Crime Prevention & Scam Awareness



MONROE TOWNSHIP POLICE DEPARTMENT







Part I: Crime Prevention



AT HOME

- If you have an alarm system: USE IT
- Keeps doors and windows locked (First and Second Floor Windows)
 - Utilize Deadbolt locks / Solid Core Doors
 - LOCK your interior garage door
 - DO NOT keep ladders accessible, ladders have been used to enter through the second stories of residences
 - LOCK your sheds
- Utilize lighting (Exterior and Interior) (Sensor Lights)
- Surveillance Video Equipment
 - Examples: Ring, Arlo, Nest, etc.
- Keep valuables out of sight
- If away, advise Police for a "Vacation Notice"
 - Police will provided additional patrols of area and check your residence while you are away (call volume permitting)
- Be aware of anything suspicious for both you and neighbors
- If you see something suspicious report immediately
- "IF YOU SEE SOMETHING, SAY SOMETHING!"





Voluntary Security Camera Registry



https://monroetwppolice.org/forms-permits/voluntary-camera-registry-program/

3 Municipal Plaza, Monroe Township, NJ 08831, Middleses County 722.521.8222 or 609.655.3250 / Contact Us	First Name *		
Monroe Township Police Department ***BONGS *** COMMITMENT ** ***PROTESSORMENT *** SERVICE ** ***PROTESSORMENT **** SERVICE ** ****PROTESSORMENT ***** ****PROTESSORMENT ****** ****PROTESSORMENT ******* *****PROTESSORMENT ******** ****************************			
Home Office of the Chief Departments Forms & Permits Information News & Events Contact	Address *		
Voluntary Security Camera Registry			
The Monroe Township Police Department is committed to a continuing partnership with our community. In always striving to expand that partnership, the Monroe Township Police Department is initiating the Security Camera Registry. This voluntary program will encourage both residents and business owners within the Township to register their home or business surveillance systems, which will increase safety and the reduction of crime, continuing to keep our community safe to the control of the control of the community safe to the control of the c	Email Address *		
During investigations, officers are often unaware of the various residences and businesses that have captured footage that is valuable to an investigation, which can lead to a successful and safe resolution.	Location of Camera System * Residence Business		
Benefits of this program include, expediting the retrieval of video footage as well as allowing officers quicker resolutions and obtaining pertinent information. Moreover, it reduces time in canvassing areas attempting to locate surveillance systems.	Are the images/video saved to a DVR or similar device? *		
If you are registered with this program and a crime occurs in your area, you may be contacted by a member of the Nonroe Township Police Department. This request may include examining the time frame in question and the recordings your system has. This will be arranged at your convenience and assistance provided to you in feeded to access recordings.	○ Yes ○ No		
Again, this program is 100% voluntary and all information kept confidential. Moreover, only law enforcement will view any footage provided by you.	Time period data is stored (i.e. 24 hours, 7 days, 30 days)		
This program is an additional useful tool which offers residents and business owners the opportunity to partner with the Monroe Township Police Department to continue to keep our Township safe. Please note that this program does not give police the ability to tap into any home or business surveillance feeds.			
How it Works	Description of areas recorded (i.e. street, front, side, par		
Registration – Please fill out the form below. It only takes a few minutes to complete.			
Confirmation - Once you complete your registration, a member of the Monroe Township Police Department will contact you to confirm your registration.	Is the camera system monitored by a third-party compar		
H Assistance is Needed - You will only be contacted if a criminal incident takes place in the area of your security cameras. Police may request a copy of the video / images. Again, assistance downloading these can be provided.	○ Yes ○ No		
This program continues the partnership with our residents and businesses to always keep Monroe Township safe. Any questions regarding this program, please contact Sgt. Ronald Breuer at 732-521-0222 ext. 152 or by email at cameras@monroetwppolice.org.	In the event your security camera captures footage need memorializing and/or downloading such data? *		
Terms and Conditions:	○ Yes ○ No		
1. Any video / images provided to the Monroe Township Police Department relating to criminal activity may be used as evidence.			
Footage provided is for Official Use Only by the Monroe Township Police Department or assisting agency.	Submit Registration		
Under no circumstances shall registrants construe that they are acting as an agent of the Police Department.	- Sabrite He Bast Selon		
4. If necessary, the Monroe Township Police Department will contact you utilizing the information you provided.			
5. You agree not to release any provided video/images to media or other outlet.			

