Bank Account Fraud

A Financial Disease With a Proven Cure

Bank account and transaction fraud is a fast-spreading disease in the financial services world. Some of this disease hits people randomly, but that is very rare. Nearly all other times, the disease strikes people who are most prone to getting it.

But there is a cure, both with medicine and plenty of preventative action.

This communication from Denison State Bank is being sent to all our checking account holders with hopes to explain bank fraud more fully and what can be done to avoid it.

The best way to avoid bank fraud is to not put yourself into a situation that increases the chances for outside influence and intrusion into your private banking information. You as the account holder control the keys to the lid on your checking account. If you keep the keys secured and to yourself, any chances of outside access are nearly impossible.

Keep clicking through next pages, 2-8

About DSB Customers and Fraud

FACT
Denison State Bank and its core data systems processor, CSI, have not been subject to any breaches or hacks that broke into their operating systems and account holder information. Some merchants, including global brand names, have exposed certain levels of confidential customer information.

FACT
Nearly all of the account and transaction fraud that has been reported to the bank is the result of decisions and actions by the account holders.

FACT
As an account holder at a regulated U.S. bank, you have several rights and protections provided by law and backed by the goodwill of Denison State Bank.

Read on to know the facts about bank fraud and how you can avoid it.

Delivered to you by the Digital Banking department of

DENISON STATE BANK

October 2022

online@dsbks.com
1-800-633-2423
www.dsbks.com

Don’t get hooked with phishing

Phishing, vishing and smishing - they may be funny words, but they are very serious when it comes to how they can cause loss of money.

PHISHING
Phishing is the criminal attempt to acquire sensitive information such as usernames, passwords and card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email, directing users to enter personal financial details on a link to a fake form or website whose look and feel are almost identical to a legitimate one, such as their bank. Phishing attempts often look as if they are sent from trusted companies you may already know. Typically, phishing scams require you to click on a link and complete an action like confirming personal information. The message may even mention suspicious activity on a personal account.

• *Protect yourself* by remembering that your financial institution will never send an email asking for personal information or send you to a special site to “update personal information.” A bank has no reason to email you for account information it already has. If you receive an email asking you to click a link or provide account information, assume it’s fraudulent. Don’t click any links and mark the email as spam. If you do not know the source, delete the email and contact the source yourself to verify and/or report the scam.

Urgent action: A common theme in phishing emails is the urgent call to action. Cybercriminals want to scare you into acting immediately without thinking. The email says there was suspicious activity on your account, and you should log in immediately to avoid having it frozen or closed.

No legitimate business would close a customer’s account without giving reasonable notice. Contact your bank through your normal channels to check your balance and account activity if you aren’t sure.

Tip: Misspelled words and grammatical errors are another red flag. Major corporations have professional editors to make sure the content is correct.

VISHING
Vishing is the name for phishing attacks using the telephone. The term is a combination of voice and phishing, and is typically used to steal card numbers, bank account numbers and passwords. You might receive a phone call advising you that your debit/credit card has been used illegally, and to call a certain number to “verify” your account number. Banks or other financial institutions don’t call for your PIN or checking account number. Never provide this over the phone.

• *Protect yourself* by being suspicious of any phone call asking you to provide card or bank numbers. Rather than provide the information, contact your bank or card company directly to verify the validity of the message.

SMISHING
Smishing is yet another variation of phishing, the name a combination of SMS (Short Message Service, the technology used in text messaging) and phishing. In this scam, the fraudster uses text messages to lure you to a website or perhaps to use a phone number that connects to an automated voice response system. The smishing text message typically urges your immediate attention. For example, it might say it is confirming an order for a large computer purchase, and you need to follow directions in order not to be charged for the item. Once you click on the URL or call the phone number, you are asked to provide card numbers, account numbers, PIN numbers, etc.

• *Protect yourself* by assuming that no legitimate business would contact you by text message with a request of this nature. Texting should be a permission-based activity extended only to company customers who have opted-in to receiving texts or whose registrations with an online service includes text notices to service the account.

