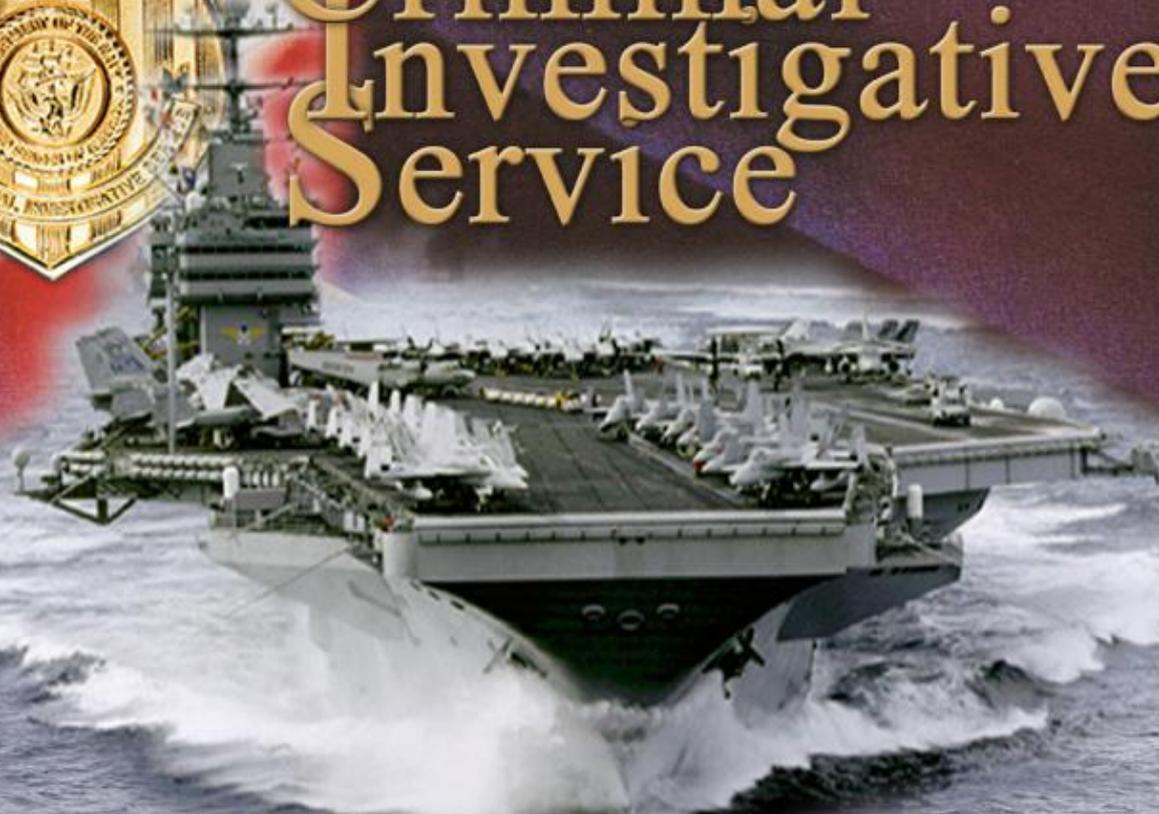




Naval Criminal Investigative Service



IDENTITY THEFT AWARENESS

OVERVIEW

- What is Identity Theft?
- How Do They Do It?
- Preventive Actions
- What to Do If You are a Victim
- Why Do They Do It?



What Is Identity Theft?

- Acquiring key pieces of someone's personally identifying information (name, address, DOB, SSAN, etc...) in order to impersonate them and to:
 - Take over their financial accounts/credit cards and withdraw funds or make purchases
 - Open new accounts
 - Obtain loans
 - Obtain credit cards
 - Obtain driver's licenses or other identifying documents



How Do They Do It?

- There are too many methods to list all, but below are some examples ranging from very high tech to very low tech:
 - Hacking
 - Card reading/cloning devices
 - Phishing
 - Corrupting postal or other employees with access
 - Dumpster diving/theft of unsecured personal data

Preventive Actions

- Safeguard all items containing PID
- **NEVER** give personal information over the telephone or internet unless you initiated the contact
- Shred, shred, shred!
- Order your credit report from the three credit bureaus once a year to check for discrepancies
 - Get a free credit report: www.annualcreditreport.com
- Promptly report changes of address/telephone number

Preventive Actions

- Know your credit/debit cards
 - Limit use, particularly on the internet, so you can easily recognize fraudulent activity
 - Sign up for online statement access, if available, and review your transactions regularly
 - Report lost or stolen credit/debit cards immediately
 - If your credit/debit card expired and you haven't received a new one, or if you applied for a new credit/debit card and it hasn't arrived, call!
- If eligible, use the Active Duty Alert

What to do if You are a Victim

- Contact all creditors immediately by telephone, and follow up with written correspondence informing them of the problem
 - Failure to act in a timely manner can increase your liability with some creditors
- Call the fraud unit at each of the three credit bureaus and request a fraud alert be placed on your credit file
 - For a limited time will require creditors call you prior to accounts being opened in your name

What to do if You are a Victim

- Call your local Military or Civilian Police Department to file a complaint
- Contact DMV in your home state of record and any other states where credit was opened in your name to see if another license was issued in your name
- Keep a log of all contacts and make copies of all documents
- File a report with the FTC

Why Do They Do It?

- Relatively easy way to make money
- Generally low risk
 - Difficult to identify suspects
 - Prosecutorial thresholds
 - Jurisdictional issues
 - Corporate indifference
 - Insurance policies
 - If the company doesn't take a loss, they often won't provide information without a subpoena

Conclusion

- Identity theft is one of the fastest growing crimes and technology makes it easier and easier
- It can take years to recover from identity theft, so the best practice is to avoid ever becoming a victim

