

Introduction to Fraud Detective Kirby Shoemake





 In criminal law, fraud is an intentional deception or coercion made for personal gain and to damage another individual in some way shape or form.







 Fraud can be committed through many forms of media, including mail, wire, phone, and the Internet (computer crime and internet fraud).



Common Local Scams/Fraud



- Law Enforcement / Relative requesting "bail money" for a family member who was arrested.
- Law Enforcement agency (FBI, Sheriff, Federal Agent) demanding money for a "warrant" or you will go to jail.
- Craigslist work from home/secret shopper
- Utility companies demanding payment for past due bills
- Jury Duty Coordinator claiming you did not report
- Emails requesting to verify your account (credit card, bank, website) info.



Common Scams Among Elderly



- Grandparent scam A senior might receive an urgent phone call from someone who claims to be a grandchild who has an emergency, is out of town and needs money fast. The caller begs the grandparent not to tell his parents and to wire money quickly. Scammers might use actual relatives' names and information they get from social media.
- Jury duty scam The caller will claim to be a court officer and say there's a warrant for the victim's arrest, for failing to report for jury duty. The caller also claims that there's a fine for not showing up, and that unless the fine is paid immediately, via Green Dot Card Money Card or Western Union MoneyGram, the victim will be arrested.
- <u>Lottery scam</u> The caller claims a person won a foreign lottery and requests that the "winner" wire money or send a check to cover taxes and fees. Legitimate contests don't request money upfront. The caller might ask for bank information, claiming they want to direct deposit winnings electronically.
- IRS scam The caller says they're an IRS agent or police officer calling about a past due tax balance. Unless the debt is paid immediately with a Green Dot Card Money Card or Western Union MoneyGram, officers will arrest the victim that day, the caller claims. These scammers might use caller ID hacks, so that the ID name or number appears to be that of the IRS.
- <u>Utility scam</u> The caller claims to be a local utility provider representative; sometimes, they have the victim's correct account number and may have obtained personal information via social media. They tell the resident that they have to pay a late utility bill immediately, via Green Dot Card Money Card or Western Union MoneyGram, or service will be cut.

Tell-Tale Signs of a Scam

- You are contacted/solicited.
- They promise reward, prize, or personal gain.
- They request your personal information.
- You must make a "deposit" or pay a small "fee" to obtain your prize or reward.
- You have to wire, Western Union, or get a Green Dot Card.

Tell Tale Signs of a Con Artist

- They offer you something for nothing.
- They get you to like them or feel sorry for them.
- They make you think their "deal" is a now or never thing.
- They make you believe you can get rich.
- They get you to believe their deal has made others rich.





Credit Card Fraud



- What is Credit/Debit Card Abuse?
- How your card is compromised and or stolen.
- Ways to protect your credit/debit card information



Texas PC 32.02



- A person commits an offense if:
- (1) with intent to obtain a benefit fraudulently, he presents or uses a credit card or debit card with knowledge that:
- (A) the card, whether or not expired, has not been issued to him and is not used with the effective consent of the cardholder; or
- (B) the card has expired or has been revoked or cancelled;
- (2) with intent to obtain a benefit, he uses a fictitious credit card or debit card or the pretended number or description of a fictitious card;
- (3) he receives a benefit that he knows has been obtained in violation of this section;
- (4) he steals a credit card or debit card or, with knowledge that it has been stolen, receives a credit card or debit card with intent to use it, to sell it, or to transfer it to a person other than the issuer or the cardholder;
- (5) he buys a credit card or debit card from a person who he knows is not the issuer;
- (6) not being the issuer, he sells a credit card or debit card;
- (7) he uses or induces the cardholder to use the cardholder's credit card or debit card to obtain property or service for the actor's benefit for which the cardholder is financially unable to pay;
- (8) not being the cardholder, and without the effective consent of the cardholder, he possesses a credit card or debit card with intent to use it;
- (9) he possesses two or more incomplete credit cards or debit cards that have not been issued to him with intent to complete them without the effective consent of the issuer. For purposes of this subdivision, a card is incomplete if part of the matter that an issuer requires to appear on the card before it can be used, other than the signature of the cardholder, has not yet been stamped, embossed, imprinted, or written on it;
- (10) being authorized by an issuer to furnish goods or services on presentation of a credit card or debit card, he, with intent to defraud the issuer or the cardholder, furnishes goods or services on presentation of a credit card or debit card obtained or retained in violation of this section or a credit card or debit card that is forged, expired, or revoked; or
- (11) being authorized by an issuer to furnish goods or services on presentation of a credit card or debit card, he, with intent to defraud the issuer or a cardholder, fails to furnish goods or services that he represents in writing to the issuer that he has furnished.