Address *	
Email Address *	Phone Number *
Location of Camera System *	Recording period *
Residence Business	○ Motion Only ○ Continuous ○ Business Hours
Are the images/video saved to a DVR or similar device? * Yes No Time period data is stored (i.e. 24 hours, 7 days, 30 days) *	
Description of areas recorded (i.e. street, front, side, parking lo	ot) *
Is the camera system monitored by a third-party company? *	
○ Yes ○ No	
In the event your security camera captures footage needed to i memorializing and/or downloading such data? *	nvestigate a crime and/or ensure the safety of the community, are you proficient i
○ Yes ○ No	
Submit Registration	

Last Name



Crime Prevention



VEHICLE

- Keep vehicles locked (even when you are home)
- Keep valuables out of sight and out of mind
 - DO NOT keep wallets, purses, cash, checkbooks, credit cards, jewelry inside your vehicle
- DO NOT leave keys/key fobs and garage door openers inside the vehicle
- Most vehicle burglaries are to unlocked vehicles (easy access)
 - Burglars will walk around checking for unlocked vehicles!
- Most motor vehicle thefts occur because keys/key fobs are left in the vehicle!
- LOCK YOUR VEHICLES!



What to do if I am a Victim of MV Theft/Burglary



- Know your credit card information
 - Create logins for mobile apps and online portals
 - **KNOW YOUR LOGIN INFORMATION AND PASSWORDS**











- Be familiar with how to "LOCK YOUR CARD" and monitor recent transaction history
- If your credit/debit cards are stolen, CONTACT YOUR BANKING INSTITUIONS IMMEDIATELY TO CANCEL ALL STOLEN CREDIT/DEBIT CARDS! They will issue you new account numbers and cards.
- If you have EZPASS, create an online account/download mobile app so you can monitor travel activity/use in real time
- •If you have ONSTAR or vehicle tracking service in your vehicle, make sure you activate them and keep them up to date
 - These subscriptions cost money but can be very beneficial in recovering motor vehicles that have been stolen













According to the FBI: Home burglary every 15.4 seconds in U.S.



Distraction Burglaries



- Subject poses as contractor/public utility service/tree service
- Knocks on door and distracts victim by taking outside or another part of the house,
 - A second suspect enters the home and steals valuables
- Victim is often unaware of the crime until much later

Questions to think about...

- Did you make an appointment or is the visit unannounced?
 - Call company to verify they are legitimate/ask for ID
 - Call the police if you are unsure



Thefts in the Home



- In a large number of thefts within senior communities, Home Health Aids are the prime suspects.
 - Cleaning persons are also common
- Protect your valuables when aids or cleaning personnel are in the home
- DO NOT SHARE locations of jewelry and cash with anybody that you do not trust
- When hiring cleaning companies or health aides, DO YOUR RESEARCH!
 - Use a trusted and recommended service (READ REVIEWS!)
 - AVOID "Craigslist"





What are Identity Theft and Identity Fraud?



• The U.S. Department of Justice defines Identity Theft and Identity Fraud as:

"Terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."





How Do They Operate?



- Many operate internationally.
- Makes apprehension and investigation difficult.
- Many use leading questions and use wording to gain trust.
- Some use scare tactics, such as "you will be arrested."
- Most use masked IP addresses and/or fake telephone numbers.
 - There is computer technology that allows a caller to change their phone number.

