THE FORTNIGHTLY CLUB

of

REDLANDS, CALIFORNIA

Founded 24 January1895

Meeting Number 1946

December 19, 2019

4:00 P.M.

Fraud, Fraud Schemes, and Identity Theft

By: Gary Fagan

Assembly Room, A.K. Smiley Public Library

SUMMARY

This paper will provide a basic introduction to fraud, common fraud schemes, and identity theft. The paper will provide a working definition of the acts, and words that constitute criminal fraud. It will then discuss common traits or behaviors that make an individual or business organization vulnerable to be preyed upon and become fraud victims.

The paper will continue on to identify historically common reoccurring fraud schemes and how they are perpetrated. This will include Nigerian scams, including lottery or inheritance scams, and extortion scams. It will include Ponzi and securities fraud scams, sweet-heart scams, affinity scams, loan forgiveness scams, and business email compromises.

The paper will then address identity theft. It will define identity theft and then review common methods by which an identity is stolen including phishing, spoofing, social engineering, mail and trash thefts. It will then discuss the ways the stolen identity is used to commit fraud

About the Author-

Gary is a retired Chief Deputy District Attorney. Gary was a prosecutor with the San Bernardino District Attorney's office from 1977- 2017. After extensive trial work and supervision assignments, Gary oversaw the District Attorney's Specialized Prosecution Division which was responsible for, among other areas, major frauds, securities fraud, real estate fraud, insurance fraud, welfare fraud, and consumer fraud. Gary wrote the District Attorney's identity theft manual.

INTRODUCTION

Let's start with two simple questions for you. Is there anybody reading this paper that likes their money, property or possessions? Is there anybody here that likes their unique identity and good name? I'll assume that most, if not all of you, answered affirmatively. This is generally good news. There is however bad news as well, so do a large number of scam artists, fraudsters, thieves, cyber criminals and otherwise shameless individuals that like and want all of these things that are yours for themselves and their criminal enterprises. This is what I will address.

This paper will provide a basic introduction to fraud, common fraud schemes, and identity theft. The paper will provide a working definition of the acts, and words that constitute criminal fraud. It will then discuss common traits or behaviors that make an individual or business organization vulnerable to be preyed upon and become fraud victims.

The paper will continue on to identify historically common reoccurring fraud schemes and how they are perpetrated. This will include sweet heart scams, Nigerian scams, including lottery or inheritance scams. It will include Ponzi and securities fraud scams, extortion scams, affinity scams, loan refinancing and forgiveness scams, and business email compromises.

The paper will then address identity theft. It will define identity theft and then review common methods by which an identity is stolen including phishing, spoofing, social engineering, skimmers and mail and trash thefts. It will also discuss the ways the stolen information is used to commit fraud

FRAUD DEFINED

A criminal fraud centers on a lie or misrepresentation. The lie is used to enable or allow someone to get something, in our case money, property, or something of value, which they would not be able to acquire or be entitled to without the

lie. The lie must be intentional, that is not an accident or accidental misunderstanding such as might the case when a person responds to an advertisement of "jaguar for sale", advertised as: "beautiful, powerful, runs great, in great shape, 4 years old" and who is then shocked to find that a cat, not a car, is being offered for sale. Not every deception or lie is the basis for fraud. Although the fraudster does not always actually have to acquire that which he seeks there must be some indication that he or she intended to receive it.

The familiar terms confidence game, con-man, scammer, scam artist, and so on describe fraud and its perpetrators. As will be noted, below, the perpetrators of fraud range from just plain unscrupulous individuals to highly educated people with special knowledge or skills required to construct or execute their schemes. Organized crime syndicates based in Eastern Europe, Africa, South America, and the United States perpetrate and profit from fraud schemes.

Perhaps, the first clear identifiable deception, and probable fraud occurs in Chapter 3 in the book of Genesis, when the snake, in lose interpretation, basically says to an unsuspecting Eve, "Hey, just eat the apple, nothing will come of it. What could go wrong?" Although it is hard to ascribe a motive that benefitted the snake, he got something- Eve eating the apple- which it could not have gotten without the lie.