 Credit/Debit Card Abuse is the unauthorized use of your card to make a purchase no matter the amount or how the purchase is made. (In a store, internet, etc)

Common Ways Your Card is Compromised

- Skimming
 - Your cards electronic information is "skimmed" by a device that captures its information.
- The numbers of the card are written down along with the PIN.
- Recommend you use a credit card in lieu of a debit card in public and online.



Ways to Protect Your Card



- Never leave your cards unattended at work, in a vehicle, etc.
- Protect your Personal Identification Number (PIN) or security code. Don't write it down, memorize it.
- Always check your card when returned to you after a purchase.
- Report lost or stolen cards immediately. Most fraudulent use of cards takes place within minutes of their being lost or stolen.
- Destroy unwanted cards.
- Make a list of all your cards and their numbers. This key information is helpful when reporting lost or stolen cards.
- Always check your monthly statement. Make sure the charges are yours. Report them to your card company if the entry is not yours.
- Never give your card number over the phone unless you are dealing with a reputable company. The only time you should give it is when you have called to place an order.





- What is check fraud?
- How are your checks compromised?
- Ways to protect yourself from it happening to you.



Texas PC 32.21



- Sec. 32.21. FORGERY. (a) For purposes of this section:
- (1) "Forge" means:
- (A) to alter, make, complete, execute, or authenticate any writing so that it purports:
- (i) to be the act of another who did not authorize that act;
- (ii) to have been executed at a time or place or in a numbered sequence other than was in fact the case; or
- (iii) to be a copy of an original when no such original existed;
- (B) to issue, transfer, register the transfer of, pass, publish, or otherwise utter a writing that is forged within the meaning of Paragraph (A); or
- (C) to possess a writing that is forged within the meaning of Paragraph (A) with intent to utter it in a manner specified in Paragraph (B).

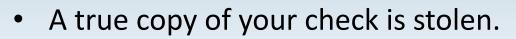




 To make or pass a "check" that is not a true, or valid authorized check.



Common Ways your Checks are Compromised



- An image of your check is obtained.
- Your routing number and bank account number are obtained.

Identity Theft

- What is identity theft?
- Ways to protect yourself.





Texas PC 32.51



- Sec. 32.51. FRAUDULENT USE OR POSSESSION OF IDENTIFYING INFORMATION. (a) In this section:
- (1) "Identifying information" means information that alone or in conjunction with other information identifies a person, including a person's:
- (A) name and date of birth;
- (B) unique biometric data, including the person's fingerprint, voice print, or retina or iris image;
- (C) unique electronic identification number, address, routing code, or financial institution account number;
- (D) telecommunication identifying information or access device; and
- (E) social security number or other government-issued identification number.

Bottom Line...



 Someone used your name, SSN, date of birth, and or address as their own.



Ways to Protect your Information



- Keep your Social Security card/number in a safe location.
- Don't leave your driver's license in your vehicle.
- Report loss of your SSN card and or Texas Driver's License to Law Enforcement immediately.
- Destroy old tax returns when they are no longer needed.
- Check your credit report.

