# MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

*FOR COMCEN/SIG USE*

PRECEDENCE ACTION/PRECEDENCE INFO
**"PRIORITY"**

**FM: CG, PA**

**TO: All Unit Commanders**
**Attn: G6/Signal Officer/IS Officer**

**INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA**

**INFO: CSAFP**
**Attn: J6**

GROUP:
**16 November 2015**

SECURITY CLASSIFICATION:
**CONFIDENTIAL**

ORIGINATOR:
**6/CMB 1611-25-2015**

1. References:

   a. Command Guidance
   b. Cybersecurity Awareness
   c. VAPT and PANET Monitoring Result

2. As per above references, forwarded is the Cyber Security Bulletin number 034 with topic regarding **WHAT IS IDENTITY THEFT?.**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cyber Security Awareness of the Philippine Army.

4. For information and widest dissemination.

| **DRAFTER'S NAME AND TITLE** | **PHONE NR:** |
|---|---|
| MAJ JOEY T FONTIVEROS (INF) PA<br>Chief, CMB, OG6, PA | 6630 |
| **RELEASER'S NAME AND TITLE** | |
| COL VENER ODILON D MARIANO GSC (SC)PA<br>AC OF S FOR CEIS, G6, PA | |

HEADQUARTERS
PHILIPPINE ARMY
***OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6***
Fort Andres Bonifacio, Metro Manila

6/CMB 16 November 2015

**CYBER SECURITY BULLETIN**

**Cyber Security Bulletin: #034**

## What Is Identity Theft?

Individuals work hard to support themselves or their family. But they would be really frustrated if someone else uses their name to apply for credit cards, runs bills of thousands of pesos using the card, opens bank accounts in their name, or worse yet, commits a crime in their name.

Identity theft or ID fraud refers to crimes in which a person wrongfully obtains key pieces of personal identifying information such as date of birth, social security numbers and driver's license numbers and uses them for their own personal gain. Fraudsters create a persona similar to the victim and take advantage of his/her authority and privileges.


**Original** **Identity Theft**

**Same Name: TRENT CHARLES ARSENAUL**

### Personal Information that Can Be Stolen

All an identity thief needs is a piece of personal information, which may include:

- Names
- Addresses
- A date of birth

- A mother's maiden name
- Telephone numbers
- Social security numbers
- Driver's license numbers
- Credit card/bank account numbers
- Birth certificates
- Passport numbers

**How Do Attackers Steal Identity?**

Identity thieves may use traditional as well as Internet methods to steal identity.

**Physical Methods:**

- ✓ **Stealing Computers, Laptops, and Backup Media**: Stealing is a common method. The thieves steal hardware from places such as hotels and recreational places such as clubs or government organizations. Given adequate time, they can recover valuable data from these media.
- ✓ **Social Engineering**: This technique is the act of manipulating people's trust to perform certain actions or divulge private information without using technical cracking methods.
- ✓ **Theft of Personal Belongings**: Wallets/purses usually contain a person's credit cards and driver's license. Attackers may steal the belongings on streets or in other busy areas.
- ✓ **Mail theft and rerouting**: Mailboxes are not often protected and may contain bank documents (credit cards or account statements), administrative forms, and more. Criminals may use this information to get credit cards or for rerouting the mail to a new address.
- ✓ **Shoulder surfing**: Criminals may find user information by glancing at documents, personal identification numbers (PINs) typed into an automatic teller machine (ATM), or overhearing conversations.
- ✓ **Skimming**: Skimming refers to stealing credit/debit card numbers by using a special storage device when processing the card.
- ✓ **Pretexting**: Fraudsters may pose as executives from financial institutions, telephone companies, and other sources to obtain personal information of the user.

**Internet Methods**

- ✓ **Pharming**: Pharming is an advanced form of phishing in which the connection between the IP address and its target server is redirected. The attacker may use cache poisoning (modify the Internet address with that of a rogue address) to do this. When the user types in the Internet address, he/she is redirected to the rogue website that is similar to the original website.
- ✓ **Keyloggers and Password Stealers**: An attacker may infect the user's

computer with Trojans and then collect the keyword strokes to steal passwords, user names, and other sensitive information.

- ✓ **Phishing**: The fraudster may pretend to be a financial institution or from a reputed organization and send spam or pop-up messages to trick the users to reveal their personal information. Criminals may also use emails to send fake forms such as Internal Revenue Service (IRS) forms to gather information from the victims.
- ✓ **Hacking**: Attackers may compromise user systems and route information using listening devices such as sniffers and scanners. Attackers gain access to an abundance of data, decrypt it (if necessary), and use it for identity theft.

**What Do Attackers Do with Stolen Identity?**

Once the identity thieves collect the stolen information, they can use it for the following purposes:

**In credit card fraud, criminals may:**

Use the information to route the mail to a new residential address. This way, the victims will not be able to receive any credit card bills and the criminal can just keep piling up the credit on their cards and severely affect their credit scores.

The criminal may also use the information to apply for a new credit card in the victim's name and run high bills using the cards.

**In phone or utilities fraud, the criminal may:**

Apply for a new phone contract or a wireless connection and run up bills in users' name. Use user information to obtain utility services such as electricity, heating, or cable TV.

**In bank/finance fraud, the criminal may:**

- ✓ Generate forged checks using the victim's name or account number
- ✓ Open a bank account in the victim's name and write bad checks
- ✓ Duplicate the user's ATM or debit card and withdraw money, thus depleting the victim's bank resources
- ✓ Apply for bank loans

**In government documents fraud, the criminal may:**

- ✓ Obtain a driver's license, government ID, and more, with a user's name and the criminal's picture
- ✓ Obtain social security benefits and other government benefits that rightfully belong to the user
- ✓ File tax returns in a user's name and obtain tax benefits

**Other frauds may include:**

- ✓ Acquiring a job using the user's SSS Number
- ✓ Leasing a house in the user's name

**Identity Theft Protection Checklist**

Guidelines that help protect the user from becoming an identity theft victim include:

- ☐ Never give away the social security information or private contact information on the phone - unless you initiated the phone call
- ☐ Shred papers with personal information, credit card offers
- ☐ Ensure your name is not present in the marketers' hit lists
- ☐ Use strong passwords for all financial accounts
- ☐ Check the telephone and cell phone bills for calls you did not make
- ☐ Read before you click
- ☐ Stop pre-approved credit offers
- ☐ Read website privacy policies

**Reference:**

CSCU Module 10 Social Engineering and Identity Theft