

PHILIPPINE NATIONAL POLICE



PRIMER ON CYBERCRIME INVESTIGATION

MARCH 2023

PRIMER ON CYBERCRIME INVESTIGATION

PNP Anti-Cybercrime Group
Camp BGen Rafael T Crame, Quezon City,
Philippines
2023



Republic of the Philippines
DEPARTMENT OF THE INTERIOR AND LOCAL GOVERNMENT
DILG-NAPOLCOM Center, EDSA cor. Quezon Avenue, West Triangle, Quezon City
www.dilg.gov.ph

MESSAGE

In behalf of the Department of the Interior and Local Government (DILG), let me express my warmest greetings and congratulations to the **Philippine National Police (PNP) -Anti-Cybercrime Group (ACG)** for coming up with this **Primer on Cybercrime Investigation!**

My commendations, as well, to the ACG-Technical Working Group who tirelessly worked in partnership with the Department of Justice (DOJ) in producing this fundamental and up-to-date primer. This primer will make it handy for our cybercops to ensure a more efficient and effective implementation and enforcement of pertinent laws on cybercrime and other cyber-related crimes.

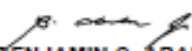


This Primer aims to provide the necessary assistance to our cybercop investigators in endorsing cases before the National Prosecution Service. This publication is a tool in keeping with the policy of the state to keep law enforcement agencies abreast with the development in the field of law, here and abroad concerning cybersecurity, for the successful prosecution of criminals.

As part of my commitment to uphold rule of law, rest assured of my full support towards the attainment of the continuing success of your endeavor in cyber environment and in ensuring the safety of Filipinos, especially women and children, and other vulnerable sectors in cyberspace.

May you keep in mind and heart your learning from this Primer and always live by your oath as public safety heroes.

Makakaasa po kayo sa inyong Kagawarang matino, mahusay, at maaasahan sa ating ilang hangaring pagtibayin ang kagalingan ng PNP-ACG para sa kaligtasan ng mga Filipino netizens!


ATTY. BENJAMIN C. ABALOS, JR.
Secretary

MESSAGE

The Philippine National Police is pleased to provide the Cybercop Investigators with this Primer which outlines the substantive and procedural aspect of Republic Act No. 10175, also known as "The Cybercrime Prevention Act of 2012"; other related laws; and the Rule on Cybercrime Warrants pursuant to A.M. 11-17-03 of the Supreme Court. The drafting of this Primer was through the efforts of the Anti-Cybercrime Group (ACG) personnel in collaboration with the Department of Justice-Office of the Cybercrime.




It has always been the intention of the organization to equip its investigators with sufficient knowledge in the field of investigation in this era where perpetrators are taking advantage of their anonymity in the commission of crime. This primer will aid the organic members of the PNP ACG to be more competent in the field of investigation amidst the continuing and alarming increase of cases committed by means of Information and Communication Technology.

This primer will serve as a guide for investigators from the different PNP Regional, Provincial, and District Police Offices, who are handling cyber-related offenses.

Thank you and congratulations to the PNP ANTI-CYBERCRIME GROUP for a job well done.

Life is beautiful.


RODOLFO S. AZURIN, JR.
Police General
Chief, PNP

"Life is Beautiful... Kalighasan Nyo, Sagot Ko. Tulang-tulang Tiyo."



Republic of the Philippines
NATIONAL POLICE COMMISSION
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
DIRECTORATE FOR INVESTIGATION AND DETECTIVE MANAGEMENT
Camp BGen Rafael T. Crame, Quezon City

MESSAGE

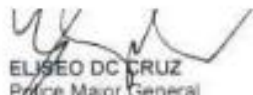
The Philippine National Police – Anti Cybercrime Group (PNP-ACG) has been relentless in its efforts to equip its personnel to combat cybercrimes. With the various challenges that law enforcement are facing on cybercrime, we need to cope up and provide support to our investigators.

