Fraud Complaints

*Complaints by victim Age (2019)*

*Age 60 & Over Decreased 5% From Previous Year*

Fraud Complaints

Complaints by victim Age (2019)
Compared to Representation in Population

*Percentages are based on the number of consumer fraud complaints where victims reported their age: 858,299 in CY-2019 (51%).
Common Frauds and Scams in Nebraska
Common Frauds and Scams in Nebraska

Based on Fraud Complaints to NE AGO and the Federal Trade Commission

“The Dirty Dozen”

- Imposter Scams
- Identity Theft
- Home Repair and Improvement
- Telephone and Mobile Services
- Online Shopping
- Prizes, Sweepstakes and Lotteries
- Banks, Lenders, and Credit Bureaus
- Debt Collection
- Auto Related
- Internet Services
- Travel and Timeshares
- Health Care
Popular Imposter Schemes

The More Things Change, The More Things Remain the Same

- **Government Officials Scam**
  - “This is the IRS. You’ve failed to respond to our notices regarding your past due tax obligation.”
  - “This is the Social Security Administration. We’ve had to temporarily suspend your account.”
  - “Congratulations! You qualify for a free government grant worth tens of thousands of dollars.”

- **Tech Support Scam**
  - “We’ve detected a virus or other malware on your computer…”

- **Romance Scam**
  - “You sound perfect! I can’t wait to meet you. Oh, wouldn’t you know it? Something has come up, an emergency taking up all my short-term cash. We’ll have to postpone our meeting…unless you by chance might possibly be able to help?”

- **Family Emergency (Grandparents) Scam**
  - “Grandma? Grandpa? It’s me, your oldest grandchild. I’m in trouble and need your help. Please don’t tell Mom!”

- **Irregular or Fraudulent Activity**
  - Suspicious activity has resulted in your account being disabled or suspended. Your account is subject to a compulsory security update which you now need login to enable.
ID Fraud Again Nation’s Most Filed Complaint

A Leading Consumer Complaint for 20 Years Now

- Over 20% of ALL fraud complaints filed in 2019 were attributed to Identity Fraud in all its various forms.
- Total Identity Fraud reached $16.9 billion in 2019 an amount on par with four of the past five years though the highest dollar loss since 2013.
- Ironically, the identity fraud incident rate fell for the third year in a row to 5.1%. Though this represents a drop in the number of victims, the damage inflicted is more complex to prevent or remediate.
- New Accounts and Other Frauds soared more than 72%, nearly matching the total from the Top Three report types the previous year.
- Loan or Lease Fraud doubled in 2019 led by sharp increases in Business/Personal Loans, Auto Loan/Leases, and Student Loans.
- Phone or Utilities Fraud increased more than one-third, reaching its highest reported rate ever. Remains a growing area of serious concern.

Consumer Protection Recommendations

*Challenge is Changing Existing Behaviors including Technology Adoption*

- **Move to cashless payments including the use of digital of wallets** to manage in-store and online payments. The technology encrypts and tokenizes data so if stolen it is useless to criminals.

- **Adopt a zero trust contact policy.** Most consumers fail at questioning the authority and authenticity of a caller or message. Hang up and call your financial institution.

- **Use strong passwords or a password manager** to secure accounts. Vary passwords between accounts. Turn on two-factor authentication wherever possible.

- **Secure your devices.** Institute screen locks, avoid public Wi-Fi and/or use a VPN, and install anti-malware. Anti-malware protection is essential for all devices.

- **Place a security freeze on credit reports.** They’re free, made easy, and can be activated by phone, online, or mail. Freezes prevent anyone from accessing your credit and opening new accounts in your name.

- **Sign up for account alerts everywhere.** Banks, credit card issuers and brokerages provide their customers with the option to receive notifications of suspicious activity.