Top 10 Fraud Categories

Rank	Category	# of Reports	% of Reporting \$ Loss	Total \$ Loss	Median \$ Loss
1	Imposter Scams	645,874	13%	\$576.0 Million	\$650
2	Online Shopping and Negative Reviews	177,642	68%	\$136.6 Million	\$110
3	Prizes, Sweepstakes and Lotteries	124,956	8%	\$121.8 Million	\$872
4	Telephone and Mobile Services	83,660	16%	\$20.9 Million	\$178
5	Internet Services	67,406	36%	\$53.6 Million	\$140
6	Travel, Vacations and Timeshare Plans	37,152	47%	\$105.9 Million	\$600
7	Foreign Money Offers and Fake Checks	31,171	26%	\$34.5 Million	\$1,500
8	Business and Job Opportunities	27,816	39%	\$85.8 Million	\$1,000
9	Health Care	27,800	45%	\$12.5 Million	\$149
10	Advance Payments for Credit Services	17,480	67%	\$22.7 Million	\$382

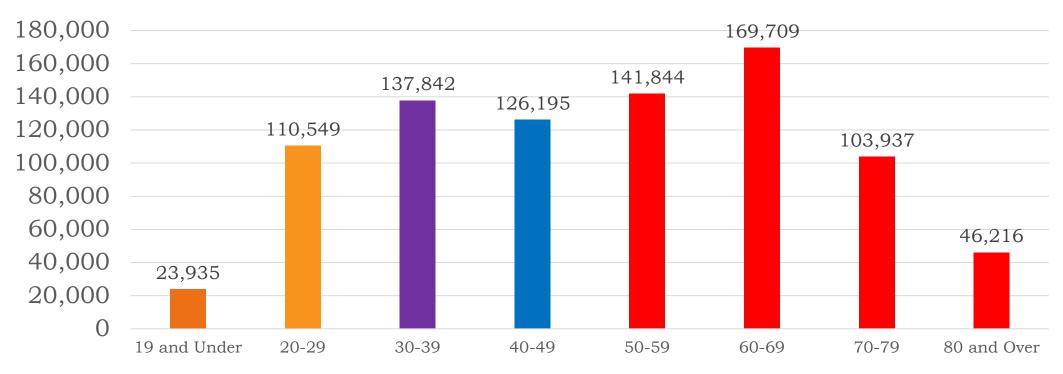


Who it impacts most?



(FTC Consumer Sentinel Network)

of Reports in 2019



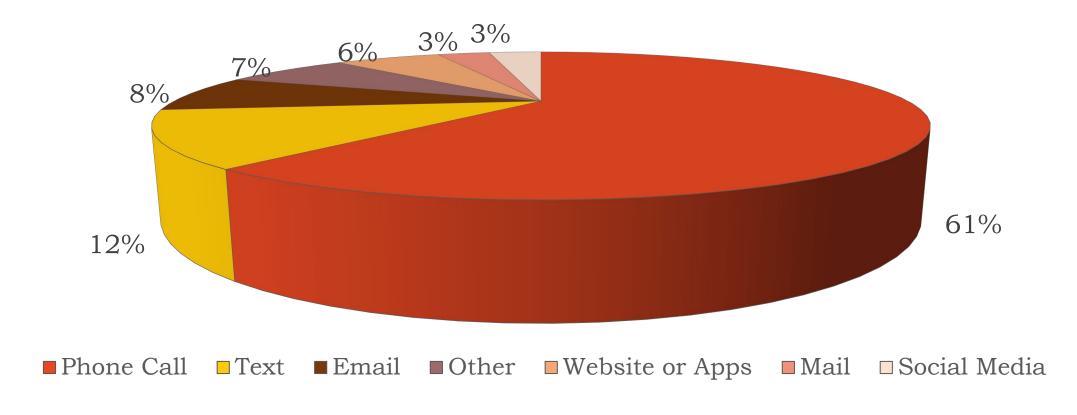
* Approx. 51% of Monroe Twp. is over the age of 55*