Use your gut feeling. If it does not sound right, it probably is not right. Think before you click.

Keep your computer, phone, devices clean

For all the internet's advantages, it can also make users vulnerable to fraud, identity theft and other scams. The American Bankers Association offers the following tips to help consumers stay safe and secure online:

• **Keep your computers and mobile devices up to date.** Having the latest security software, web browser, and operating system versions are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.

• **Malware,** a blend of the words "malicious" and "software," can infiltrate or damage a computer system without the owner's knowledge. Getting malware can happen with an innocent click of a link. Malware includes computer viruses, worms, trojan horses, spyware, adware, and other malicious and unwanted software. You can purchase and install anti-malware and anti-virus software protection.

• **Keep personal information personal.** Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools. Lock down your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of requests to connect from people you do not know.

• **Secure your home Wi-Fi.** Always protect your home wireless network with a password.

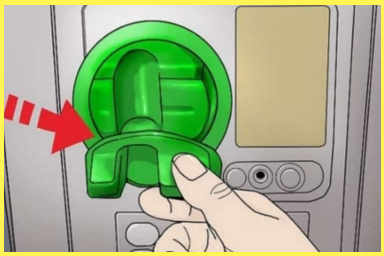
• **Purchase safely.** Before making purchases online, make sure the website uses secure technology. When you are at the checkout screen, verify that the web address begins with https. Also, check to see if a tiny locked padlock symbol appears on the page.

• **Back up files.** If you create data files such as in Word and Excel, subscribe to a back-up program to ensure you don't lose your data.

Look for ATM skimmers

Card fraudsters insert a "skimmer' device on ATMs that can read and capture a card's magnetic stripe and keypad information. With that in hand, the skimmer will sell that data to criminals who create new cards with your account numbers.

Protect yourself by using ATMs from banks you know and trust. Thieves like to put skimmers on ATMs that have low traffic and no surveillance cameras. If you notice a change at an ATM you use routinely, such as a color difference in the card reader or a gap where something appears to be glued onto the slot where you insert your card, that's a warning it's been tampered with.



Example: **JastgLialw80$** (from Journey's 'Just a small town girl Living in a lonely world')

Strong passwords are key to anti-hacking

Another way hackers may try to access your bank account is to steal or guess your password. If they can log into your account, they can use your sensitive information for personal gain and identity theft. They can then open credit card accounts in your name, purchase merchandise, or transfer money out of your account.

Cybercriminals use technology to guess billions of passwords per second. However, it's more difficult to guess long passwords with a combination of letters and numbers. For example, hacker software can instantly guess a password consisting of eight letters. Adding one uppercase letter extends the time it takes to crack a password to 22 minutes. **In contrast, a 12-character password with an uppercase letter, a number, and a symbol would take 34,000 years to crack.**

At some point, almost everyone has used the same password for different websites. But this is one of the simplest ways for hackers to get into your accounts. If they figure out the password for one, they can sometimes access your other logins.

Use unique passwords for each website. Set strong passwords. A strong password is at least eight characters in length and includes a mix of upper and lowercase letters, numbers, and special characters, as required in passwords for DSBconnect digital logins.

Everywhere you look, there's a

Bank scams are a common way for criminals to gain access to people's personal and financial information. Scammers use various methods to trick people into giving up sensitive information like bank account numbers and passwords.

Here are some common bank scams and what you can do to protect yourself.

Overpayment Scams
If you provide services or sell products online, you could fall victim to an overpayment scam. Overpayment scams typically begin with someone sending you a counterfeit check or money order for more than the amount owed. Then, they ask you to deposit the money in the bank and wire the difference back to you.

Unfortunately, since the check was fake, you could owe the bank a returned check fee. You're also out any funds you wired to them and the product if you shipped it.

Check-Cashing Scams
Another scam involving checks is the check-cashing scam. This scam preys on the compassion and generosity of other people. An individual approaches you outside of a bank or other financial institution asking if you will cash a check for them. They may mention that they don't have an account at this particular bank but need the money.