(Javelin Strategy & Research, 2020 Identity Fraud Study, April 2020.)
Move to Cashless Payments Underway

Question Becomes One of Adaptation and Training (and through whom)

How COVID-19 is accelerating the shift to a cashless society

PHILADELPHIA — Tom Ivory, the founder of the Baker Street Bread Co., in Philadelphia Chestnut Hill section, fought a valiant effort for years to retain his breads by imposing a minimum cash and purchase of 60. But more customers wanted to go cashless, and Ivory eventually relented and accepted plastic for any transaction, no matter how small. Almost 90% of the purchases at the cafe and store are now paid through credit cards or other electronic transfer — up from 10% just five years ago.

“I have to keep up with technology,” Ivory said. “To operate as just a cash business today is a suicide mission. You’re just not going to succeed.”

The coronavirus pandemic has accelerated the trend toward a cashless economy, financial experts say, fueled by the growth of e-commerce and the fear of handling paper money contaminated with COVID-19. During the lockdown, when Baker Street’s retail business was limited to takeout at the doorway and was conducted only by phone or online, nearly every transaction was cashless.

Southwest Airlines will no longer accept cash in the US

Put away those Franklin, Grants and Jacksons because Southwest Airlines is no longer accepting cash to buy tickets at airports in the U.S.

It’s part of the Dallas-based airline’s effort to cut back on handling paper currency that goes back more than a decade. As of July 1, Southwest stopped accepting cash payments at ticket counters to buy flights or to pay for upgrades and extra luggage.

Many companies and even national governments are encouraging people to stop using cash as a way to cut down on social contact and disease spread during the COVID-19 pandemic.
Move to Cashless Payments Underway

Begin by Leveraging Existing Card Relationships
Security Freeze
- Directive prohibiting the release of your credit report and credit score without your express authorization.
- Enact by phone, online, or by mail. If by mail, recommended that you do so by Certified Mail Return Receipt Requested.
- Do so with all 3 credit bureaus.
- No charge to freeze and/or temporarily thaw.
- In conjunction with monitoring your free credit report(s), you have the DIY equivalent of name brand identity theft protection.
- Note: You may want to consider a separate freeze with the National Consumer Telecommunications and Utilities Exchange (NCTUE). Available online or by mail.

*N.R.S. 8 2601 to 8 2615 Credit Report Protection Act. 8 2603. Security freeze; request
- - -

www.ProtectTheGoodLife.Nebraska.gov
Miracle Therapies and Cures
Miracle Therapies and Cures
FDA Warns Specifically About Stem Cell Therapies

- Researchers hope stem cells will one day be effective in the treatment of many medical conditions and diseases.

- Stem cells have been called everything from cure-alls to miracle treatments. Don’t believe the hype.

- Unscrupulous providers abound offering stem cell products that are both unapproved and unproven.

- The U.S. Food and Drug Administration has the authority to regulate stem cell products in the United States. It is increasing its oversight and enforcement to protect people from dishonest and unscrupulous stem cell clinics.
Miracle Therapies and Cures

Popularly Marketed Through Free Educational Seminars

TIREO OF LIVING V THE PAIN NEUROI

Maybe it’s time you start!

Millions Suffer from

Symptoms of Peripheral
• Burning
• Itching at night
• Cramps of the leg
• Changes in your skin
• Weakness or tingles
• Difficulty walking

TWO DAYS ONLY! FREE
Regenerative Medicine Seminar

Tuesday, January 14th
Holiday Inn Lincoln
2500 Tamarac Road
Lincoln, NE 68512
12PM and 6PM

Wednesday, January 15th
Fairfield Inn Lincoln
8465 Andorra Drive
Lincoln, NE 68526
12PM and 6PM

5 TOPICS WE’LL DISCUSS
1. Identifying your symptoms
2. Are you a stem cell candidate?
3. What is stem cell treatment like?

5 MILLIONS SUFFER FROM KNEE PAIN

MAYBE IT’S TIME TO THINK ABOUT
REGENERATIVE MEDICINE

Maybe we can help!