Fraud Reports by Contact Method



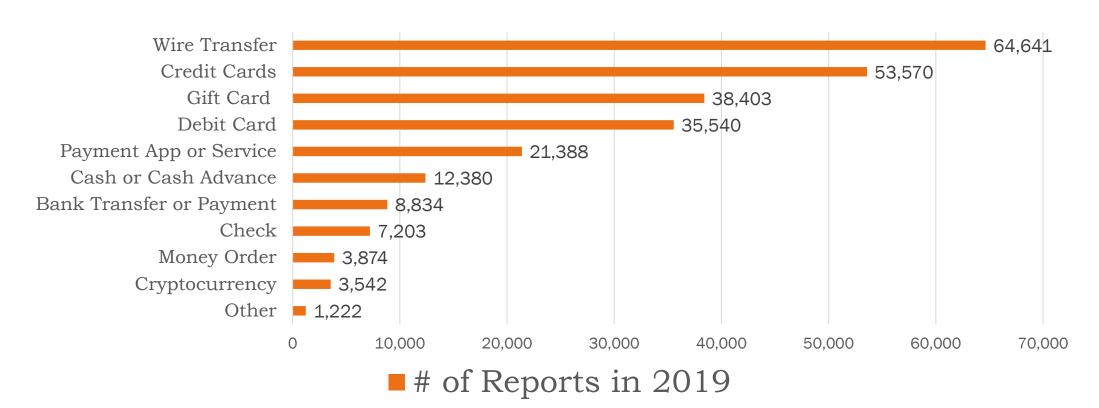
(FTC Consumer Sentinel Network)





Fraud Reports by Payment Method





(FTC Consumer Sentinel Network)



What is the cost?

(FTC Consumer Sentinel Network)



- In 2019, there were 1,723,234 reported identity frauds nationwide.
 - Out of those, 23% reported a monetary loss.
- Those 23%, contributed to a total net loss of

\$1,862,000,000

• That is a \$293 million dollar increase from 2018.



Types of Identity Theft/Fraud



- IRS Scams
- Lottery/Sweepstakes Scam
- Grandchild/Family Arrest Scam
- Romance Scam
- Vacation Scam
- Home Improvement Scam
- Mortgage/Debt Relief Scam
- Charity Scam

- "Can you hear me now?" Scam
- Secret/Mystery Shopper Scam
- Email Compromise
- •FBI Lock Screen
- •Computer Repair Scam
- Phishing Websites/E-mails
- ATM Skimmers



Grandchild/Family Arrest Scam



- The caller will pretend to be a family member and will ask leading questions in an attempt to assume a family member's identity.
 - The caller might also disguise their voice in an attempt to imitate a family member.
- Once they have assumed an identity, the caller will claim that they have been arrested and that they need you to pay their bail.
- The caller will try to legitimize the court system process as much as possible.
 - The individual on the phone could also advise the victim that a courier of the court will report to your residence to pick up cash bail.
 - The courier could possibly provide the victim with a receipt for the payment and notate a fraudulent case number.
 - The caller on the phone could also request the victim go to FedEx and/or UPS to send them packages with cash payment.
- •Once again, the caller could request payment via Cash, Gift Cards, Western Union, or Money Order.
 - DO NOT GIVE CASH TO AN UNKNOWN INDIVIDUAL AND DO NOT SEND CASH VIA MAIL.
 - Pay attention to the requested payment method.
 - BE SKEPTICAL



IRS Scams



- Very common during tax season.
- A person purporting to be an IRS agent will contact an individual and claim that he/she is an "agent" with the IRS and that the individual has any of the following:
 - unclaimed taxes
 - multiple social security numbers
 - a warrant out for their arrest
- If the individual does not pay the amount owed, a warrant will be issued for his/her arrest.
- The payment will be requested immediately and in a specific way such as gift cards and/or money transfer.
- "The IRS does not initiate contact with taxpayers e-mail to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels." (IRS.GOV)





IRS/False Tax Return



- Thieves will use your personal information to file a completely separate tax return in your name.
- You will then be unable to file your own tax return.
- The thief ultimately obtains your identity and uses it.
- Very prevalent today, especially with COVID refund payments.
- If you notice any fraudulent transactions in related to your tax return, you must contact the IRS immediately.



Lottery/Sweepstakes Scam



- The caller will purport to be an "agent," who is calling to notify an individual that he/she won a large sum of money.
- Notification can also come in the form of an e-mail, or letter.
- The ploy is that you **HAVE** to pay the taxes/fees before you are able to collect your winnings.
- The "agent" will request the payment for the taxes/fees via gift cards, money order, and/or wire transfer.



CONGRATULATIONS!!

Your Email was selected in Powerball Lottery Draw with the sum of 1.5million dollars. Kindly send your Full Name, Address and Phone Number for claims.