This Primer will serve as a guide for our PNP personnel to ensure that proper steps are being followed in the conduct of Cybercrime Investigation

May the challenges and complexities of the cyber threat be confronted squarely, with a firm resolve to overcome and defeat it.

Congratulations everyone!




ELISEO DC CRUZ
Police Major General
Director, DIDM

"Life Is Beautiful...Kaligtasan Nyo, Sagot Ko. Tulong-tulong Tayo."



Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp 8 Gen Rafael T Crame, Quezon City



PREFACE

The Philippine National Police Anti-Cybercrime Group (PNP ACG) continues to progress on transformation milestones in its journey of becoming a highly responsive and dynamic unit towards a safer cyber environment.

To address the issues on cybercrime, Republic Act (RA) No. 10175 otherwise known as the "Cybercrime Prevention Act of 2012" was enacted on September 12, 2012. Said law penalizes cybercrimes and also mandated the PNP and NBI to organize cybercrime units manned by special investigators to exclusively handle cases involving violations of RA No. 10175.



Among the PNP ACG functions are the following: investigate all cybercrimes where computer systems are involved, conduct data recovery and forensic analysis on computer systems and other electronic evidence seized, and formulate guidelines on investigation.

In January 2022¹, there are 76.01 million internet users in the Philippines wherein the country's internet penetration rate stood at 68 percent of the total population at the start of 2022. However, the availability and convenience of the internet did not only captivate the Filipinos, but launched a breeding ground for cybercriminals.

Thus, with the continuing challenges on cybercrime investigation, the PNP ACG prepared a primer to be used by the investigators in filing cybercrime and cyber-related cases before the Prosecutor's Office. This Primer, however is supplementary to the existing Revised PNP Operational Procedures and other related DIDM issuances.

JOEL B. DORIA
Police Brigadier General
Director, Anti-Cybercrime Group

ACKNOWLEDGEMENT

It is with great pleasure that I present to you the Primer on Cybercrime Investigation.

In year 2000, the most notorious "virus story" took place wherein over ten million computers from around the world were infected. This devastating event in cyber-history was written by a young, tech-savvy Filipino who created the "I Love You Virus."

Over two decades later, its impact has remained breeding, diversifying, and growing. This became more evident when cyberspace has totally become an extension of the physical world and digital transformation has increased our reliance on connectivity. As a result, we in law enforcement are compelled to repurpose our cybercrime responses.

Under the mandate of "ensuring a safe and secure cyberspace for Filipinos," the PNP Anti-Cybercrime Group (ACG) has been thriving not just to deliver, but also to strengthen policing capabilities to respond to the growing menace of cybercrime. Among the Group's biggest objectives at present is to enhance the skills of its investigators and increase its efficacy in terms of cyber response.

Optimistically, this Primer shall provide cybercrime investigators with a valuable resource to form part of our ongoing pursuit of developing the overall Anti-Cybercrime strategy of the PNP. It is likewise hoped that this Primer will be an effective tool for designing more robust strategies and initiatives to overcome challenges that are pronged in cybercrime investigation.

Lastly, I recommend this Primer to other PNP uniformed personnel who serve as first responders considering that in this now highly digitalized world, most incidents involve the use of digital devices and the internet.

To the men and women of the PNP ACG and those who particularly contributed in the creation of this Primer. Especially, the Current Technical Working Group led by PCOL VILLAMOR Q TULIAO, PCOL VINA H GUZMAN, PCOL NOVA G DE CASTRO, PCOL REYNALDO SG DELA CRUZ, PCOL DOMINGO D SORIANO, PCOL ALEJANDREA G SILVIO, PCOL RHODORA D MAYLAS, PCOL IRENE C CENA, PLTCOL DEODENNIS JOY E MARMOL, PCOL FERDINAND S RAYMUNDO, PLTCOL ROBERT D BONGAYON, JR, PLTCOL JAY D GUILLERMO and PCPT JULIUS VINCENT T LIBANG and the Previous Technical Working Group led by PCOL BERNARD R YANG, PCOL ALBERTO D GARCIA, JR, PCOL MARLO A CASTILLO, PCOL FIDEL B FORTALEZA, JR, PCOL ZALDY K ABELLERA, and PLTCOL ALLAN D DOCYOGEN thank you very much. *Mabuhay tayong lahat.*