You can deposit the check and pull cash from your account to pay the person their funds. However, the clearing process can take several days. So, when the check doesn't clear, the funds are held against your account.

Unsolicited Check Fraud
Have you ever received a check in the mail that you weren't expecting? It could look like a rebate check or a refund for overpayment. Inspect the check thoroughly, paying close attention to any fine print on the front or back. There's a chance that you are entering into a legally binding contract by signing the check and cashing it. Scammers use tactics like this to get you to authorize memberships, loans and other longer-term commitments that could cost you dearly. Checks that have pre-printed payee endorsement on the back side are not negotiable and are fraud.

Scammers are counting on you blindly accepting the check as free money and cashing it. Be wary of cashing any rebate or refund check you weren't expecting.

Automatic Withdrawal Scams
Automatic withdrawals are a great way to automate your savings, pay bills and more. Scammers like automatic withdrawals too, but for other reasons.

The way this scam works is that individuals receive a phone call or postcard indicating that they've won a prize or qualified for a special offer. The goal is to get you to read off the numbers at the bottom of your personal checks. They often play this off as a way to verify that you qualify for the offer.

Once the scammer has your checking and bank information, they put it on demand draft, which is processed like a check but doesn't require a signature. Upon receiving the draft, your bank will transfer money from your checking account to pay the scammer. Unless you pay close attention to your daily bank transactions, you may not notice the scam until much later.

(continued next page)

fraud scam waiting for you

Government Imposter Scams
Another scam is when someone pretends to be a government official. You receive a phone call from the imposter claiming you've won a prize that requires payment of taxes or fees so they can process it. The scammer may threaten to send you to prison if you don't pay a supposed outstanding debt. The reality is that you will never receive a call from a federal agency asking for payment of any kind.

Scammers may use a fake federal agency name like the National Sweepstakes Bureau or the names of real agencies, like the Federal Trade Commission. Either way, it's a scam because this isn't a strategy used by federal agencies to collect payments.

Charity Scams
Scammers also like to take advantage of people's kindness by impersonating charities. They call people asking for donations to a charity or cause. Some scammers will disguise the phone number, so it shows up as a local area code on your caller ID.

You can sometimes spot charity scams by the vague claims they make and the lack of tangible ways your donations are used. Scammers also like to use fake names that sound like the names of legitimate charities.

Employment Scams
Employment scams are another common way scammers try to gain access to people's financial accounts. The scammer promises guaranteed work in exchange for an up-front fee. They may also ask for bank account information so they can transfer commission payments to you. This is all a front to get your bank account information, though. Job scams often come through emails, but scammers also target people by phone and mail. In some cases, job websites may unknowingly approve job postings that turn out to be scams.

How to tell if email is legit

Below are five red flags that can help determine if an email is legitimate.

Spelling and bad grammar
Legitimate companies employ copy editors to review content before circulation, so there should be no spelling or grammatical errors. Cybercriminals, on the other hand, tend not to worry about such niceties. Beware when you see misspellings or other grammatical inaccuracies.

Links in emails
Look before you click. Whenever an email contains a link that you want to access, before you click to open it, hover your cursor over the link to see if the addresses match. If not, refrain from clicking.

Threats
One sign that may indicate a phishing scheme is receiving a threat, such as, "Your account will be closed if you don't respond by clicking the link below." Another red flag is alerts that your security has been compromised.

Be Wary Of Emails Concealing Their True Identity. If someone sends you an email using a mail header that has no useful identifying data (e.g., W6T7S8@provider.com), that may be an indication that the person is hiding something and is not legitimate.

Spoofing company websites
Cybercriminals will place logos and other imagery belonging to the companies they're impersonating into the email message body, then link those images to their malicious scam sites. If you click on an image and are brought to the supposed site, look closely at the URL. Some scammers will use an address that closely resembles the URL of the company they're looking to imitate; an example would be www.applle.com. You can also hover over the images. The spoofed site looks very much like the legitimate site. Access to the shadow web is funneled to the attacker's machine, allowing the attacker to monitor all of the victim's activities, including passwords or account numbers the victim enters.

