

REQUEST FOR COUNCIL ACTION CITY OF SAN DIEGO	CERTIFICATE NUMBER (FOR COMPTROLLER'S USE ONLY)
--	--

TO: CITY COUNCIL	FROM (ORIGINATING DEPARTMENT): Police Department	DATE: 9/17/2014
---------------------	---	--------------------

SUBJECT: This is an informational report from the San Diego Police Department regarding the investigation of Identity Theft.

PRIMARY CONTACT (NAME, PHONE): Lt. Rich Freedman,(619) 446-1035	SECONDARY CONTACT (NAME, PHONE): Sgt. Mark Van Abel, (619) 446-1046
--	--

COMPLETE FOR ACCOUNTING PURPOSES

FUND					
FUNCTIONAL AREA					
COST CENTER					
GENERAL LEDGER ACCT					
WBS OR INTERNAL ORDER					
CAPITAL PROJECT No.					
AMOUNT	0.00	0.00	0.00	0.00	0.00



FUND					
FUNCTIONAL AREA					
COST CENTER					
GENERAL LEDGER ACCT					
WBS OR INTERNAL ORDER					
CAPITAL PROJECT No.					
AMOUNT	0.00	0.00	0.00	0.00	0.00

COST SUMMARY (IF APPLICABLE):

ROUTING AND APPROVALS

CONTRIBUTORS/REVIEWERS:	APPROVING AUTHORITY	APPROVAL SIGNATURE	DATE SIGNED
Liaison Office	ORIG DEPT.	Ramirez, David	09/17/2014
	CFO		
	DEPUTY CHIEF		
	COO		
	CITY ATTORNEY	Folkman, Paige	09/22/2014
	COUNCIL PRESIDENTS OFFICE		

PREPARATION OF: RESOLUTIONS ORDINANCE(S) AGREEMENT(S) DEED(S)

Information report only

STAFF RECOMMENDATIONS:
None

SPECIAL CONDITIONS (REFER TO A.R. 3.20 FOR INFORMATION ON COMPLETING THIS SECTION)

COUNCIL DISTRICT(S):	All
COMMUNITY AREA(S):	All
ENVIRONMENTAL IMPACT:	None

CITY CLERK
INSTRUCTIONS:

None

**COUNCIL ACTION
EXECUTIVE SUMMARY SHEET
CITY OF SAN DIEGO**

DATE: 9/17/2014

ORIGINATING DEPARTMENT: Police Department

SUBJECT: This is an informational report from the San Diego Police Department regarding the investigation of Identity Theft.

COUNCIL DISTRICT(S): All

CONTACT/PHONE NUMBER: Lt. Rich Freedman/(619) 446-1035

DESCRIPTIVE SUMMARY OF ITEM:

This is an informational report / presentation from the San Diego Police Department regarding information relative to the investigation of Identity Theft by the Department's ID Theft Unit and the impact of identity theft on residents of the City of San Diego.

STAFF RECOMMENDATION:

None

EXECUTIVE SUMMARY OF ITEM BACKGROUND:The Identity Theft Unit investigates criminal matters that involve identity theft rings and /or fraudulent credit applications submitted to businesses, credit agencies or banks utilizing a victim's personal identifying information.

This unit also assists area station investigators and investigating units in problem solving efforts involving financial crimes and actively seeks community partnerships when starting problem solving projects as necessary within the City of San Diego.

The unit provides assistance to citizens and businesses by referring them to appropriate investigative agencies where they can obtain assistance in dealing with problems not handled by the unit and also provides information to and training for residents of San Diego.

Administrative Information-

The Identity Theft Unit is comprised of one sergeant and six detectives. In 2013, the unit received 4,076 reports of Identity Theft. January thru August 2014 the unit has received 2,842 cases. This is an increase of approximately 20 additional cases per month.

FISCAL CONSIDERATIONS:None

EQUAL OPPORTUNITY CONTRACTING INFORMATION (IF APPLICABLE):N/A

PREVIOUS COUNCIL and/or COMMITTEE ACTION (describe any changes made to the item from what was presented at committee):Previously presented to PSLN on October 3, 2013

COMMUNITY PARTICIPATION AND PUBLIC OUTREACH EFFORTS:None

KEY STAKEHOLDERS AND PROJECTED IMPACTS:N/A

Ramirez, David

Originating Department

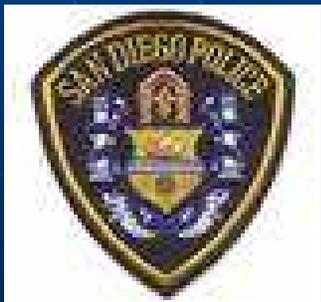
Deputy Chief/Chief Operating Officer



Economic Crimes Section

San Diego Police Department

Identity Theft Unit





Agenda

- Trends in ID Theft
- Compromised PII
- How your information is obtained
- How your information is used
- How to protect yourself
- What to do if you are a victim
- Common scams

Trends

Identity Theft / Fraud Statistics

Data

Average number of U.S. identity fraud victims annually 11,571,900

Percent of U.S. households that reported some type of identity fraud 7 %

Average financial loss per identity theft incident \$4,930

Total financial loss attributed to identity theft in 2013 \$24.7 billion

Total financial loss attributed to identity theft in 2012 \$21 billion

Total financial loss attributed to identity theft in 2010 \$13.2 billion

Source: U.S. Department of Justice, Javelin Strategy & Research

Research Date: 7.8.2014

Trends



87%

SINCE

2010

What is Identity Theft

- The theft of personal identifying information;
- Used to fraudulently obtain, or attempt to obtain, credit, goods, services, real property, or medical services/information;
- Of another;
- Without consent.

