Investigator Matthew Britten

- New York State Police Bureau of Criminal Investigations (BCI)
- Investigator for almost 10 years
- 16 plus years as a New York State Trooper
- I have worked in the Clifton Park barracks for over 9 years.
- Well versed in Fraud and Identity Theft

FRAUD AND IDENTITY THEFT SCAMS PREVENTION

Elder fraud

- ✓ **Seniors aged 60 and older account for about 15 percent of the population in the United States**
- ✓ **According to some estimates, seniors comprise 30 percent of fraud victims**

Why are seniors targeted?

- ✓ **Seniors can be more vulnerable**
- ✓ **Some seniors are very trusting**
- ✓ **Older people often believe the pitches they hear**
- ✓ **Seniors have trouble spotting fraud**
- ✓ **Older victims find it difficult to end unwanted telemarketing calls**
- ✓ **Seniors are often reluctant to seek advice about financial matters**

Generalizations about seniors

- ✓ **Have a lot of assets**
- ✓ **Open to claims of quick profits to bolster their retirement savings**
- ✓ **Have trouble remembering things**
- ✓ **Isolated socially and desire company**
- ✓ **Have strong values about politeness in dealing with others**
- ✓ **Often avoid reporting that they've been scammed**

Another way to reduce unwanted phone calls.

What is Anonymous Call Rejection and how does it work?
Anonymous Call Rejection allows you to block unwanted calls from people who choose not to display their Caller ID information.

Anonymous Call Rejection is included in the price of your TWC Phone plan.

To use Anonymous Call Rejection, dial *77 to activate and wait for the confirmation tone. All unidentified calls will be rejected.

Phishing

- ✓ **A term is used for emails that claim to be from your bank, a reputable business or a government agency**
- ✓ **Criminals ask for personal information such as Social Security numbers or account numbers to steal funds and/or steal identities**

Warning signs of fraud

- ✓ **Be suspicious if you hear**
  - **You've won a prize or free gift**
  - **You've been selected to receive a special offer**
  - **You must act immediately or lose out**
  - **You must pay for shipping your prize or free gift**
  - **Give us your credit card number and expiration date to verify that you are a credit cardholder**

More warning signs of fraud

- ✓ **You're asked for personal information**
- ✓ **You're asked to donate to an agency whose name sounds like a well known charity**
- ✓ **You're one of only a chosen few to receive this offer**
- ✓ **A courier will come to your home to get your payment**

Protect your assets

- ✓ **Never**
  - **reveal your financial information to someone who calls you on the phone**
  - **allow strangers to come into your home**
  - **believe that a stranger will use your money for a good purpose**
  - **assign power of attorney to people you don’t know very well**
  - **sign contracts that have any blank lines in them**

ID theft

- ✓ **ID theft criminals use your personal information to apply for credit or government benefits**
  - **Your name**
  - **Your birth date**
  - **Your Social Security number**
  - **Your address**
  - **Your bank account or credit card numbers**

Caretaker crimes

- ✓ **Be alert for caregivers**
  - **who try to isolate you from your friends and family**
  - **who ask about your will and investments**
  - **who ask to be given power of attorney**
  - **who try to dominate or influence you**
- ✓ **Tell family members or call adult protective services**

Protect your property and assets

- ✓ **Financial exploitation is often committed by a person that is trusted by the victim**
- ✓ **Keep all important financial documents under lock and key in your home**
- ✓ **Store valuables in a bank safe deposit box**

Fake cashier's checks

- ✓ Crooks scan want ads looking for victims
- ✓ Answer ads and offer to pay by "cashier's check" for more than the sales price
- ✓ Ask you to wire the remainder of the money back to them or to give the extra money and the merchandise to a "shipper"
- ✓ Check turns out to be a fake and you lose the merchandise and the money

Overpayment – Counterfeit Check

With overpayment scams, fraudsters play the role of buyer and target consumers selling a service or product. The “buyer” sends the seller a legitimate-looking check, usually drawn on a well-known bank, for an amount higher than the agreed-upon price. They contact an explanation for this overpayment and instruct the seller to deposit the check and wire back the excess funds. Weeks later, the victim learns the check is fake, but is still on the hook to pay the bank back for any money withdrawn.