JOEL B. DORIA

Police Brigadier General
Director, Anti-Cybercrime Group

TABLE OF CONTENTS

PRELIMINARY PAGES

Message of the SILG	i
Message of the CPNP	ii
Message of TDIDM	iii
Preface	iv
Acknowledgement	v

CHAPTER 1 INTRODUCTION

Section 1-1	Background	1
Section 1-2	Legal Basis	2

CHAPTER 2 CORE CYBERCRIMES

Section 2-1	“Illegal Access”	5
	Section 4(a)(1) RA 10175	
Section 2-2	“Illegal Interception”	8
	Section 4(a)(2) RA 10175	
Section 2-3	“Data Interference”	12
	Section 4(a)(3) RA 10175	
Section 2-4	“System Interference”	15
	Section 4(a)(4) RA 10175	
Section 2-5	“Misuse of Device”	18
	Section 4(a)(5) RA 10175	
Section 2-6	“Cyber-Squatting”	22
	Section 4(a)(6) RA 10175	
Section 2-7	“Computer-Related Forgery”	26
	Section 4(b)(1) RA 10175	
Section 2-8	“Computer-Related Fraud”	29
	Section 4(b)(2) RA 10175	
Section 2-9	“Computer-Related Identity Theft”	33
	Section 4(b)(3) RA 10175	

Section 2-10	“Cybersex” Section 4(c)(1) RA 10175	36
Section 2-11	“Child Pornography” Section 4(c)(2) RA 10175	39
Section 2-12	“Libel” Section 4(c)(4) RA 10175	41
Section 2-13	“Other Offenses” Section 5 RA 10175	44
CHAPTER 3	CYBER-RELATED CRIMES	
Section 3-1	“Unlawful Use of Means of Publication and Unlawful Utterance” (Art. 154, RPC)	47
Section 3-2	“Grave Threat” (Art.282, RPC)	49
Section 3-3	“Grave Coercion” (Art. 286, RPC)	51
Section 3-4	“Unjust Vexation” (Art.287, RPC)	54
Section 3-5	“Swindling/Estafa” (Art.315, RPC) as amended by RA 101075	56
Section 3-6	“Robbery with Intimidation if Persons” (Art. 294, RPC)	60
Section 3-7	“Access Device Regulation Act” (RA 8484)	63
Section 3-8	“Access Devices Regulation Act” (RA 11449)	67
Section 3-9	“Anti-Photo and Video Voyeurism” (RA No. 9995)	71
Section 3-10	“Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or	74

	Exploitation Materials (CSAEM) Act” (RA No. 11930)	
Section 3-11	“Anti-Violence against Women and Children” (RA No. 9262)	80
Section 3-12	“Special Protection against Child Abuse, Exploitation and Discrimination, and for other purposes” (RA No. 7610)	85
Section 3-13	“Safe Spaces Act” (RA No. 11313)	88
Section 3-14	“Migrant Workers and Overseas Filipino Act of 1995, as amended xx” (RA No. 8042 as amended by RA 10022)	91
Section 3-15	“Intellectual Property Code of the Philippines” (RA No. 8293)	97
Section 3-16	“Obstruction of Justice” (PD No. 1829) in relation to RA 10175 and Sec 27 of A.M. 17-11-03 (Rule on Cybercrime Warrant	107
APPENDIX		110
ANNEXES		117
REFERENCES		197
TECHNICAL WORKING GROUP		198
PNP ACG HOTLINE NUMBERS		200

CHAPTER 1

INTRODUCTION

Section 1-1 Background

1.1 Overview. The increase of crimes committed through information and communications technologies has become a challenge to law enforcement. Cybercrime around the globe continues to grow in size and scope, creating new and changing existing forms of crime with the stroke of a keyboard. This threat knows no boundaries with a single malicious cybercrime incident able to hit victims in numerous jurisdictions.

