Police- Document Crimes Detail (DCD)

Information Provided by the Police Department

M-F 7 am to 4 pm, except Holidays and weekends. Call: 602-534-5958

Idenity Theft- How to protect yourself and what to do if victimized

Document Crimes is charged with the investigation of identity theft, forgery, credit card fraud, and embezzlement.

Many of the offenders committing identity theft and forgery are drug abusers. In order to finance their addiction these offenders are stealing mail, dumpster diving behind businesses and breaking into cars, homes and businesses looking for any documents or articles that may contain this information. Your personal information is then being used to apply for credit cards, retail credit or to counterfeit checks with your account number.

It is important to protect your information at all times and ensure that any business that obtains your information in the course of doing business is questioned by you as to how they are going to protect or destroy that information once they have finished with it.

If you find that you have been victimized, refer to the information supplied on this site. Follow the steps outlined and keep a personal file on each incident to aid in clearing up your credit. Included on this site are downloadable forms and tip sheets that you may print and use at your discretion.

Identity Theft

If someone has used your personal identifying information, such as your social security number, date of birth and name, to open lines of credit or to obtain services, you will first need to contact all 3 major credit reporting bureaus to place a "Fraud Alert" on your credit report. When you call the following toll-free numbers, this will notify businesses that you may be the victim of fraud. Request a copy of your credit report to review. Contact the following bureaus:

Trans Union:	1-800-680-7289
Experian:	1 888 397 3742
Equifax:	1-800-525-6285

Review all of the information on your credit report and determine if the entry is a mistake or fraudulent.

The following information will assist us in investigating your case: a copy of your credit report listing the fraudulent accounts, collection notice or other documents that identify where the crime occurred, etc.

If you feel that you have been the victim of an Identity Theft, contact Crime Stop at 602-262-6151 and request an Identity Theft report. A report may be taken over the phone. To assist you in the correction of your credit and to help ensure that you are not responsible for the debts incurred be the identity thief download and print the Identity Theft Victim's Packet from our web page.

Fraudulent Checks

If your checkbook has been stolen or lost, call Crime Stop at 602-262-6151 and request a Call-Back Officer to do a Theft or Loss report.

If your stolen/lost checks are being used in Phoenix by someone forging your signature, you need to first contact your bank to close your account. You will also need to complete an Affidavit of Forgery at your bank for any forged check that has cleared. In many cases, the forged checks will be handled primarily by your bank. Your bank will credit your account once you complete the Affidavit of Forgery. They will send a

copy of your Affidavit, along with the original check, back to the business that accepted the check. It is now the responsibility of that business to file the police report since they lost either cash or merchandise.

If you still desire a report for Identity Theft call Crime Stop at 602-262-6151.

If you are a merchant that has received a forged check that was returned to you from the bank, the Phoenix Police Department requires that you are able to present the original check, with the Affidavit fo Forgery completed by the account holder, as well as the employee who completed the transaction with the suspect. When this information is available, download the Business Forgery Report Packet from our web page. Once completed, the packet can be mailed to the Document Crimes Detail. Please follow all instructions carefully. Please note that if there is a confirmed forgery in progress, with the suspect still at your location, immediately call 9-1-1. In this case, no Affidavit is required.

If you have received a check back from the bank that is not payable due to a Closed Account or Non-sufficient Funds (NSF), contact the County Attorney's Check Enforcement Bureau at 602-372-7300.

Credit Card Fraud

The Phoenix Police Department will only take a report if the physical plastic card has been stolen. Call Crime Stop at 602-262-6151 to make a theft report.

If only the credit card number has been compromised and you still have possession of the plastic card, immediately notify your bank or credit card issuer to cancel the card. You will also need to complete a dispute form for any unauthorized charges. The credit card company may issue you a "temporary credit" and send a "charge-back" to the business that accepted the card number, without seeing the physical card. The business, who now suffers the loss, will need to complete the police report, if they so desire.

If you still desire a report for Identity Theft call Crime Stop at 602-262-6151.

Computer and Telephonic 'Phishing' Schemes

Phishing is a scheme where criminals attempt to identify a legitimate email address by sending a familiar looking computer generated email message. Phishing can take place at the worksite, home or anywhere a computer user has access to email. Phishing emails provide the recipient with a website link. If the link is 'clicked', the unaware user is sent to a fraudulent website. At the fraudulent website, the request for personal information such as a social security number, personal account numbers, or passwords may look legitimate. These schemes can also occur via the telephone. The caller may even have some level of information regarding you personally which was obtained through other means, which they will use to entice you into believing the call is legitimate.

The Document Crime Detail would like to make you aware of preventative measures that will thwart these criminals. **Never provide an unsolicited email or phone caller with any personal information especially if the request comes from a bank where you do business, a credit card institution for a credit card you carry, or other financial type site that you may do business with.** These institutions will never make this type of request unless you have initiated the call. If you are unsure of the request, initiate contact with your financial institution at a later time. For further information contact any member of the Property Crimes Bureau Document Crime Detail at 534-5940.