TWO DAYS ONLY! FREE
Regenerative Medicine Seminar

Tuesday, January 14th
Holiday Inn Lincoln
2500 Tamarac Road
Lincoln, NE 68512
12PM and 6PM

Wednesday, January 15th
Fairfield Inn Lincoln
8465 Andorra Drive
Lincoln, NE 68526
12PM and 6PM
Miracle Therapies and Cures

Suit: Deceptive and Misleading Statements to Consumers

Nebraska AG files lawsuit against Omaha stem cell clinic

Nebraska Attorney General Doug Peterson on Thursday filed a lawsuit against an Omaha-based stem cell clinic.

The lawsuit, filed in Douglas County District Court, alleges that the Regenerative Medicine & Anti-Aging Institute of Omaha and its owner, Travis and Emily Autur, made more than $6 million by making deceptive and misleading statements to consumers regarding the ability of their stem cell therapy to treat specific diseases and health conditions.

The lawsuit also alleges the clinic misrepresented that stem cell therapy is safe and that larger doses are more effective, without possessing the necessary evidence to make these types of claims.

It seeks to stop the clinic from making deceptive and misleading claims regarding its treatments, to refund money to patients and to pay an undetermined amount of civil penalties.

According to Peterson, the Auturs operate a network of companies across the country that advertise and sell stem cell therapy directly to consumers, with clinics also located in Arizona, Florida, Maine, Montana, Vermont, Virginia and Washington.

Through the Food and Drug Administration has noted the potential of stem cells to treat and cure some diseases and medical conditions, the therapy is not FDA-approved. In September, the FDA warned consumers that the unapproved use of stem cell treatments can be “particularly unsafe,” and may lead to adverse reactions, such as the failure of cells to function as expected and tumor growth.
Coronavirus Impact
COVID-19

Record Reports of Unreceived Goods, Ruined Plans

- **Online Shopping**
  - In Q2 more people reported problems with online shopping than in any other months on record.
  - More than half said they never got the items they ordered.
  - Predominant items ordered but not received: facemasks, sanitizer, toilet paper, thermometers, and gloves.

- **Travel and Vacations**
  - Lack of refunds, credits or vouchers.
  - Per the US Department of Transportation, airlines *must* offer refunds even when flight disruptions are outside their control.
  - For cruises, check ticket contract and more from Federal Maritime Commission.

- **Internet Information Services**
  - Malware and Scareware intended to damage or disable computers and systems or scare you into making some form of payment.
  - Phishing and Spoofing in an attempt to deceive the unsuspecting recipient into divulging personal information, e.g. passwords, card numbers, and bank account information.
COVID-19

Internet Information Services includes Scare Scam

This is your badluck. I'm aware 112214 is your password. More importantly, I know your secret and I've evidence of your secret. You do not know me and no one paid me to examine you.

It is just your bad luck that I came across your blunder. The truth is, I setup a malware on the adult vids (sexually graphic) and you visited this web site to experience fun (you know what I mean). While you were busy watching videos, your browser started working as a Rdp (Remote desktop) with a keylogger which provided me with access to your display screen and also web cam.

Right after that, my software obtained your entire contacts from messenger, social networks, as well as e-mail.

Next, I put in more time than I should've digging into your life and made a double display video. 1st part shows the video you had been viewing and 2nd part shows the view of your web cam (its you doing dirty things).

Honestly, I am willing to forget everything about you and allow you to move on with your daily life. And I am going to give you two options that will make it happen. The two choices to either ignore this letter, or simply pay me $3200. Let us examine above 2 options in more detail.

Option 1 is to ignore this mail. Let us see what will happen if you choose this path. I will certainly send out your video to all of your contacts including members of your family, co-workers, and so forth. It does't protect you from the humiliation your family will have to feel when friends and family discover your sordid videos from me.

Other Option is to make the payment of $3200. We will call this my "privacy charges". I will explain what happens if you opt this option. Your secret will remain your secret. I'll erase the recording immediately. You move on with your daily life as though none of this ever happened.

