulent activity. For more information, visit http://www.microsoft.com/en-us/news/presskits/dcu/ .*

If you think you have been a victim of phishing and your personal information has been compromised **contact The Dime Bank immediately at 1-888-4MY-DIME (1-888-469-3463) during our regular business hours. If you need to report your card stolen after banking hours please call our automated telephone system at 1-866-342-5693 (1-866-DIAL-MY D*ime*). You should also contact your local law enforcement office.**

Back to menu

*This website is not affiliated with The Dime Bank.

For more information, visit any of the following websites:

FBI FRAUD ALERT Poster - http://www.fbi.gov/majcases/fraud/fraud_alert.pdf*

Federal Deposit Insurance Corp.
http://www.fdic.gov/consumers/consumer/news/cnwin0304/phishing.html*

Federal Trade Commission – Protecting America's Consumers - http://www.ftc.gov*
Information on Phishing - http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm*
Information on Identity Theft - http://www.ftc.gov/idtheft*

Anti-Phishing Working Group - http://www.antiphishing.org*

National Consumers League - http://www.phishinginfo.org/*

OCC Consumer Protection News - http://www.occ.gov/Consumer/phishing.htm*

Suspicious activity should be reported to the Internet Crime Complaint Center a partnership between the FBI and the National White Collar Crime Center at http://www.ic3.gov/*

Identity Theft Information - www.consumer.gov/idtheft* or call **1-877-ID-THEFT**

Back to menu

*This website is not affiliated with The Dime Bank.