Lottery/Nigerian Scams

Phishing scams can also occur through email or letter indicating in some fashion that you have won a lottery. The letter/email indicates that you have won this lottery, usually from some foreign country and all you have to do is either send them a "nominal" fee to cover taxes and they will forward the money. Other times they will send you a cashiers check for you to cash with a request to send them back a portion to cover these taxes/handling fees. These checks are counterfeit and like the letters/emails, will most likely

contain grammatical errors.

The passing of these checks is considered a forgery. You will put yourself in a position of proving that you are not a willing participant in this fraud. The authors of this fraud are often overseas and are counting on the greed of the recipients to try and cash these checks. Due to the large number of their correspondents world wide, the amount of money these criminals receive via successful transactions and "taxes/fees" runs into the millions of dollars each year. Remember, if it is too good to be true, IT IS!

Nigerian letters/emails will represent themselves as successful individuals who are unable to remove their own money from their accounts due to the hostile government where they live, or some other sympathy style story. They request that you do something for them in exchange for money to be sent to you. It may be to set up an American Bank Account or to provide your own account number or it may be to pick up packages for them. If an American responds to them, they will begin to try and convince them to wire money, often thousands of dollars in order to initiate the money transfer. Of course the victim will never receive any money. If you have received any of these inquiries, ignore them as they are a fraud. Remember, if it is too good to be true, IT IS!

Preventative Measures

Your greatest asset for securing your good name is understanding where the thieves get your information. Here are a few of the many ways thieves can obtain your personal identifying information:

1. Coming into possession of your lost or stolen wallet or purse.
2. Stealing your mail, or diverting it to another mailbox via a change of address request.
3. "Dumpster Diving" into your trash and gathering important documents.
4. "Pretext" calls where the thief poses as your bank, internet service provider, or other organization with which you may or may not have had financial dealing and they call you to "verify your account information" because of a problem they had with their "records system."
5. Other crimes such as burglary or breaking into a vehicle where the thief looks to steal financial information, wallets, purses, or other items containing such information.
6. Internet transactions on unsecured sites or with illegitimate companies posing as a reputable "safe" business with which you may do business.

Knowing how the thieves get the information, it is now clear how best to protect that information: you should begin immediately to practice these simple steps:

1. Protect your Social Security number, credit card numbers, account passwords and other personal information.

Use common sense, and be suspicious when things don't seem right. Never divulge your information over the phone unless you initiated the phone call. If personal information is requested ask questions. It is your right to know why it's needed, how it will be used, and who needs it.

If you get an unsolicited offer that sounds too good to be true it probably is! If a caller claims to represent your financial institution, the police department or some similar organization and asks you to "verify" (reveal) confidential information, hang up fast and consider reporting the incident. Real bankers and government investigators don't make these kinds of calls.

2. Minimize the damage in case your wallet gets lost or stolen.

Don't carry around more checks, credit cards or other bank items than you really need. Limit the number of credit cards you carry by canceling the ones you don't use. Don't carry your Social Security number in your wallet or have it pre-printed on your checks. Pick passwords and Personal Identification (PIN) numbers that will be tough for someone else to figure out-don't use your birth date or home address, for example. Don't keep this information on or near your checkbook, ATM card or debit cards. Also, don't leave your wallet unattended in a store, restaurant, office or other public place even for a few minutes.

3. Protect your incoming and outgoing mail.

Promptly remove mail from your mailbox after it has been delivered. If you're going on vacation have your mail held at your local post office or ask someone you *know and trust* to collect your mail. Deposit outgoing mail in the Postal Service's blue collection boxes, hand it directly to a mail carrier or take it to a local post office.

According to Postal Inspector Virgil Moore, Public Information Officer for the Phoenix Field Office, when writing checks use "gel-ink" pens. Moore, said that currently they have found that checks written using "gel" ink are unable to be chemically erased and therefore more difficult to forge or counterfeit.

4. Keep thieves from turning your trash into their cash.

"Dumpster divers" pick through trash looking for pre-approved credit card applications and receipts, canceled checks, bank statements, expired charge cards and other documents or information they can use to counterfeit or order new checks or credit cards. To keep these from happening use a "cross-cut" shredder and shred any document that contains any part of or all of your personal information. "Cross-cut" shredding makes confetti out of the documents and makes it virtually impossible for the thief to paste them back together.

5. Practice home security.

Safely store extra checks, credit cards, or other financial documents. Consider using a document safe for these items. Don't advertise to burglars that you're away from home. Use timers on your lights and temporarily stop delivery of your newspaper and mail or ask a *trusted* neighbor to pick up any items that may arrive unexpectedly at your home.

6. Pay attention to your bank account statements and credit card bills.

ALWAYS check into discrepancies in your records or if you notice something suspicious, such as a missing payment or an unauthorized withdrawal. Also, contact the appropriate institution if a bank statement or credit card bill doesn't arrive on time because that could be a sign someone has stolen account information and changed your mailing address in order to run up big bills in your name from another location.