VICTIMS

Let's turn our attention to victims now. Who gets victimized by fraud? Well, potentially anybody or everybody. However, fraudsters identify particular situations and types of individuals that are more susceptible to victimization than others. Vulnerable individuals are easily defrauded. These include the elderly, and the mentally or physically incapacitated. Those that are gullible or naïve are frequently targeted. In this context we are referring to people that don't have the knowledge or sophistication to understand what is being told to them or the full implication of what they are committing their money or property to. Certainly, people who think that people are basically good or can't perceive why

someone would lie to them about something that looks like it would be a benefit to them fall into this category of frequent victims. This group of potential victims are particularly vulnerable to investment fraud or loan fraud.

People who find themselves in deep financial trouble, either of their own doing or due to economic changes and who are desperate for a way out and willing to take risks they would not ordinarily take find themselves easily victimized.

This occurred following the 2008 housing collapse where more than 50% of Inland Empire homes were underwater. The amount owed on mortgages exceed the market value of the homes. Feeling desperate or actually being desperate, many people were victimized by mortgage fraud, home rescue schemes, and "walk away schemes". Another particularly vulnerable group are those who have suffered catastrophic loss incurred from a fire, earthquake, and other natural disasters as well those who have incurred large medical bills after serious illness or injury. After every devastating fire, even before the fire department has collected its hoses, con artists, unlicensed contractors, phony remediation companies and others descend on devasted neighborhoods to prey upon fire victims.

Similarly, those who are lonely, who have lost companions, who are in new environs, or who are looking for love can be vulnerable and be preyed upon by sweetheart scams.

Fearful individuals, those easily intimidated by verbal or written threats, or overbearing personalities, are targeted by threatening phone calls, emails or in person attacks demanding money to resolve an imaginary crisis. The fear of having done something wrong, even if it is factually baseless, provides an opening for victimization, particularly if the potential victim is fearful of injury to loved ones or of their good reputation being besmirched.

People careless in responding to emails, activating hyperlinks or not carefully examining where their personal information, such as passwords, electronic financial transactions or personal identifying information are stored or who

unknowingly provide them to spoofed websites or emails or phishing attacks unwittingly provide themselves as easy victims of fraud.

The last easily characterized group of victims is often the most unsympathetic. These are people who are best characterized as greedy. They fall prey to promises of extraordinary returns on their investments, returns that far exceed prevailing market rates of return. Often, these people are enticed by reassurances that they are smarter than the average investor, or are, in some way, especially eligible or entitled to these special investment opportunities.

Now that faith in your fellow man or women has been dashed, let's talk about fraud schemes

THE SCHEMES

Nigerian Scams

These are all variations of the same set of scams. They are so named because many of them had their origin in Nigeria and its organized crime networks, although currently other individuals acting independently, as well as Eastern European and other organized crime networks perpetrate these frauds. Originally, this scheme was generated by individual blind telephone calls, or bulk mail. Technology, by way of concealed origin robocalls or anonymously generated email, has extended the volume of these fraud attempts and reduced the cost in soliciting victims. As is the case in real fishing, the fisherman, or in this case the fraudster, doesn't care how many times the hook comes out of the water empty, so long as occasionally he hooks a keeper. These frauds are often successful with victims that are gullible, naïve or desperate.

Let's review some recurrent variations of Nigerian scams.

The *Lottery Winner scam*- This is a Nigerian scam variation. - This variation is perhaps one of the first large scale scams. It involves the victim receiving a

notification that they have won the Irish Sweepstakes, the Canadian Lottery, or some other undiscovered lottery prize that remains unclaimed. This is the lie. The catch is that in order to claim the prize the "winner" needs to pay the taxes and processing fees. Payment is usually demanded by gift card, money orders or prepaid credit cards before the "winnings" can be disbursed. An address, usually a post office or private mail drop, or a wire transfer account is provided by the perpetrator. The obvious warning here is that if you didn't buy a ticket you cannot have winnings.