Rental property – Scam

Sophisticated scammers use the Internet, and particularly free classified websites, to prey on unsuspecting real estate victims. Rental property scams generally happen in one of two ways:
1. Renters are looking for a house or an apartment to lease and get scammed by an "owner." Victims come across a place in a great area, at a great price. The advertisement looks legitimate so they start communicating with the "owner," generally by email. The owner says the place is theirs if they wire money to cover an application fee, security deposit, etc. They wire

the money, and then never hear from the “owner” again.

2. Owners are renting out their house or apartment and get scammed by a “renter.” “Renters” contact victims, generally by email, and express interest in renting the house or apartment. Scammers send a check for the deposit but then cancel the deal. Victims wire the money back only to find out the check was a fake.

The “owner” actually has taken photo’s from legitimate websites. Zillow/Realtor.com

Travel scams

- ✓ **Before buying travel packages**
  - **Get the offer in writing**
  - **Check to see if the company is legitimate:**
    - **the Better Business Bureau**
    - **state attorney general's office**
    - **your local consumer protection agency**
    - **the U.S. Dept. of Transportation (DOT) at 202-366-2396**
  - **Always use a credit card to purchase travel**

Contractor fraud

- ✓ **Traveling contractors are rarely licensed or insured and often take a large cash payment up front**
- ✓ **They will probably never return to complete the work**
- ✓ **When you need a contractor for a home improvement job, get at least 3 estimates from reputable local contractors**

The most important thing to remember when looking for a reputable contractor: it's best to work with someone who has a history of good performance and good service. As with other types of referrals, your friends, neighbors and coworkers may know where to start. Ask around and do some research before you even spend time interviewing a contractor.

1.NEVER EVER PAY CASH! Pay your contractor by check or credit card so you have documentation and recourse should you need it. Do not give your debit card number.

2.Never pay for the job upfront or you may never see this “contractor” again. No reputable contractor will ask for most—or all—of his payment immediately. Most legitimate contractors only bill AFTER the job is done to your satisfaction.

Charities

- ✓ **‘Sound-alike’ names can be tricky**
- ✓ **Nonprofit and charitable groups must file IRS Form 990**
  - **Check 990s at GuideStar www.guidestar.org**
- ✓ **Before you donate, check to see if the charity is legitimate**
  - **www.charitywatch.org: 773-529-2300**

Get Paid to Shop Get Paid to Shop

You're offered a job to be a mystery shopper. Your "boss" sends you a check to cover the cost of the items you'll buy at the store you are evaluating. When you get the check the money is for more than it should be. The fraudster will ask you to wire the extra back to him. The check turns out to be a fake and once you've sent the money, there's no way to recover the funds.

Work-at-home scams

- ✓ **Do not respond—these offers are scams**
- ✓ **If you respond, you'll be asked to pay for supplies upfront**
- ✓ **Might ask you for your credit card, bank account or Social Security numbers for fraudulent uses**
- ✓ **Package Forwarding - The scam victims then receive the package, along with**

instructions on where to send the package next. After re-mailing the stolen goods — with your own money — you'll supposedly get a check for your services. Sometimes payment comes, and sometimes it doesn't. In either event, it's usually the police who show up wanting to know why you received stolen goods at their own address. Try explaining that one.