Yours Sincerely Mr. James Hodges Head Of Operations



Lottery Scam Example



- A resident of Monroe, Victim #1, was contacted via telephone by an individual in Jamaica, who stated that she had won the lottery.
 - Before Victim #1 could collect her "winnings," she had to wire the individual money to cover the taxes.
- Over the course of the next few months, Victim #1 wired a total of \$248,000.00 to this individual.
- During this time period, Victim #1 contacted the Monroe Township Police Department once because she was concerned when the individual stated that he was going to visit her at her residence.
- The Detective Bureau at the Monroe Township Police Department immediately opened an investigation in this matter and even set up a sting operation at Victim #1's residence, in the event that this individual showed up.
- Monroe Township Police Department advised Victim #1 that she was a victim of a scam and to avoid all future communication with this individual.
 - But, the individual developed such a strong relationship with Victim #1, that she continued to maintain contact because she was convinced that she would eventually receive her "winnings."
- Ultimately, Victim #1 realized that her life savings had dwindled and she sadly took her own life.



Romance Scams



- Scammers develop a relationship with an individual via direct messaging applications such as: Kik, WhatsApp, Facebook Messenger, Instagram, and Twitter.
- The individual will profess their love quickly, without ever meeting in person.
- The individual will then make claims that they need money for medications, travel, or other emergencies.

Signs of a Scam



Professes love quickly.

Claims to be from the U.S., but is overseas for business or military service.



Asks for money, and lures you off the dating site.



Claims to need money

— for emergencies,
hospital bills, or travel.

Plans to visit, but can't because of an emergency.



Vacation Scam



- Initiated by an automated telephone call, where the caller states that you have been "selected" for a **FREE VACATION**.
- Upon a call back, the caller will request personal information and money for fees.
- Before you can receive your "voucher," the caller will request money to cover expenses and fees.





Home Improvement Scam



IN-PERSON SCAM.

- Starts with a phone call or a solicitor going door to door.
- The contractor will attempt to sell you home improvements and they will require a down payment before they start working.
 - They may even provide an official looking contract.
- After they have their money, they will either never show up, or they will start the job and never finish it.
 - They may even damage your home in the process.

HOW TO AVOID:

- DO YOUR HOMEWORK.
- MAKE SURE TO HIRE LICENSED CONTRACTORS.
- AVOID MAKING LARGE DEPOSITS.



Mortgage/Debt Relief Scam



- Initiated by an automated telephone call, or an e-mail.
- The caller will claim that they will work with your lenders (banks) to significantly lower your payments.
 - Loan modifications or debt relief.
- The caller will ask for your personal and financial information before they "begin."
- After your have divulged your information, they will either disappear or they will claim to need a deposit.
- This could cost you thousands and could continue for an extended period of time.



Charity Scam



- The caller will identify themselves as a charity and will request a monetary donation.
 - This is very common after a natural disaster.
- The caller will attempt to gain sympathy from you and guilt you into donating.
- Before you donate any amount, DO YOUR HOMEWORK.
- Side note:
 - MONROE TOWNSHIP PBA/ NJ STATE PBA DOES NOT MAKE PHONE CALLS TO REQUEST DONATIONS.
 - THESE ARE SCAMS!





"Can You Hear Me Now" Scam



- A new and popular scam.
 - You might not even realize that you have been scammed.
- You will receive a telephone call from an unknown number, and the caller will ask "Can you hear me now?"
 - The caller might repeat this question many times.
- The caller is prompting you into saying "Yes."
 - They will record your response and use this recording for unauthorized purchases.
- BEST COURSE OF ACTION TO AVOID THIS SCAM IS TO EITHER NOT ANSWER TELEPHONE NUMBERS THAT YOU DO NOT RECOGNIZE, OR TO SIMPLY HANG UP.





Secret/Mystery Shopper Scam



- Initiated via e-mail, or letter in the mail.
- Will request an individual use the guise of a "customer" to evaluate the customer service and/or the gift card purchasing procedures at a variety of stores.
- The individual will be supplied with explicit instructions to imitate authenticity.
 - The instructions may even include a seemingly legitimate letterhead, or use a company name.
 - May promise a salary if the "assignment" is completed.
- The individual may receive a check and/or request personal information.
 - In the situations where a check is supplied, the check will bounce soon after it is deposited and you will be left with the charges.
- BE SKEPTICAL IF YOU ARE EVER ASKED FOR PAYMENT IN THE FORM OF A GIFT CARD.