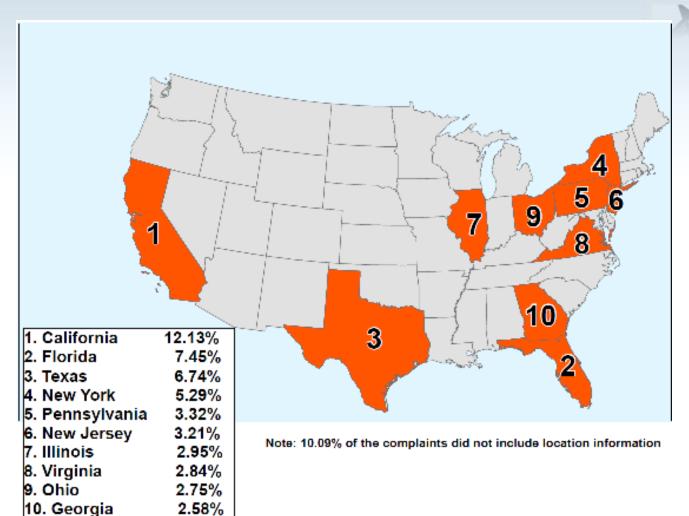
National and State Monetary Loss



- Out of 50 Countries World Wide the United States is #1 with a Nation Wide Loss from fraud estimated at \$574 Million Dollars.
- Out of the 50 States Texas is #2 with an a Statewide estimated loss due to fraud of \$56 Million Dollars.

Where the Scams Originate by State Ranking



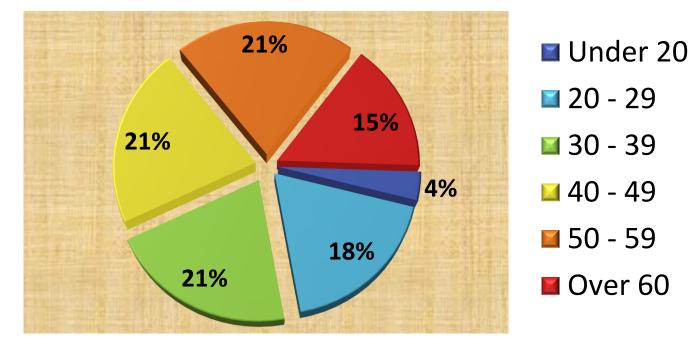


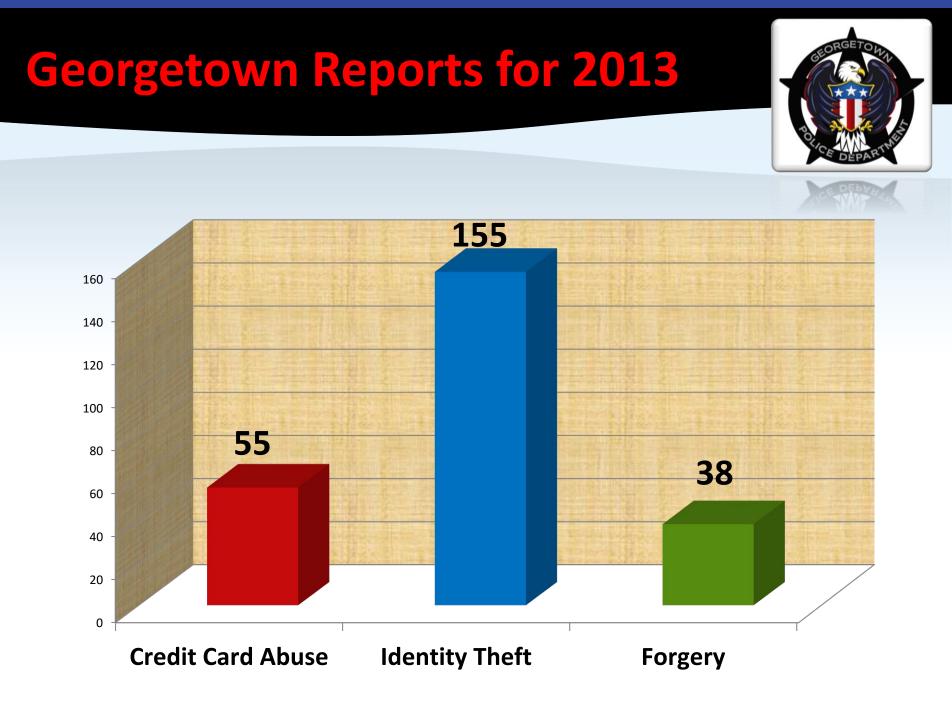
Who are the Targets?



- Victims 50 years or older account for 36% of all fraud in the US.
- Increase of 11.7% from 2012.