Cybercriminals do not just defraud, harass, stalk, abuse and threaten innocent citizens online, but they also abuse the internet for money laundering, trafficking illegal goods like drugs, guns, Child abuse materials and even live-stream murders, abuses and terrorist acts. The internet and electronic devices are also abused to plan, coordinate and even facilitate traditional crimes in the physical world (Guide for First Responders to Cybercrime Investigations, C-PROC, Version 5, Page 5, October 2021).

On December 9, 2016, then President Rodrigo R Duterte signed the BUDAPEST Convention on Cybercrime which was ratified by the Philippine Senate on February 19, 2018. The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest

Convention from the Council of Europe, is the first international treaty on cybercrime.

However, prior to accession of the Philippines to the treaty, RA No. 10175 or the Cybercrime Prevention Act of 2012 was enacted which provided the substantive law on cybercrime and procedures on the search, seizure, and examination of digital evidence. It also mandated the National Bureau of Investigation and the Philippine National Police to be responsible for the efficient and effective law enforcement of the provisions of the Act.

This Primer contains the basic list of the pieces of evidence in the conduct of cybercrime and cyber-related investigation to guide our investigators in filing cases under RA No. 10175 to include Sim Card registrations, Text and Instant Messages, Audio/Video Files, IP address, social media post, files and documents from Drives, Electronic Financial Transactions and Email.

Section 1-2 Legal Basis

1.2 Section 4 of RA 10175 – Cybercrime Offenses

- a. Offenses against the confidentiality, integrity and availability of computer data and systems
 - 1) Illegal Access;
 - 2) Illegal Interception;

- 3) Data Interference;
- 4) System Interference;
- 5) Misuse of Devices; and
- 6) Cyber-squatting.
- b. Computer-related Offenses
 - 1) Computer-related Forgery;
 - 2) Computer-related Fraud; and
 - 3) Computer-related Identity Theft.
- c. Content-related Offenses
 - 1) Cybersex;
 - 2) Child Pornography; and
 - 3) Unsolicited Commercial Communications.

1.3 Section 5 of RA 10175 – Other Offenses

- a. Aiding or Abetting in the Commission of Cybercrime; and
- b. Attempt in the Commission of Cybercrime.

1.4 Section 6 of RA 10175 - All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be

covered by the relevant provisions of this Act: Provided, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be

CHAPTER 2

CORE CYBERCRIMES

Section 2-1 “Illegal Access” Section 4(a)(1) RA No. 10175

2.1 Definition. The access to the whole or any part of a computer system without right or in excess of authority.

2.2 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant (alleging that the suspect committed the act without right or in excess of authority, or not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law);
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of call logs, computer logs, network logs, and system logs;
- e. Print Screen and/or Screen shots of text messages from the alleged fraudster/scammer, email/s and phishing link/s in PDF form (if applicable);

- f. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- g. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- h. Details of any method of payment (if applicable);
- i. Consent of victim to examine computer or digital devices;
- j. Duly approved request for Digital Forensic Examination;
- k. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- l. Affidavit/Certificate of preservation of evidence (manner of preservation);
- m. Case Referral (inquest) or Case Investigation Report (regular filing);
- n. NPS Investigation Data Form;

Additional requirements if the offended party is a juridical person:

- o. Board resolution for the company representative; and

- p. IT Report (fraud management report)/affidavit.

2.3 Notes

- a. Use of timestamp in preserving the online post. When using software tools that are freely available, use two applications for validation;
- b. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- c. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- d. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- e. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- f. The use of the term “hacking” in cases involving Illegal Access is discouraged;
- g. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure

submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and

- h. Evaluate for possible Money Laundering investigation (conduct asset tracking and recommend for freeze order, civil and criminal forfeiture).