Telemarketing Sales Rule

- ✓ **No sales calls between 9 p.m. and 8 a.m.**
- ✓ **Must tell you what company they are calling from and that they are selling something**
- ✓ **No purchase needed to enter or win promotions, prizes or contests**
- ✓ **Cannot ask for advance payment for credit services**
- ✓ **No abusive or obscene language, threats or intimidation**
- ✓ **Goods or services cannot be misrepresented or exaggerated**
- ✓ **Telemarketers cannot withdraw a payment from your checking account without your written or recorded oral permission**

Avoid investment fraud

- ✓ **Do your homework about investments**
- ✓ **If you are targeted with questionable investment offers, notify the U.S. Securities and Exchange Commission (SEC)**
- ✓ **Call your state attorney general's office to file a complaint**

Pyramid schemes

- ✓ **Promoters recruit investors and use them to recruit more investors**
- ✓ **Investors are promised a fabulous return, such as 20% a year**
- ✓ **Some investors might receive money but eventually, the organizers run off with everything**
- ✓ **Pyramid schemes are often called “investment clubs” or “gifting circles,” and can involve the sale of products or distributorships**

Video

- 42:58 – 44:30

Credit card fraud

- ✓ **Keep an eye on your credit cards at all times**
- ✓ **Unscrupulous employees might steal the information from your credit card and use it to make counterfeit cards**
- ✓ **Shred all credit card statements, receipts and solicitations before throwing them away**

Credit card loss protection

- ✓ **Don’t buy the worthless credit card loss protection and insurance programs sold by telemarketers**
- ✓ **Your liability for unauthorized credit card charges is limited to $50**

Dumpster diving

- ✓ **Crooks look in garbage cans and elsewhere for discarded credit card statements and receipts to obtain the card numbers**
- ✓ **These papers can be used to steal your identity and set up credit in your name**
- ✓ **Shred sensitive papers**

If you become a victim...

- ✓ **Call the police**
  - **You may need a police report to help you prove that you were a victim**
- ✓ **Contact your state and local law enforcement agencies such as your district attorney's office or the state attorney general**

Your Relative is in Trouble

You get a phone call from a person claiming to be a friend or family member in trouble who needs cash quickly. This is the "person in need scam" also referred to as the "grandparent scam." Don't send the money unless you can verify with your friend or family member that the story is true

Grand Parent Scam

- The "Grand Parent Scam" has been occurring nationally for several years now. The victim, usually an elderly person, male or female receives a call from a person over seas claiming to be their Grandson or someone associated with him or her in some way. The calls are random cold call, fishing for information from unsuspecting elderly victims. The scam starts out by trying to engage the elderly victim in a story of some kind of trouble involving their grandson - such as a motor vehicle accident, arrest, or injury. The key the suspect on the other end of the line is to convince the elderly victim that this situation is

- legitimate; their Grandson is in some kind of trouble and needs immediate money. The caller convinces the victim to wire money via Western Union or Money Gram. Now they are also having the victims purchase Green Dot / Money Pak cards. The caller also instructs the victim not to reach out to other family members advising them of the current situation, to aid in the success of the scam. The elderly victim that does fall for this scam, usually goes directly to the bank, withdraws the money and wires the money or more recently now with Green Dot/ Money Pak cards. Its only several days later when they haven't heard from their Grandson,

- they finally put the pieces together, talk to other family members or even their Grandson, they realize they've been a victim of a scam.
- Furthermore the suspect will continue to evolve the scam once money is initially received, some victims will continue to send money multiple times.
- When in doubt, and BEFORE YOU SEND ANY MONEY, contact the State Department's Office of Overseas Citizens Services (OCS) at 1-888-407-4747. We will help you verify whether the situation is legitimate or a scam!

Online Dating/Relationship Scam

- The relationship scam starts simply: A man and woman meet on the Internet. The relationship progresses: They email, talk on the phone, and trade pictures. And, finally, they make plans to meet, and even to get married. As the relationship gets stronger, things start to change. The man asks the woman to wire him money; he needs bus fare to visit a sick uncle.

- The first wire transfer is small but the requests keep coming and growing—his daughter needs emergency surgery, he needs airfare to come for a visit, etc. The payback promises are empty; the money's gone, and so is he or she.