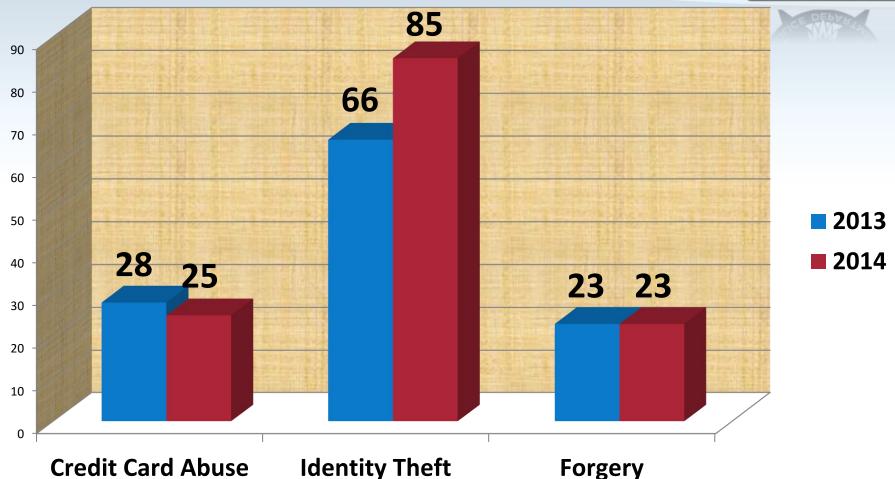
2013 Age Demographic of Complaints





Georgetown Reports Comparing 1st Half of 2013 to 2014





Protect Yourself



- Law Enforcement will NEVER call you and demand money for warrants, fees, or arrests.
- Never withdraw money from a check until the bank CLEARS the check.
- People NEVER over pay for anything. (purposely or accidently).
- If it is too good to be true IT IS!
- Secure your personal information at home.
- Don't give out personal information unless you initiated the contact.



Protect Yourself cont..

- Treat your mail and trash carefully.
- Don't carry your SSN in your wallet or purse.
- Give your SSN only when absolutely necessary.
- Keep copy of everything in your wallet or purse.
- Be cautious when responding to promotions.
- Pick up new checks at your bank instead of having them delivered to your home.
- Write checks using gel ink (won't wash off).



Free Annual Credit Report

SC BERARTUR

- www.annualcreditreport.com
- 1-877-322-8228
- 1 free report every 12 months from each major nationwide consumer reporting companies







Credit Opt Out



- www.OptOutPrescreen.com
- 1-888-567-8688
- 5 year registration or permanently
- To opt out of receiving offers of credit in the mail that are based on your credit report
- You will be asked to provide your SSN, which the consumer reporting companies need to match you with their file.
- It is free and you can opt back in at anytime.

National Do Not Call Registry

- www.donotcall.gov/
- Gives you a choice about whether to receive telemarketing calls at home.
- 31 days to go into effect.
- 5 year registration
- Placing your number on the registry will stop MOST telemarketing calls, but not all.
- Calls from companies with which you have an existing business relationship.





Texas No Call List

CORGETONAL TATATA

- www.texasnocall.com
- 1-866-896-6225
- Will further help limit calls to home or mobile numbers.
- Applies to any telephone marketer, including retail electric providers.
- 3 year registration
- Sponsored by the Public Utility Commission (PUC).





- https://www.oag.state.tx.us/consumer/scams.shtml (Texas Attorney General)
- http://www.FTC.gov/idtheft (Federal Trade Commission)
- http://oig.ssa.gov/report-fraud-waste-or-abuse (Social Security Number Fraud)
- https://ic3.gov (Internet Crime Complaint Center)
- Texas Penal Code

Report It by LeadsOnline.com

- www.reportit.leadsonline.com
- Citizen Property Inventory System

Register your property at reportit.leadsonline.com

General Public

Keep a secure, online record of valuable property, accessible from anywhere. All for free.

Law Enforcement

Help law enforcement recover stolen property faster than before.

Safe. Secure. Free.

Knowing what you own – the difference between recovering and not recovering stolen property.



QUESTIONS?



Detective Kirby Shoemake Georgetown Police Department General Crimes Unit Phone:512-930-8491 Fax:512-930-2591 kirby.shoemake@georgetown.org