PEOPLES STATE BANK
NEWS TO USE

September 2021

FRAUDS & SCAMS

New Data Shows FTC Received over 2.1 Million Fraud Reports from Consumers in 2020

The Federal Trade Commission received more than 2.1 million fraud reports from consumers in 2020, according to newly released data, with imposter scams remaining the most common type of fraud reported to the agency.

Online shopping was the second-most common fraud category reported by consumers, elevated by a surge of reports in the early days of the pandemic. The top five fraud categories also included internet services; prizes, sweepstakes and lotteries; and telephone and mobile services.

Consumers reported losing more than $3.3 billion to fraud in 2020, which was almost a 50% increase from 2019 where the loss was approximately $1.8 billion. Nearly $1.2 billion of losses reported last year were due to imposter scams, and online shopping accounted for about $246 million in reported losses from consumers.

Over a third of all consumers who filed a fraud report with the FTC , reported losing money, up from about 23% for the prior year.

The FTC's Consumer Sentinel Network is a database that receives reports directly from consumers as well as from federal, state and local law enforcement agencies, the BBB, industry members, and non-profit corporations. Twenty five state now contribute to Sentinel. Reports from around the country about consumer protection issues are a key source for FTC investigations that stop illegal activities, and when possible, provide refunds to consumers.

Sentinel received more than 4.7 million reports in 2020; these include the fraud reports detailed above, as well as identity theft reports and complaints related to other consumer issues, such as problems with credit bureaus and banks and lenders. In 2020, there were nearly twice as many reports of identity theft received through the FTC's IdentityTheft.gov website as there were in 2019. Source FTC

Inside this issue

Special points of interest

- Over 2.1 Million Fraud Reports in 2020
- How to Play It Safe When Looking for Love Online
- Identity Theft is not a joke
- Former IT professional robs victims of over $3.5 million

Telephone Scams

Telephone scammers try to steal your money or person information. Scams may come through phone calls from real people, robocalls, or text messages. Scammers often make fake promises, such as opportunities to buy products, invest your money, or receive free product trials. They may also offer you money through free grants and lotteries. Some scammers may call with threats of jail or lawsuits if you don't pay them.

Protect yourself from telephone scams:

DO: Register your phone number with the DO NOT CALL REGISTRY, be wary of callers claiming you''ve won a prize or vacation package, hang up on suspicious calls, be cautious of called ID. Scammers can change the phone number that shows up on your caller ID screen. This is called 'spoofing'.

DON'T: give in to pressure to take immediate action, don't say anything if a caller starts the call asking "Can you hear me?"—this is a common tactic for scammers to record you saying "yes." Scammers record your responses and use it as proof that you agreed to a purchase or credit card charge; don't' provide your credit card number, bank account information, or other personal information to a caller; don't send money if a caller tells you to wire money or pay with a prepaid debit card. Source: USA.gov

REPORT TELEPHONE SCAMS TO FEDERAL AGENCIES

How to Play it Safe When Looking for Love Online

Never send money or gifts to someone you haven't met in person—even if they send you money first.

Talk to someone you trust about this new love interest. It can be easy to miss things that don't add up. So pay attention if your friends or family are concerned.

Take it slowly. Ask questions and look for inconsistent answers.

Try a reverse-image search of the profile pictures. If they are associated with another name, or with details that don't match up, it's a scam.

What You Need To Know About Romance Scams

They say love hurts. With romance scams that's doubly true-hearts are broken and wallets are emptied. For three years in a row, people have reported losing more money on romance scams than on any other fraud type identified in Sentinel. In 2020, reported losses to romance scams reached a record $304 million, which is about a 50% increase from 2019. That averages out to a median dollar loss of $2,500 per individual. From 2016 to 2020, the number of reports nearly tripled, while the reported dollar losses increased more than 400%.

What happened in 2020 that caused the losses to spike? An obvious reason may be the pandemic limiting our ability to meet in person. But putting the pandemic aside, the number of people using an online dating service or app has also increased. And there are plenty of romance scammers ready to take advantage.

Scammers fabricate attractive online profiles to draw people in, often using pictures from the web and using made up names. Some go a step further and assume identities of real people. Once they make contact, they make up reasons not to meet in person. With the pandemic, this has been easier and inspired new twists to their stories. Many people reported that their so-called suitor claimed to be unable to travel due to the pandemic.

While many people report losing money on romance scams that start on dating apps, even more say they were targets on social media. Sooner or later these scammers always ask for money. They may say it's for a phone card to keep chatting, or might claim it is for a medical emergency. The stories are endless and intended to create a sense of urgency that pushes people to send money over and over again.

In 2020, reports of gift cards being used to send money to romance scammers increased by nearly 70%. Gift cards, along with wire transfers are the most frequently reported payment methods for romance scams. Source: FTC.gov

What To Know About Identity Theft

What Is Identity Theft?

Identity theft is when someone uses your personal or financial information without your permission. They might steal your name and address, credit card, or bank account numbers, Social Security number, or medical insurance account numbers. They could use them to: buy things with your credit cards, get new credit cards in your name, open a phone, electricity, or gas account in your name, steal your tax refund, use your health insurance to get medical care, or even pretend to be you if they are arrested.

How To Protect Yourself Against Identity Theft

Taking steps to protect your personal information can help you avoid identity theft. Here's what you can do to stay ahead of identity thieves. Protect documents that have personal information, ask questions before giving out your Social Security number, protect your information from scammers online and on your phone. Keep your financial records, and other documents that have personal information in a safe place. When you decide to get rid of these documents, shred them before you throw them away.

How To Know if Someone Stole Your Identity

Here's what you can do to detect identity theft. Track what bills you owe and when they are due, review your bills (charges for things you didn't buy could be a sign of identity theft, as can a new bill you didn't expect), check your bank account statement, get and review your credit reports.

If you discover that someone is misusing your personal information, go to IdentityTheft.gov to report and recover from identity theft.

Monitoring Services, Recovery Services and Identity Theft Insurance

Many companies sell identity theft protection services that may include credit monitoring, identity monitoring, identity recovery services, and identity theft insurance. These services also may be offered by your bank, credit card provider, employer's benefits program, or insurance company. Source: FTC

If you have any topics you would like to see covered in future newsletters, please email jwills@esbmi.bank.

Real Identity Theft Story

Kenneth Gibson is a 47-year old former IT professional from Nevada. Between 2012 and 2017, he was working for a large company where he had access to the Personally Identifiable information of thousands of employees and customers.

During this time, Gibson methodically stole data from his employer until the day he left the company. He then set up 8 computers to run an automatic script of the victim's information to open fraudulent accounts & transfer money. The automated system ran 24/7.

Over time, he opened up about 8,000 unauthorized PayPal accounts with the stolen identities. He would then apply for, and open, credit accounts linked to those PayPal accounts, withdrawing money via cash advances. The stolen money enabled Gibson and his family to live lavishly. He bought a boat, traveled extensively, and was alleged to be a frequent gambler.

Eventually, after he got tired of having to make multiple trips to the ATM to retrieve his stolen cash, Gibson requested that PayPal mail him a check. However, the name on one of these requested checks matched one of Gibson's victims. This is where law enforcement could make their move after 4 months on the case.

Gibson ultimately confessed, and the FBI was able to locate the computers he had operating in a leased office space.

On July 30, 2018, he was sentenced to 4 years in prison along with 3 years of supervised release and 100 hours of community service. In addition he must pay $1 million in restitution and forfeit assets to account for the $3.5 million stolen.

Source: Identityforce.com