- Online dating CAN BE is a great way to meet people. It's also a playground for liars and scammers. So, be careful who you invest your time and emotions in. Take a good long look at the profiles of anyone who messages you. Ask personal questions about where they live and what they do and research to see if what they say matches with reality. Watch out for people who fall head over heels for you after a few chats. Never give anyone money and ditch anyone who asks for it. Ask for photos and lots of them and anything else that you need to prove the person you are talking to is trust

- worthy. If this person is interested and honest they will have no problem providing what you ask for. Use these tips and If you are talking with a scammer, you will soon find out.

- The IRS is Looking for You

- You get a phone call claiming you owe "back taxes" and will be arrested if you don't transfer money fast. This is a scam. Remember, the IRS typically contacts people by mail, not by phone. The agency will never ask for payments via a wire transfer or ask for a credit card number over the phone.

IRS SCAM

- The IRS continues to warn consumers to guard against scam phone calls from thieves intent on stealing their money or their identity. Criminals pose as the IRS to trick victims out of their money or personal information. Here are several tips to help you avoid being a victim of these scams:

Scammers make unsolicited calls.

- Thieves call taxpayers claiming to be IRS

- officials. They demand that the victim pay a bogus tax bill. They con the victim into sending cash, usually through a prepaid debit card or wire transfer. They may also leave “urgent” callback requests through phone “robo-calls,” or via phishing email.

- •Callers try to scare their victims. Many phone scams use threats to intimidate and bully a victim into paying. They may even threaten to arrest, deport or revoke the license of their victim if they don’t get the money.

- •Scams use caller ID spoofing. Scammers often alter caller ID to make it look like the IRS or another agency is calling. The callers use IRS titles and fake badge numbers to appear legitimate. They may use the victim's name, address and other personal information to make the call sound official.

- •Cons try new tricks all the time. Some schemes provide an actual IRS address where they tell the victim to mail a receipt for the payment they make. Others use emails that

- contain a fake IRS document with a phone number or an email address for a reply. These scams often use official IRS letterhead in emails or regular mail that they send to their victims. They try these ploys to make the ruse look official.
- •Scams cost victims over $23 million. The Treasury Inspector General for Tax Administration, or TIGTA, has received reports of about 736,000 scam contacts since October 2013. Nearly 4,550 victims have collectively paid over $23 million as a result of the scam.

- The IRS will not:

- •Call you to demand immediate payment. The IRS will not call you if you owe taxes without first sending you a bill in the mail.

- •Demand that you pay taxes and not allow you to question or appeal the amount you owe.

- •Require that you pay your taxes a certain way.

- For instance, require that you pay with a prepaid debit card.
- •Ask for your credit or debit card numbers over the phone.

•Threaten to bring in police or other agencies to arrest you for not paying.

- If you don’t owe taxes, or have no reason to think that you do:

- •Do not give out any information. Hang up immediately.

- •Contact TIGTA to report the call. Use their “IRS Impersonation Scam Reporting” web page. You can also call 800-366-4484.

- •Report it to the Federal Trade Commission. Use the “FTC Complaint Assistant” on FTC.gov. Please add "IRS Telephone Scam" in the notes.

- NATIONAL GRID CUSTOMERS OF PAYMENT SCAMS – DIRECT FROM THE NATIONAL GRID WEBSITE.

- Customer Phone Payments Are Accepted, But Never Demanded

- National Grid again is reminding its customers of a nationwide utility bill scam. National Grid electric customers have received telephone calls from individuals claiming to work for National Grid. These scammers demand payment, through a pre-paid card, on past due

- balances for electric accounts and threaten customers that their service will immediately be shut-off for non-payment. In some cases the caller also tells the customer that they may have a faulty meter that is dangerous and in need of replacing for a substantial fee. The electric meter is the property of National Grid. Customers are not responsible for meter replacement costs. Callers are then directed to purchase a pre-paid card to make an immediate payment in order to keep their power on.