E-Mail Compromise Scam



- The actor will hack into the victim's email.
- From there, the actor will change one character in the domain.
 - All future correspondence via this e-mail will be forwarded to the actor's email.
- This is common with businesses and large organizations.
- Example:

johndoe@email.com

johndoe@emaiil.com



FBI Lock Screen Scam



- A pop-up ad will suddenly appear and claim that the FBI has locked your computer.
- This ransomware virus is implanted on your device via the actor.
- The ad will claim that you will have to pay a fee (usually \$500.00 plus), to "unlock" your computer.

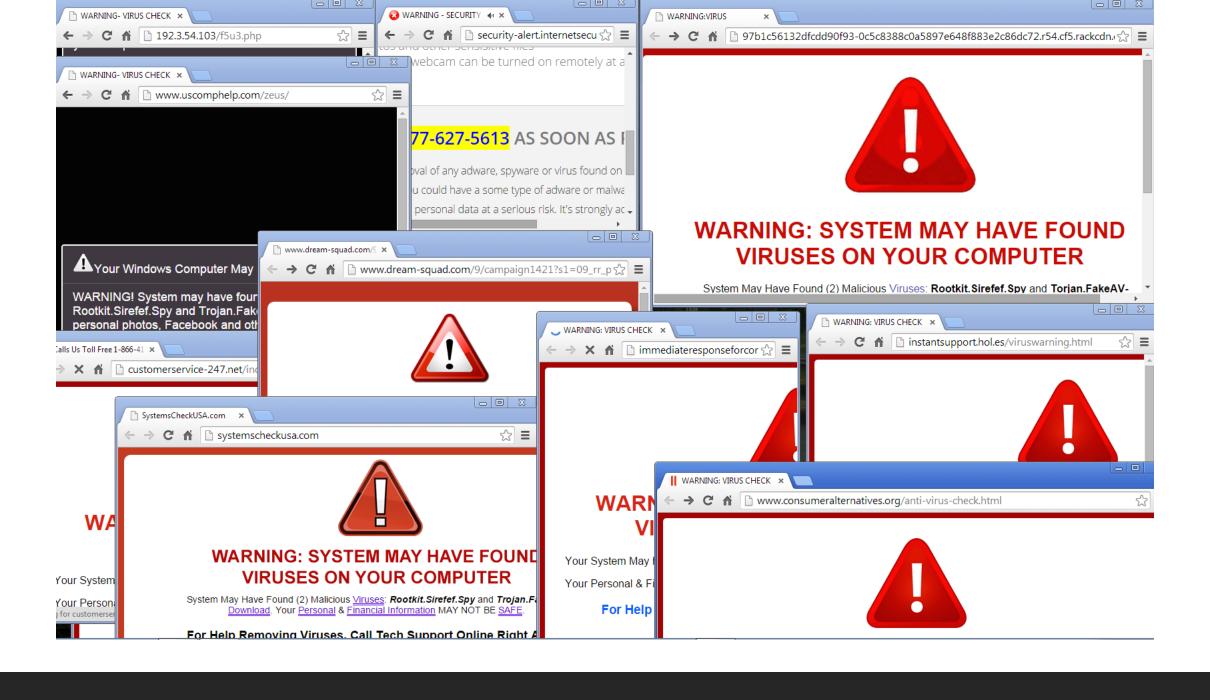




Computer Repair Scam



- A pop-up ad will suddenly appear and claim that your device has been infected with a virus.
- Then you will either be instructed to click on a link to take action, or you may receive an e-mail and/or a telephone call about the "virus."
 - The caller may claim to be an expert in malware and antivirus software.
 - The caller may also request payment for services.
- They will then walk you through the steps for them to gain control of your device to "fix" the problem.
 - ONCE CONTROL IS GAINED, THE INFORMATION ON YOUR COMPUTER IS COMPROMISED.