The *lost inheritances or tax refunds scam* - In this variation, instead of a notification of unclaimed winnings, the lie is that there is an inheritance from a long lost relative, or tax refund, in your favor, waiting to be claimed. The victim is told that in order to claim this untold wealth the estate taxes or refund fees must be paid in advance.

The *Grandchild in trouble or Grandparent Scam*- This scam is most frequently done by telephone. The caller, often in a garbled voice, obscured by lots of background noise, often accompanied by crying or with desperation in the speaker's voice starts by saying, "Grandma, Grandpa, Auntie…etc. I'm in trouble, in – pick a foreign country- and I need your help". The target, usually, startled will say any number of grandchildren's names which the scammer will then use. The lie is that the "grandchild" is in jail, has been in a car accident, is in the hospital, etc. and needs money for bail, medical bills, or to leave the country. The posing grandchild demands the money be sent immediately, again by money order, or immediate wire transfer. The lie here is that the victim's loved one is in danger. The reality is that the child is safely at home. Victims can avoid being victimized by pausing to ascertain the location of their loved one.

The *outstanding warrants scam*- This is a threat or extortion scam, usually perpetrated by telephone. There are two common variances to this scheme. In the first, the caller claims to be from the "warrant detail" of a local police agency. The caller states that an officer is on the way to arrest the you for outstanding

traffic or other criminal warrants, but, if you pay right now, your arrest will be stopped. A variation on this is that the caller claims to be from the IRS and that not only will you be arrested but all your accounts will be seized. Often a credit card payment, providing your credit card number, name on the card, expiration date, and security code on the back is demanded. The lie here is that police agencies don't call and tell you they are on the way to arrest you, and fines are payable to a court, not the police. Likewise, the IRS never makes phone calls of this nature.

One prevalent red flag warning sign in these scams is there is a demand for immediate payment and that the payment is often demanded by way of Western Union money orders or wire transfers, postal money orders, gift cards, prepaid credit cards such as Visa Vanilla or Green dot cards, or cybercurrency like Bitcoin or Ethereum or by credit card transaction. Many of these methods of payment are used to launder money and untraceable when deposited or cashed.

Sweetheart Scams

Let's face it, who doesn't want to be flirted with. Who doesn't want to be loved? Who can resist someone who is attractive, wealthy, and promises to love you when you are sixty-four, or older? This is the basic come on or core of a sweetheart scam. The con artist- male or female- starts and maintains a relationship that the target believes is genuine. The perpetrator certainly does not believe this is a genuine relationship. The goal is to acquire money or financial control over the victim's assets. Seeking to make the old adage, "there is no fool, like an old fool" true these scams often target seniors and are a pathway to financial elder abuse where the perpetrator acquires complete control over the mark's finances.

The elderly are not the only targets. On line dating services and chat rooms provide the opportunity, to quote an old song, "for anyone to be whomever they want to be on the internet". Boosts, professions of love and affection, representations of who a person is and what they have accomplished, their

wealth, and even photographs are unverifiable fictions. Often the victim feels that they have found their "soulmate", "Mr. Right", or a trophy catch. The lie is that the professed lover does not have reciprocal feelings. He or she is only after the victim's money. This scam has, historically, also involved in person relationships, including, if enough money or property is involved, intimate relationships with the target. Having a real person to touch and hear sweet nothings from makes the target much more easily manipulated and vulnerable.

The warning signs of a scam are most evident when the pseudo-lover starts to ask for money; money to help get them through a tough time; money as a short-term loan; money for plane tickets for a special rendezvous; or money for whatever the false lover con artist thinks the victim will pay for. Here, again, the payment is requested in money orders, prepaid credit cards, authorization to charge on the victim's accounts and so on until the victim becomes suspicious or, more sadly, all the money is gone. The "pseudo-sweetheart" is then gone, leaving the victim emotionally and financially victimized.