7. Review your credit report approximately once a year.

Monitor your credit report for accuracy, looking for unauthorized bank accounts, credit cards, purchases, etc. Look for anything suspicious in the section of your credit report that lists who has received a copy of your credit history. This may be an indication a thief is trying to obtain fraudulent benefits, or is merely casing you as a viable victim.

To order your report, call the three major credit bureaus at these toll-free numbers: Equifax at (800) 685-1111, Experian at (888) 397-3742, or Trans Union at (800) 888-4213. By law, the most you can be charged for a copy of your report is $8.50. To be safe, consider getting a copy from each of the three companies.

8. Practice "on-line" or internet safety.

Be suspicious of web offers that "seem to good to be true." Ensure the web site you are using is legitimate, or has been formally examined and certified secure and reliable by a legitimate certifying agency such as the Better Business Bureau or the like.

Use your credit card and social security number only when absolutely necessary. Only use wesites who you believe are using secure communication links that are encrypted (scrambled). Again, keep your PIN numbers and passwords confidential, and DON'T write them down and leave them next to, on or near your computer. (prevention information paraphrased from the FDIC Consumer News - Summer 2000)

Identity Theft Prevention for Businesses

Identity theft related crime has been identified as the fast growing crime trend in America today. In 2004, the Federal Trade Commission identified the Phoenix metropolitan area as having the highest rate of identity related crime per capita of any other city in the nation. In order to make a positive impact, law enforcement and businesses must coordinate our efforts to better protect ourselves and the citizens we serve.

The Phoenix Police Department has responded proactively to this threat to our community. In 2004, The Document Crime Detail (DCD) was increased by six detectives and one supervisor, in order to bring additional resources to combat this alarming crime trend. The DCD is also currently participating with the FBI/Bank Fraud Task Force and the Postal Inspection Service Identity Crimes Task Force. The Document Crime Detail is dedicated to addressing this crime through aggressive investigative intervention involving other plain clothes investigative units and coordination with financial institutions and the hotel/motel industry.

The home computer has revolutionized the ability of the average criminal to involve themselves in identity related crimes. A large majority of the offenders are being identified as having illegal drug addictions and are utilizing identity theft to further their ability to afford these drugs.

These criminals are stealing mail in order to discover checks (routing and account numbers), credit cards and/or applications (items of mail containing personal information that can be utilized to obtain credit). By using check and ID writing software, offenders are making counterfeit checks and ID's in order to write checks for cash or to purchase retail items.

These suspects are also compromising the credit card industry by obtaining credit cards via the internet application process using stolen personal information. They are also obtaining stolen credit cards through mail theft, burglary from vehicle and other related crimes. Another form of credit card fraud occurs when the offender obtains the credit card numbers from discarded receipts, applications and other paperwork discarded into dumpsters by individuals and businesses.

While advances in technology and the advent of the internet have made it possible for businesses to become more user friendly, it also opened the door for the perpetration of fraudulent activity under cover of anonymity. With the adoption of the below listed business practices you can help to curtail fraud while still presenting a positive user friendly atmosphere for your customers and limit your exposure to civil liability through reckless handling of your customer's personal information.

How to protect your clients/customers

Keep all documents containing personal information of your clients, customers and employees under lock and key.

When personal information is held within a computer, ensure that it can only be accessed and tracked by authorized personnel using passwords and is protected with an appropriate level of security/fire walls. When the information has been transferred to the computer, any handwritten information should be

shredded.

Shred customer personal or account information and receipts before discarding them. Consider keeping shredders within reach of those employees who handle personal/account information on a regular basis.

Create policies to restrict the handling of customer information to a limited number of employees.

Customer personal information such as credit applications, sales receipts/carbon copies should not be temporarily kept within reach of the casual observer. This will help to deter theft by criminals or corrupt employees. Provide a secure receptacle for employees and citizens to throw out applications/receipts or provide informational signs advising them not to carelessly discard these documents.

How to protect your business from fraud

When accepting credit applications or checks, require the applicant to provide a finger print directly on the application or check. This is common practice in the banking community and should be readily accepted. This aids law enforcement with identifying exactly who presented the documents.

Install video surveillance in areas where business is conducted with a "loop time" of at least one month. This will allow ample time for the fraud to be detected and the suspect transaction to be pulled for evidence.

Video evidence along with a finger print is very good evidence and reduces the possibility that employees would have to attend court.

Require a photographic ID be presented during check and credit card transactions, along with a finger print on the sales receipt and/or check. Inkless pads are cheap and readily available for each register. Debit card transactions utilizing a PIN number need not fall into this category.

If your business retails to other businesses utilizing a business account number and company credit card listed in your computer, understand that this information is often corrupted by ex-employees of the customer business. Always require that your sales representatives call a responsible party with the company to verify the transaction.

If your business accepts telephone or internet orders, always utilize the 3-digit verification number printed on the signature line of the card. This number should not be recorded on the internet order form or receipts generated from sales. This ensures that the card itself is in the possession of the customer and isn't being stolen from a compromised recklessly discarded document.