Phishing Scam



- The individual is fooled to click on a link onto what they believe is a legitimate website, but in reality the website is a fake.
 - For Example:
 - Banking websites
 - Retail Stores
 - Bill Payment Services
- If the individual uses their login credentials on these fake websites, their credentials are then compromised.
- The hacker will then have full access to your personal accounts.
- This can be avoided by double checking URL's and ensuring that your are utilizing trusted websites.



ATM Skimmers

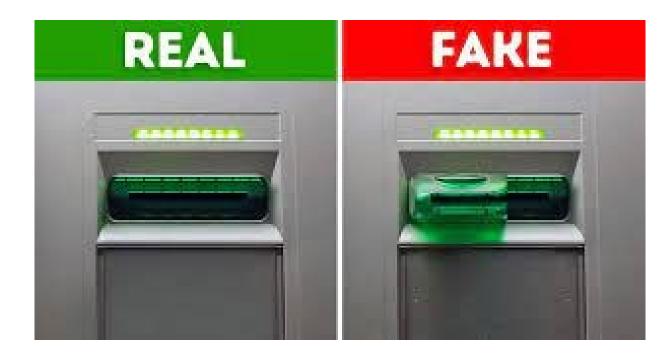


- Micro card readers and cameras capture your card number and pin.
- Card may be "cloned," or the account accessed can be compromised.
- Micro card readers can be placed on almost any ATM, or it can be hardwired to the terminal.
- Nearly impossible to see on the ATM.
- Be skeptical if you see something odd on the ATM and ONLY use trusted ATM's.











- Thieves can steal your identity and use it for medical insurance claims/unemployment claims.
 - Situations like this, involve an individual purporting to be someone they are not to be able to receive certain benefits and/or a monetary gain.
- This could lead to unexpected out of pocket expenses, higher insurance rates, tax implications, and inaccurate medical records.
- You MUST always check "Explanation of Benefits" (EOB).
- Any discrepancies, or unusual deductions immediately contact your insurance company and physician.



Social Security Theft



- With a stolen Social Security number, an identity thief can:
 - Assume your identity.
 - Or, use your Social Security number and create a different name and biological information in a combination, thus creating a completely new identity.
- Social Security cards have little to no modern security features, making false duplication **EASY**.
- Protect the physical Social Security card and be wary to whom you share that information with.





How it impacts us in Monroe...



• In Monroe Township alone, frauds have increased 267.03% since 2011.

• In 2011, 185 frauds were reported and in 2019, 679 frauds were

reported.





Example of a Scenario



Susan receives a phone call from an unknown telephone number and the caller introduces himself/herself as law enforcement official and advises Susan that she has multiple warrants out for her arrest. The caller states that Susan's social security number has been used to open multiple bank accounts throughout the country and these accounts have a \$300,000.00 outstanding balance.

The caller then advises Susan that if she does not pay off her debt, that federal marshals will show up at her residence with a warrant for her arrest.

Susan is understandably nervous and asks how she could avoid arrest.

The caller then advises Susan to visit the local Walgreens on Applegarth Road to purchase gift cards to serve as payment for her debt.

Susan then leaves for Walgreens and purchases \$2,000 worth of gift Target cards. When she returns home, she scratches off the barcode on the reverse side of the gift card and reads off the gift card numbers to the caller.

Unfortunately, Susan has just become a victim of identity theft/identity fraud.



How to avoid Identity Theft/Identity Fraud?



1. Spot Imposters

• Scammers often pretend to be someone you trust, like a family member, a charity, or a company you do business with. Do not send money or give out personal information in response to an unexpected request- whether it comes as a text, a phone call or an email.

2. Do Online Searches

- Do your research before you say "yes" to anything.
- Type a company or product name into a search engine to see reviews and/or prior scam complaints.
- Type the related phone number(s) into a search engine to see if they are related to prior scams.

3. Don't Believe Your Caller ID

- Technology makes it easy for scammers to fake caller ID information, so the name and telephone number you see aren't always real.
- If someone calls asking for money and/or personal information, HANG UP.
- If it is that important, the caller will leave a voicemail.

(Obtained from ftc.gov/scams)



How to avoid Identity Theft/Identity Fraud?