Bank Examiner Scams

In this scheme, the perpetrator poses as a Treasury or Secret Service agent or bank examiner. The perpetrator selects a bank customer, often elderly, who has been identified by surveillance, asking the customer to assist them in detecting fraud or thievery at the bank. The victim is told they can be a secret agent. The victim is instructed to withdraw cash from their account so that it can be secretly marked and traced when redeposited. The victim is told that the posing agent cannot do this directly because he thinks the bank has been "tipped off". The first withdrawal is often small and is returned to the victim to build confidence. The next withdrawal is larger or direct access to the victim's account is requested. The money is then stolen, or the account is drained.

Ponzi Schemes

Ponzi schemes are investment or securities fraud schemes, named after Charles Ponzi, who in the early 1900's devised a fraud scheme involving the purchase

and sale of postal coupons. The central aspect of all variations of a Ponzi scam is that money is solicited from investors with promises of huge returns, or no risk returns on the investment. There is, in fact, no legitimate investment. The con artist takes money from new investors to pay preceding investors until there are no new investors or their money is insufficient to pay the preceding investors. Of course, the con man takes all of his money first. The perpetrator relies on the initial investors to spread the news of their good fortune to others. If the scam involves investors recruiting new investors, instead of the scheme originator, it is a pyramid scheme.

Terms like, "your original investment is guaranteed", "there is no risk involved", "why settle for 3% when you can get 11%", "Don't be left out" are often key phrases in the solicitation. All are lies. There are no risk-free investments. These scams often victimize people who are greedy in the sense that they want more than average or prevailing market returns. The scammer through his or her lies has led the victims to have confidence in him or her and their ability to deliver on the false promise. This is where the term "con-man" originates. Certainly, the adage, "if it seems too good to be true, it probably is" provides sound advice and warning to potential victims.

Affinity Scams

Affinity scams are not so much an independent fraud scheme as it is a description of how victims are selected for a scheme. Affinity scams target individuals that have something in common, an affinity, with either other victims, the perpetrator, or both. These can be people who belong to the same church, social group, sewing club, or country club. Bernie Madoff used his affinity with affluent members of his country club to perpetrate one of the largest *Ponzi* schemes in recent history.

Implicit in the implementation of an affinity scam is the belief that the perpetrator is one of us, and therefore can be trusted; if he is one of us, he wouldn't cheat us or do anything that would hurt us. Sadly, those who are

victimized by affinity scams, not only lose their money and property, but also, lose their trust in other members of the community with which they share an affinity. Often victims of affinity scams are too ashamed and embarrassed to admit that they have been victimized. This allows the scam to continue undetected.

Home Rescue Scams

After the 2008 economic downturn, more than fifty percent of the homes in the Inland Empire were upside down. That is, the homeowners owed more on their mortgages than the properties were worth. This situation provided fertile ground for a variety of home rescue scams, targeting people either desperate to save their homes, or walk away from them with no financial consequences.

Home rescue schemes usually promise the ability for the homeowner to walk away from their underwater homes. The scam is perpetrated by having the homeowner transferring their property, often by a quitclaim deed, to the "rescuer". The scammer then promises he will pay the mortgage or makes a representation that since the property was no longer the victim's name the victim has no obligation to pay the mortgage on a property that he no longer owns. The scammer never pays the mortgage payments but collects a fee for his services. This scheme presents a twofold fraud. The first aspect is that the homeowner has given away his property but is not legally released from the obligation to pay the mortgage. He remains still liable for the unpaid debt and suffers the consequences of the default. The second fraud is that the lender was defrauded by having the property which secured the mortgage promissory note transferred without their consent.

Desperation and a "pie in the sky" hope that the nightmare of the homeowner's home being unsellable and worth less than the mortgage made these victims particularly vulnerable. Adding insult to injury, some of the rescue scam perpetrators then purchase the "rescued" property at a foreclosure sale obtaining an ostensibly clear title to the property.