Emails from DSB employees end in @dsbks.com
Email notices from our various service providers may use a different domain.

Don't use public Wi-Fi for your mobile banking. Wi-Fi is too unsecured. Only use your mobile carrier connection.

How to set up fraud alerts on your credit file

There's good news for anyone who is worried that their financial information has fallen into the wrong hands. Consumers can place a fraud alert on their credit file.

Fraud alerts help prevent anyone from opening new accounts in your name. They act as a red flag on your credit report, visible only when creditors access your file to possibly extend your credit. To place an alert on your account, call one of the three credit reporting agencies below and order them to flag your credit file for fraud. Within 24 hours, an alert will be attached to your credit file and your name will be removed from pre-approved credit and insurance applications for two years.

An **"Initial Alert"** will be active on your credit report for 90 days. Use this if someone has gained access to personal information that could be used to open accounts in your name, such as your Social Security number or your date of birth. Once an initial alert is in place, potential creditors will need to call you verify your identification prior to extending credit. The alert will help to ensure that you are the only one opening accounts in your name.

An **"Extended Alert"** is recommended if your identity has been stolen. With an extended alert, your credit file will remain guarded for seven years. In addition, your name will be removed from lists marketing pre-screened credit offers for five years.

Members of the military on active duty are eligible for "Military Fraud Alert." This alert allows members of the military to prevent anyone from opening accounts in their name while they are overseas.

Check your credit report at least annually. You are entitled to one free credit report annually from each of the three major credit bureaus. If a hijacker is misusing your credit, clues are likely to show up here. For a free report, visit annualcreditreport.com

Remember: **If you put a freeze on your credit report, you will need to remove it before applying for a bank loan.**

Source: American Bankers Assoc. / Financial Education Corp.

How to contact the Big 3 Credit Bureaus

Experian, Equifax, and TransUnion are the three credit-reporting agencies. They share data, so after calling one agency the other two will be notified.

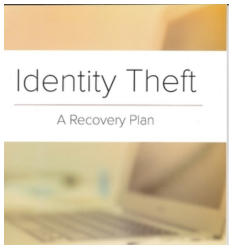
Examine their web sites to see how to place and remove freezes and alerts to your loan accounts.

Equifax	**www.equifax.com**	**1-888-766-0008**
Experian	**www.experian.com**	**1-888-397-3742**
TransUnion	**www.transunion.com**	**1-800-680-7289**

Get this free 32-page booklet at DSB

Identity theft often leads to much bigger problems

Identity theft is the fraudulent acquisition and use of a person's private identifying information, usually for financial gain. ID theft can often become a starting point for larger crimes. While financial ID theft is most common, there also can ID thefts involved in tax, medical, employment, child, and seniors information. The best source to refer to for ID theft is the



Federal Trade Commission at identitytheft.gov. In addition, Denison State Bank has their free 32-page booklet to provide in the event of ID theft. It provides detailed advice to help fix problems caused by identity theft, along with the ability to get a personal recovery plan, as well as letters and forms that might be needed.

Small businesses, orgs must be watchful too

Cybercriminals are targeting small businesses and non-profit organizations with increasingly sophisticated attacks. Combating account takeover is a shared responsibility between businesses and financial institutions. The American Bankers Association offers small businesses and organizations these tips to help prevent account takeover:

• Educate your employees. You and your employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

• Protect your online environment. It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically.

• Be careful with "BYOD" Bring Your Own Device. It is common these days for employees to use their personal mobile phones for business purposes such as multi-factor authentication. Business managers should set the level of acceptance they have for employees using personal devices.

• Reg E that covers electronic funds transfers (EFTs) does not apply to non-consumer bank accounts.