Personal Identifying Information (PII)

Include numerous types of identifying information. However, the most frequently utilized information includes:

- Name
- Address
- DOB
- Telephone Number
- SSN
- Driver License Number
- Credit/Debit Card Number
- Checking/Savings Account Numbers
- E-mail Addresses

Identity Theft

- Arguably the most pervasive crime in the United States
- So common in the United States, many businesses and consumers consider identity theft resulting in financial fraud the “cost of doing business”

How Identity Theft Occurs

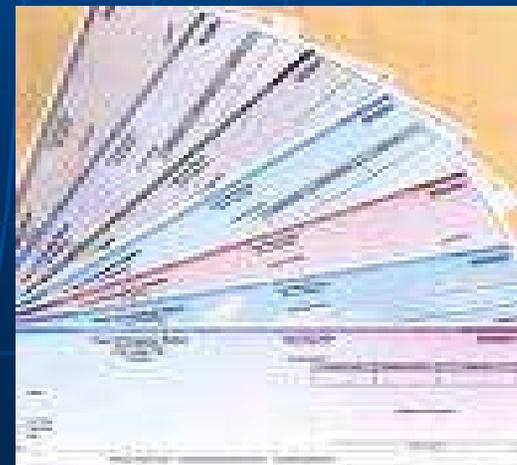
Identity thieves ...

- Steal wallets and purses
- Steal your mail
- Use skimmers
- Complete false "change of address" forms
- Rummage through trash (dumpster diving)
- Pose fraudulently as a landlord, employer or creditor to obtain credit reports
- Browse social networking websites



What's in your mail?

- Bank statements
- Credit card statements
- Pre-approved credit card offers
- Checks
- Convenience Checks



Skimming Scam

- Crooks can access your credit/debit card information at the gas pumps by installing a skimming device inside the pump
- Thief makes counterfeit card, or makes purchases over the phone or Internet, or sells the information to another "thief"

Credit Card Fraud

- Opening new accounts in your name



- Adding themselves to your existing accounts.

Neiman Marcus

- Using your account numbers on counterfeit and gift cards



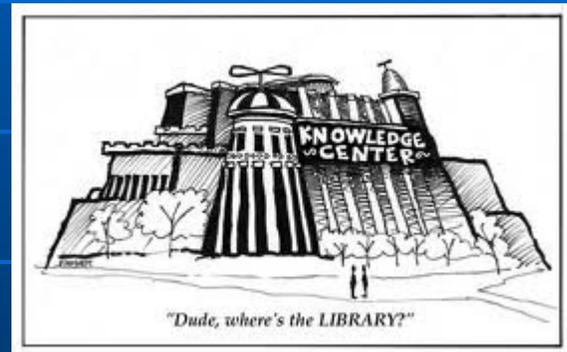
Bank Fraud

- Committing fraud by using your personal checking account and routing numbers on counterfeit checks



Fraudulent Loans

- New Car Loan
- Student Loan
- General Loan



Credit Cards vs Debit Cards

- A credit card is a bank-issued card that allows people to purchase goods or services from a merchant and to pay for them at a later date.
- If your credit card is compromised, and you report the crime within 60 days, the maximum liability for the unauthorized use of the credit card is \$50.

Credit Cards vs Debit Cards

- A debit card looks like a credit card but works like an electronic check. It is linked with the customer's checking or banking account
- If the unauthorized use of the debit card is reported within 2 business days, you cannot be held responsible for more than \$50
- If reported after 2 business days but before 60 days, the most you could lose is \$500

Tips on How to Protect Yourself

- If you encounter an unsolicited e-mail that asks you, either directly, or through a web site, for personal financial information, SSN, passwords or other identifiers, exercise extreme caution
- If you need to update your information online, use the normal process you've used before

More Tips

- Never left-click on a hyperlink on an unsolicited e-mail
- This can lead you to a suspect's website and can download harmful viruses and malware

More ways

- Carry as little identification information as possible
- Never leave your purse/wallet in your vehicle unattended
- Limit the number of credit cards you carry
- Make photocopies of every card in your wallet
- Use your credit card rather than your debit card
- Do not carry your Social Security Card or number in your wallet or purse
- Don't give personal identifying information on the phone unless you initiate the call
- Check your credit reports at least once a year

Prevention for Computer Users

- When shopping on-line, be sure you are dealing with a reputable company
- When disposing of your computer or copier, use a “wipe” program to remove data on both hard drives
- Install firewall and virus protection software

If you do become a victim...

- File a police report
- Close the accounts that have been affected
- Get as much information as possible about the fraudulent account to give to police and keep a log of your contacts
- Contact the fraud departments of the three major credit bureaus to place a fraud alert or freeze on your credit file
- File your complaint with the FTC and Post Office

Questions & Answers