Business Email Compromise

Business email compromise scams are a relatively new cybercrime-based fraud scheme. The scheme wasn't actively tracked by the FBI until 2013 and reported annual losses in 2015 were at $246 million. That number has increased to $1.3 billion in 2018 targeting over 6000 businesses or organizations. This scheme is extremely sophisticated, difficult to detect, and is usually perpetrated by organized crime cybercriminals.

As the name implies, this scam targets businesses. It has successfully targeted Fortune 500 companies, local escrow companies, and small businesses. The fraud is perpetrated by sending an email or invoice to a particular employee in the accounting or bookkeeping department directing payment as detailed in the email. The company CEO or a known vendor is impersonated in the email using authentic looking logos and stationary from the real CEO, CFO or a real vendor. These items are often the product of previous cyber intrusions of the target company or their real vendors. The counterfeit email or invoice directs or authorizes immediate payment. The payment is directed to a particular account or email address. The email at first glance appears genuine. However, the sender of the email has altered the spelling, added dots or hyphens or changed a dot com address to a dot net address or altered the wire transfer account to one that is not genuine. This is a form of spoofing. The scheme relies on the disperser of the funds to not carefully inspect the email address, the known account numbers, or checking with the true CEO or CFO for the veracity of the request.

In the instances involving real estate escrow accounts, the escrow company email or computers are hacked or taken over by the fraudster. The fraudster then alters the escrow deposit instructions or disbursements directing the payments to fraudulent but real accounts controlled by the perpetrator.

A variation of this scheme involves an email, purportedly from an employee to the human resource of accounting department indicating there has been a problem with the employee's direct deposit paycheck. The counterfeit email then

directs the employee's next and future paychecks to the included account number. The actual employee is not the originator of the request and the new account is controlled by the perpetrator, not the employee.

The victimized business may not immediately detect the fraud until the true vendor inquires about not being paid, the escrow parties ask where the money went, or the employee doesn't receive his paycheck. Through the use of proxy servers, multiple transfers or anonymizing the origin of the sender by use of TOR- the onion router, a dark web router, locating the perpetrators or recovering the stolen money is extremely challenging. Often the stolen funds are deposited in off shore accounts or otherwise laundered.

Identity Theft

Simply defined, identity theft is the acquisition and use of your personal identifying information without your consent. Personal identifying information is broadly defined to include your name, date of birth and social security information, pin numbers or access credentials, bank and credit card numbers, business names and licenses, email and email accounts, etc. Personal identifying information is stolen so that the thief can fraudulently impersonate you and your finances, acquiring credit or purchases in your name, acquiring access to your financial accounts and draining them. The thief can misrepresent themselves as you in both digital and written communications and in a multitude of different settings. Once acquired your "identity profile" can be used by the thief, or it is commonly sold individually or in a bundle of profiles, in dark web marketplaces for as little as fifty cents per profile.

Some common ways that your identity can be stolen or compromised include:

- *Mail Theft*- To paraphrase a well-known commercial, "What is in your mailbox"? Our mailboxes contain bills, bank statements, checks, social

security checks, welfare checks, preapproved credit applications, tax returns and W-2 forms. Unlocked curbside mail boxes provide easy targets for thieves. Placing the red flag up on these mail boxes is, in essence, a “steal me” invitation to potential thieves. Mail is also routinely stolen from curbside mail deposit boxes, including those placed outside the post office. To accomplish this, thieves install trapping devices in the mail deposit slot that obstructs the ability of the deposited mail to fall fully into the collection box. The trap along with the mail is then removed by the thief. These traps can be folded cardboard or plastic, cardboard with a sticky adhesive, such as the sticky tape from a rat trap, or in a myriad of other creative designs. Mail is also stolen by placing a flexible rod, with an adhesive, sometime as unsophisticated as a wad of moist bubble gum, affixed to the end, into the slot to “fish” the mail out.