- National Grid does contact customers with past due balances by phone to offer payment options, but never demands direct payment over the telephone. If customers wish, they can arrange for a payment by check, credit card or debit card if they speak directly to a customer service representative. Payment can also be made by credit card or debit card without a representative's assistance. Customers who have received calls demanding immediate payment through a pre-paid card or who may have been given fraudulent phone numbers for National Grid should make note of the company's published customer service number.

- To verify information and for any billing-related questions, customers should call National Grid’s Customer Contact Center at 1-800-322-3223

You Hit the Jackpot!

You receive an email or phone call stating you won a prize but you must pay fees before receiving it. This is the Sweepstakes Scam. No legitimate sweepstakes will ask for money up front. You should never send money to receive money!

Sweepstakes and lotteries

- ✓ **You're told that you've won a sweepstakes or the Canadian lottery**
- ✓ **You're asked to pay for processing, taxes or delivery, or provide a bank account number to verify your identity**
- ✓ **No one ever receives a penny except for the thieves**

- Avoiding Lottery Scams
- Being aware of the three main approaches taken by lottery scams is a big key to avoiding becoming a victim, but there are three additional guidelines which can help to ensure that you don’t get conned:

- 1 - Remember ‘The Participation Rule’
- First, remember that you cannot possibly win a lottery game unless you have bought yourself a ticket for that game. Scammers will try and tell you that some lottery or other has randomly picked you to win or entered a number on your

- behalf, but all of that is nonsense. If you haven't bought a ticket, you won't win a lottery prize. Bearing this rule in mind will go a long way to making you immune to the scammers.

- 2 - Take a Closer Look
- If you ever receive a written lottery communication which you think is genuine, take a closer look because there are often flaws. First, check to see if the lottery organization actually exists. 'Euro Mega Millions Corporation' might sound plausible to both EuroMillions and Mega Millions players, but it's a completely

- fictitious organization which is designed to scam you.

- Also look out for spelling and grammatical errors (for example, “Your have won a big lottary prize!”) and obvious pseudonyms (“The Very Reverend Captain Tony Blair of the Royal Lottery Commission”). The examples provided might seem hilarious but we really have seen things like this – especially in email communications from lottery scammers who don’t speak English as a first language.

- 3 - Claim Direct
- Should you receive a telephone call, postal or email communication which you really believe is genuine – and you remember buying yourself a ticket for the game in question – don’t simply go along with whatever is requested of you. Instead, dig out your ticket (if you purchased it offline), take a look at the small print on the reverse of that ticket and follow the official claims process as described. And of course, if you purchased your ticket online you should log into your account for the official claims process of your lottery vendor.

- Lottery scams are not uncommon, but they can be avoided, and adhering to the guidelines presented here will help you to do just that.

- Video 47:35 – 49:50

Craigslist Scams

- •Do not extend payment to anyone you have not met in person.
- •Beware offers involving shipping - deal with locals you can meet in person.
- •Never wire funds (e.g. Western Union) - anyone who asks you to is a scammer.
- •Don't accept cashier/certified checks or money orders - banks cash fakes, then hold you responsible.

Tech Support Scams

- In a recent twist, scam artists are using the phone to try to break into your computer. They call, claiming to be computer techs associated with well-known companies like Microsoft. They say that they've detected viruses or other malware on your computer to trick you into giving them remote access or paying for software you don't need.These scammers take advantage of your reasonable concerns about viruses and other threats. They know that

- computer users have heard time and again that it’s important to install security software. But the purpose behind their elaborate scheme isn’t to protect your computer; it’s to make money.