• Partner with your bank to prevent unauthorized transactions. Talk to your banker about programs that safeguard you from unauthorized transactions. Certain bank services offer call backs, device authentication, multi-person approval processes and batch limits help protect you from fraud.

• Pay attention to suspicious activity and react quickly. Look out for unexplained account or network activity, pop ups, and suspicious emails. If detected, contact your financial institution, stop all online activity and remove any systems that may have been compromised. Keep records of what happened.

• Understand your responsibilities and liabilities. The account agreement with your bank will detail what commercially reasonable security measures are required in your business. It is critical that you understand and implement the security safeguards in the agreement. If you don't, you could be liable for losses resulting from a takeover. Talk to your banker if you have any questions about your responsibilities.

Who to contact with fraud-related complaints

Federal Trade Commission (FTC) Consumer Response Center | www.ftc.gov You can file a complaint with FTC against a company or organization that you believe has cheated you by calling toll free 877-FTC-HELP (382-4357).

Department of Justice, Consumer Fraud Division | www.usdoj.gov "Fraud" is a link on this site under "Information for Individuals and Communities."

Consumer.gov | www.consumer.gov This is a "one-step" link to a broad range of federal information resources available online.

Social Security Administration | www.ssa.gov Report Social Security fraud by calling 1-800-269-0271.

Identity Theft Resource Center | www.idtheftcenter.org Call 858-693-7935.

How Denison State Bank protects your financial info and identity

DSBconnect Digital Banking

Secure Logins
Each registered user creates a unique username. No one else on the DSB system has the same username.

Each user creates a strong password: minimum of 8 character spaces - minimum of 1 capital letter - minimum of 1 numeral - minimum of 1 special character. Users are prompted to change their password every 365 days from date of registration.

Multi-factor authentication
Each user chooses 3 identification questions about themselves and keys in case-sensitive answers that only they should know.

NEW: Additional MFA has been added to External Transfers and Person to Person (P2P) Transfers conducted on DSBconnect. Users must provide a mobile phone number, and each time these transfers are initiated, the user must key in a one-time MFA code that is texted to the mobile phone number on record.

Bill Pay:
Per-item payment limits in put in place, either by default or by qualification of the user. Our Bill Pay service provider monitors for unusual or suspicious activity and will notify the bank before processing, and the bank will verify with the Bill Pay user before release.

Cards and Checks

Visa Debit Cards:
Reg E as well as Visa card rules protect Visa cardholders from unauthorized transactions and losses in qualified cases, which are too numerous to explain here. If an unauthorized debit card transactions posts to your bank account, contact us as soon as possible.

Checks
If you lose an entire checkbook or if it gets stolen, it may warrant closing the account and opening a new one with different account number and checks. If you lose just one or two checks, it usually does not warrant closing.

You are not liable for unauthorized checks that clear your account. If you deposit a check and it is returned for non sufficient funds or is bogus, the liability falls on you the account holder, not the bank.

View and keep your bank account statements. They may be your only record you have of fraud transactions.

Our Systems and Controls

Vendor Management
All vendors, processors and service providers that the bank contracts with are researched and vetted. We request and collect their policies and procedures on data security that must meet industry standards.

Outside Audit and Regulatory Exams
In addition to our internal policies and controls, we hire outside auditors to audit our operations, and we follow their findings for best practices and rules compliance. The bank is examined annually by the Office of State Bank Commissioner and the FDIC. The bank must demonstrate it complies with all applicable laws and regulations related to data security.

Capital
DSB retains a higher-than-required amount of capital as protection and cushion against severe losses, should they occur.

FDIC Insurance Does Not Apply To Fraud
FDIC insurance covers only in the event of a bank failure, not for individual fraudulent or unauthorized transactions. Account holders may have purchased fraud and identity theft protection insurance through private insurers.

If you discover any unauthorized transactions on any of your DSB accounts, contact the bank as soon as possible.

Call: (785) 364-3131 *Email:* online@dsbks.com *Visit:* Any DSB branch
DSBconnect: click Messages & Forms > New Request / Choose A Form