Now you may be thinking, "Let me call cops". Let me tell you, I've covered my steps to ensure this email cannot be linked returning to me and yes it will not steer clear of the evidence from destroying your lifetime. I am not seeking to steal all your savings. I am just looking to be paid for the time I put in investigating you. Let's hope you have decided to generate pretty much everything vanish entirely and pay me my confidentiality fee. You will make the payment via Bitcoins (if you don't know this, search "how to buy bitcoins" in google).

Amount to be paid: $3200
Bitcoin Address to Send: 19dqbw716B9*VW3X52zAxNjx2fGGGmD5bY (You must Delete * from this address and note it)

Explain no one what will you be transferring the bitcoin or they might not sell it to you. The method to have bitcoin can take a day or two so do not procrastinate.

I have a special pixel within this email, and right now I know that you have read this message. You have 24 hours to make the payment. If I do not get the Bitcoins, I will, no doubt send out your video recording to your contacts including members of your family, coworkers, and many others. You better come up with an excuse for friends and family before they find out. However, if I do get paid, I will erase the recording and all other proofs immediately. It's a non-negotiable offer, thus please don't waste my personal time and yours. Your time is running out. Please note that, my tracker will definitely be tracking what action you adopt when you're done reading this email. Frankly, if you search anything inappropriate I am going to send out your videotape to your members of your family, co-workers before your time ends.
COVID-19

Increase in Scam Calls Leads to Increased Benefit from Credit Bureaus

Credit reports are now free, every week

May 18, 2020
by Cathlin Tully
Attorney, Division of Privacy and Identity Protection

If you’re feeling anxious about your financial health during these uncertain times, you’re not alone. That’s why the three national credit reporting agencies are giving people weekly access to monitor their credit report — for free.

This is some helpful news, because staying on top of your credit report is one important tool to help manage your financial data. Your credit report has information about your credit history and payment history — information that lenders, creditors, and other businesses use when giving you loans or credit.
During these times of COVID-19, accessing your credit is important. That's why Equifax, Experian, and TransUnion are now offering free weekly online reports through April 2021.

Request your free credit reports

Spot identity theft early. Review your credit reports.

Suspicious activity or accounts you don't recognize can be signs of identity theft. Review your credit reports to catch problems early.

Learn more about Identity Theft

Your credit reports matter.

- Credit reports may affect your mortgage rates, credit card approvals, apartment requests, or even your job application.
- Reviewing credit reports helps you catch signs of identity theft early.

FREE Credit Reports. Federal law allows you to:

- Get a free copy of your credit report every 12 months from each credit reporting company.
- Ensure that the information on all of your credit reports is correct and up to date.
TRACED Act

Reduce Robocalls; Virtually Eliminate Caller ID “Spoofing;”
Requires Telcos to Adopt Call Authentication Framework

- Gives the Telcos and, by extension, law enforcement the ability to trace calls end-to-end regardless of network and call type.
- Requires voice providers to implement ‘an appropriate and effective call authentication framework’ within 18 months of the bill’s enactment. Enables carriers to verify that incoming calls are legitimate before they reach consumers’ phones.
- Extends window for the FCC to catch and take civil enforcement action against intentional violations to three years after a robocall is placed.
- Verizon and AT&T customers can enjoy a ‘sneak peak’ of a portion of the TRACED Act now available via ‘Call Filter’ and ‘Call Protect.’ Alerts customers to likely spam calls, reports unsolicited numbers, automatically blocks robocalls based on preferred level of risk.
TRACED Act

Reduce Robocalls; Virtually Eliminate Caller ID “Spoofing;” Requires Telcos to Adopt Call Authentication
For More Information, Contact:

Nebraska Department of Justice
Doug Peterson, Attorney General

Consumer Protection Division
2115 State Capitol Building
Lincoln, NE 68509

Phone: (402) 471-2682
My Direct Line: (402) 471-3878

Consumer Protection Hotline: (800) 727-6432
E-mail: ago.consumer@nebraska.gov
My e-mail: ryan.sothan@Nebraska.gov
Web Site: ProtectTheGoodLife.Nebraska.gov