- *Dumpster Diving* - What is in the trash? If not properly shredded the same items that arrive in your mail. Preapproved credit applications, bank and credit card statements, pin numbers and access codes. Documents with your name, date of birth and social security information including business and medical records with your name and personal information.
- *Burglary*- Your home, your office and somebody else's office are all treasure troves of personal identifying information. Most of us keep banking and credit card statements and information, past tax returns, medical records, passports, hard drives and so on at our homes. All of which are potentially more valuable, and certainly easier to haul away than your 80” television. To make life easier for these thieves many of these documents are secured in our least secure locations- are our garages and sheds.
- *Phishing, Spoofing, and Hacking*-Phishing or spoofing occurs when the con artist, uses technology to expand his potential victim pool by sending emails, texts, or other electronic communications containing a hyperlink. The body of the communication may be one of the Nigerian scams mentioned above, or a phony communication from your bank or credit

card company, Apple, Microsoft or anyone else you do business with asking you verify or reset your password, or account information. The request is fraudulent, and the sender has sent a counterfeit web page, or letterhead, a spoof. Clicking on the link and providing your information gives it away to the crook. Similarly, it may provide a gateway into your device for future access- hacking- or insertion of malware.

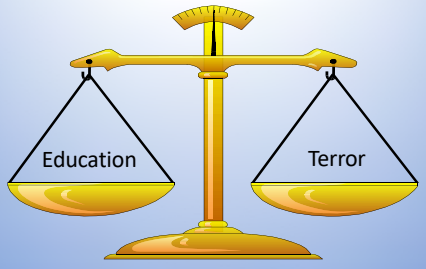
- *Compromised Employees*- Another common means of identity theft is by compromised employees. These are people that have access, either legitimately or through unauthorized means to the personal identifying information possessed by companies. These people can include receptionists, computer technicians, accounting or personnel department employees, visitors or executives and professionals. They are compromised by offers to pay for the data, desiring revenge on the company, aiding a competitor or being criminals or having family members who are gang members or criminals.
- *Social Engineering*- In a nutshell, social engineering occurs when someone talks their mark into providing personal information which is then used against them. In essence, all fraud schemes and scams rely on some degree of social engineering. The conman first acquires the confidence of the mark by promising or representing something that is not true, as in a sweetheart scam, a Nigerian scam, a Ponzi scheme, or by intimidating or frightening the mark as in in the grandchild in trouble or you have a warrant scam. In identity theft goal is to acquire your personal identifying information or a password or access to a secure computer server or site. Phrases like “can you help me out”, “I’ve forgotten my access card or passcode- can I use yours, just this once”, “I need a favor” are all red flag words.

CONCLUSION

This paper has provided a limited catalogue of frauds and scams. Unfortunately, there are many others that prey upon us. The methods and technology to advance these criminal enterprises continues to expand as law enforcement, cyber security experts, and everyday people strive to keep up. Hopefully, the paper has provided insight into the keys to identify the lies and misrepresentations that every fraud and con game relies upon to succeed.

Fraud Fraud Schemes and Identity Theft

Gary Fagan



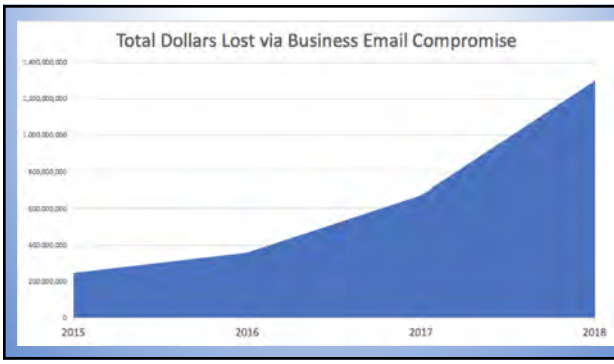
What I am Really Talking About

Frank Abagnale

The Victim Pool

Charles Ponzi

Bernie Madoff



- John.smith@sample.com
- JPMorganChase@1623

- johnsmith@sample.com
- john.smith@samp1e.com
- JMorganCase@1623

DUMPSTER DIVING

BURGLARY- THEFT

SOCIAL ENGINEERING