Republic of the Philippines

NATIONAL POLICE COMMISSION

**PHILIPPINE NATIONAL POLICE**

**PHILIPPINE NATIONAL POLICE ACADEMY**

**CADET CORPS PHILIPPINE NATIONAL POLICE**

Camp General Mariano N Castañeda, Silang, Cavite

ISO 9001:2015 Certified

**MEMORANDUM**

FOR : Acting Director, PNPA

FROM : Undersigned Cadet

SUBJECT : **Reflection Paper re: Enhancement Learning Program with ATTY RICARDO BLANCAFLOR**

DATE : December 5, 2022

1. Reference: Verbal Instruction of the Acting Director, PNPA on November 14, 2022
2. This pertains to the instruction of the Acting Director, PNPA to ﻿write a one (1) page reflection on Parojinog Case on December 6, 2022 at the PNPA Heroes Hall.
3. In connection, respectfully submits the attached reflection paper composed by the undersigned cadet.

**KENNETH B. GAKO C-23114**

CDT LT 1C “B” Coy CCPNP

**CDT 1C KENNETH B. GAKO C-23114**

*BRAVO COMPANY*

REFLECTION PAPER

*CYBERCRIME PREVENTION ACT LATEST TOOL IN LAW ENFORCEMENT*

*ATTY. RICARDO R. BLANCAFLOR*

*December 5, 2022*

The speaker discusses how Frank Agnale made up every fact in the film Catch Me if You Can. He forges his identity and makes fake IDs. Given that we work in law enforcement, it is our obligation to remove these individuals. Cybercrime must be stopped, and the dangers it presents must be understood. He also talks about how Filipinos use the internet. In the Philippines, it is a fact that Filipinos are more prone to utilize the internet and run into online fraud, phishing, and photo voyeurism.

A few key definitions of computer systems, computer data, interception, service providers, and the absence of "right" were also covered. You probably already know what territorial designation is and why it matters in computer law. What city or town was the crime committed? He also discussed the relevance of the CYBERCRIME PREVENTION ACT RA 10175 and the new crimes that it addresses.

Cybercrime, often known as computer crime, is the use of a computer to advance illicit activities like fraud, the trafficking of child pornography and other intellectual property, identity theft, and privacy concerns. The relevance of cybercrime, particularly over the Internet, has increased as the computer has assumed a more significant role in business, entertainment, and government. The majority of cybercrime consists of attacks on private, public, or business information. The personal or corporate virtual body, a collection of data features used to identify persons and organizations on the Internet, is the target of the attacks even when the physical body is not. Alternatively, our internet personas are crucial components of life in the present day. We are a collection of IDs and numbers stored in numerous computer databases that are managed by both businesses and the government. The prevalence of networked computers in our lives and the flimsiness of concepts like personal identification are both brought home by cybercrime.

Despite their best efforts to hide it, cybercriminals leave evidence of their identities and whereabouts, much like people walking on the ground leave trails that a good tracker can follow. However, worldwide cybercrime norms must be created in order to follow such signals across international borders.