4. <u>Don't Pay Upfront for a Promise</u>

- Someone might ask you to pay in advance for things like debt relief, credit and loan offers, mortgage assistance, a job, or even a vacation.
- If you do, they will probably take the money and disappear.

5. Consider How You Pay

- Credit cards have significant fraud protection built in, but some payment methods do not.
- For example, wiring money through Western Union and MoneyGram is risky because it is nearly impossible to get your money back.
- Government Offices, IRS, Law Enforcement Agencies, Tech Services, etc. will **NEVER** ask for payment in gift cards.

6. Talk to Someone

• Before you give up your money or personal information, talk to someone you trust.

(Obtained from ftc.gov/scams)



How to avoid Identity Theft/Identity Fraud?



7. Hang Up on Robocalls

- If you answer the phone and hear a recorded sales pitch, hang up and report it to the Federal Trade Commission (www.ftc.gov or by calling 1-877-382-4357).
- These calls are illegal, HANG UP.

8. <u>Be Skeptical about Free Trial Offers</u>

• Do your research and always review your monthly statements.

9. Do Not Deposit a Check and Wire Money Back

- Similar to money laundering.
- Banks must make deposited funds available within days, but if the check is fake, you will responsible for repaying the bank.
- 10. Sign Up for Free Scam Alerts from the FTC at ftc.gov/scams.



How to Avoid Spam Calls



- 1. Register your mobile, or home phone on the National Do Not Call Registry.
- This resource gives you the choice about whether to receive telemarketing calls.
- Registrations NEVER expire.
- Easy to sign up and takes just a few minutes.
- 2. Activate built-in security features on your smart phone.
- iOS 14 allows Apple users to silence calls that are identified by their service provider as being potential spam, or fraud.
 - From your home screen, tap Settings
 - Tap Phone
 - Tap Call Blocking and Identification
 - Tap the Silence Junk Callers switch ON
- Non-Apple users, check the Settings app on your phone for similar security settings, and/or contact your service provider with questions about silencing spam calls.



Who to report it to?



- Internet Scams are to be reported by the victim to the FBI online by going to <u>www.IC3.gov</u>.
- **Mail Scams** are to be reported by the victim to the USPS online by going to https://www.uspis.gov/report/ or by calling 1-800-275-8777.
- **Phone Scams** are to be reported by the victim to the Federal Trade Commission by going to <u>www.ftc.gov</u> or by calling 1-877-382-4357.
 - If the Victim divulged personal information to the caller, they are at to call 1-877-438-4338.
 - If bank account or credit card information was provided to the caller, notify the bank and/or credit card company as well.
- **IRS Scams** are to be reported by the victim to the Treasury Inspector General by going to www.treasury.gov/tigta/.
- •If you incur a monetary loss as a result of a scam, you must report it to **The Monroe Township Police Department in addition to all of the above**



N.C.I.C. Theft File



(Information obtained from FBI.gov)

What is it?

- •As of April 2005, an Identity Theft File has been developed in the National Crime Information Center (NCIC) in the Criminal Justice Information Services (CJIS) Division.
- •An FBI run database that compiles information to assist law enforcement agencies throughout the country in investigating and identifying identity theft/identity fraud.

Purpose:

•"The file will serve as a means for law enforcement to "flag" stolen identities and identify imposters encountered by law enforcement personnel."

How it works:

•This file will consist of voluntary information submitted by a victim of identity theft/identity fraud. The file consists of the the victim's full name, date of birth, social security number, identifiable characteristics, type of identity theft/identity fraud, and a personalized password created by the victim at the time of the police report.



N.C.I.C. Theft File cont.



(Information obtained from FBI.gov)

Who will have access to my information?

• The Identity Theft file will be available to all local, state, and federal agencies that have access to N.C.I.C.

How long is my information stored in the N.C.I.C. database?

- The Identity Theft file will be stored for a 5 year time period, but the victim has the option to withdraw their file from the N.C.I.C. database at any time.
- If the victim chooses to withdraw their file from the N.C.I.C. database, a written request to the entering agency is required.



Additional Resources



- For further information please visit monroetwppolice.org/information/crime-prevention/
 - Full PowerPoint along with Video Examples of most prevalent identity thefts/scams