- Keep these other tips in mind:•Don’t give control of your computer to a third party who calls you out of the blue.
- •Do not rely on caller ID alone to authenticate a caller. Criminals spoof caller ID numbers. They may appear to be calling from a legitimate company or a local number, when they’re not

- even in the same country as you.
- •Online search results might not be the best way to find technical support or get a company’s contact information. Scammers sometimes place online ads to convince you to call them. They pay to boost their ranking in search results so their websites and phone numbers appear above those of legitimate companies. If you want tech support, look for a company’s contact information on their software package or on your receipt.
- •Never provide your credit card or financial information to someone who calls and claims to

- be from tech support.
- •If a caller pressures you to buy a computer security product or says there is a subscription fee associated with the call, hang up. If you’re concerned about your computer, call your security software company directly and ask for help.
- •Never give your password on the phone. No legitimate organization calls you and asks for your password.

Protect Yourself from Fraud and Identity Theft

- Check your accounts daily.
- Notify your credit card companies or local banking institution immediately if fraudulent charges are located.
- Contact your local Police Department
- Check your credit report

- Do not send money through Money Gram or Western Union, if you haven’t done it before.

- Green Dot / Money Pak increasingly popular with those trying to steal your money.
- Once the suspects receives the numbers the on the back of the Green Dot / Money Pak cards, that money is gone within a few minutes. Very rarely recovered.
- Refillable credit cards – examples refillable American Express and Visa cards you can buy at most Supermarkets for a small fee.

Cloned Credit Cards

- The originating point of compromise is rarely found.
- Credit card numbers can be purchased online for as little as $3.00.
- Organized groups flood an area use cloned credit cards and disappear just as quickly. Surveillance images of the suspects aren't usually a concern for the suspects because they don't live in the area. Organized Groups have hit the Clifton Park area from Philadelphia, New York/Jersey and Foreign Work Visa's and so much more.

Skimming Devices

- Be careful they are out there.

- ATM machines
- Gas Station outside pumps
- Restaurants

They use overlay retrofitted devices. As well as pin point cameras to capture pin numbers.

Important Resources Regarding Identity Theft

- To exclude your name from lists for unsolicited credit card and insurance offers:
- For 5 years – Call toll free 1-888-567-8688
- Indefinitely - Is also available
- Online – go to www.optoutprescreen.com

- To exclude your name & phone number from Telemarketer do not call lists:
- You can register your home phone number or

- wireless numbers on the national Do-Not-Call list by phone or by Internet at no cost. To add a phone number to the national Do-Not-Call list via the Internet, go to www.donotcall.gov. To register by phone, call 1-888-382-1222 (voice) or 1-866-290-4236 (TTY). You must call from the phone number you wish to register.

- Telemarketers have up to 31 days from the date that you register your telephone number to remove it from their call lists and stop calling.

Credit Reporting Organizations

- Equifax Phone # 1-800-525-6285
- Experian Phone # - 1-800-397-3742
- Trans Union Phone # 1-800-680-7289

- You are entitled to one free copy of your credit report from EACH of the three credit reporting organizations. It is advisable to order one every four months. For a free report, call 1-877-322-8228 or on-line at annualcreditreport.com

Fraud Alert

- The three major credit bureaus will attach a fraud alert on your credit report to minimize future fraud. Call each of the three major credit bureaus to report the cloned card. Request a fraud alert on your credit report. This will ensure that any future creditors who check your credit with one of the credit bureaus will see the fraud alert. The creditors will have to contact you for permission before extending credit in your name.

To report ID Theft to the Federal Government

- www.ic3.gov

IC3 Mission Statement

The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

Take The Time !!!

- Stay Vigilant and have a plan.
- Continue to monitor your debit/credit card statements carefully every month to make sure that you catch every transaction. Now that your credit has suffered this violation, you need to monitor your finances with a magnifying glass so that nothing slips past you.

Additional Websites for ID Theft

- www.consumer.gov
- www.ftc.gov
- www.state.ny.us

Contact Information

- Please if you have any additional questions please contact me at the State Police barracks in Clifton Park – Address 5 Municipal Plaza or phone number 518-383-8583.
- Investigator Matthew Britten