Section 2-2 “Illegal Interception” Section 4(a)(2) RA No. 10175

2.4 Definition. The interception made by technical means without right or in excess of authority of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

Provided, however, that it shall not be unlawful for an officer, employee, or agent of a service provider, whose facilities are used in the transmission of communications, to intercept, disclose or use that communication in the normal course of employment, while engaged in any activity that is necessary to the rendition of service or to the protection of the rights or property of the service provider, *except* that the latter shall not utilize service observing or random monitoring other than for purposes of mechanical or service control quality checks.

2.5 Pieces of Evidence

- a. Incident Record Form;

- b. Affidavit of Complainant (allege that the suspect committed the act without right or in excess of authority, or not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law);
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of call logs, computer logs, network logs, and system logs;
- e. Print Screen and/or Screen Shots of text messages from the alleged fraudster/scammer, email/s and phishing link in PDF form (if applicable);
- f. For Video recordings, store in optical disk or flash drives and follow proper chain of custody;
- g. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- h. Details of any method of payment (if applicable);
- i. Consent of victim to examine computer or digital devices;

- j. Duly approved request for Digital Forensic Examination;
- k. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- l. Affidavit/Certificate of preservation of evidence (manner of preservation);
- m. Case Referral (inquest) or Case Investigation Report (regular filing);
- n. NPS Investigation Data Form;

Additional requirements if the offended party is a juridical person:

- o. Board resolution for the company representative; and
- p. IT Report (fraud management report)/affidavit.

2.6 Notes

- a. Conduct of Vulnerability Assessment and Penetration Testing (VAPT) if applicable;
- b. An example of Illegal Interception is a “man-in-the-middle attack”, which enables an offender to eavesdrop on communications between the sender and the receiver and/or impersonate the sender and/or receiver and communicate on their behalf;

- c. Request assistance from trained digital forensic examiners on CLOUD investigation;
- d. Use of Timestamp in preserving the online post. When using software tools that are freely available, use two applications for validation;
- e. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- f. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- g. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- h. If the post had already been deleted when the case was reported to ACG, the complainant has to comply with the requirement stated in Sec. 2 Rule 11 in relation to Rule 5 on Rules of Electronic Evidence. (A.M. No. 01-07-01-SC);
- i. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- j. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and

implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and

- k. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

Section 2-3 “Data Interference” Section 4(a)(3) RA No. 10175

2.7 Definition. The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right including the introduction or transmission of viruses.

2.8 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant (allege that the suspect committed the act without right or in excess of authority, or not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law);
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of call logs, computer logs, network logs, and system logs;

- e. Print Screen and/or Screen Shots of text messages from the alleged fraudster/scammer, email/s and phishing link in PDF form (if applicable);
- f. If the case involves website defacement, present a screenshot of the defaced website;
- g. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- h. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with A.M. No. 01-07-01-SC;
- i. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- j. Affidavit/Certificate of preservation of evidence (manner of preservation);
- k. Case Referral (inquest) or Case Investigation Report (regular filing);
- l. NPS Investigation Data Form;

Additional requirements if the offended party is a juridical person:

- m. Board resolution for the company representative; and
- n. IT Report (fraud management report)/affidavit.

2.9 Notes

- a. Conduct of Vulnerability Assessment and Penetration Testing (VAPT) if applicable;
- b. Use of timestamp in preserving the online post. When using software tools that are freely available, use two applications for validation;
- c. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- d. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- e. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- f. If the post had already been deleted when the case was reported to ACG, the complainant has to comply with the requirement stated in Sec. 2 Rule 11 in

relation to Rule 5 on Rules of Electronic Evidence. (A.M. No. 01-07-01-SC);

- g. Proper collection, inventory, marking, and preservation of recovered/seized evidence; and
- h. Evaluate for possible Money Laundering investigation (conduct asset tracking and recommend for freeze order, civil and criminal forfeiture).

Section 2-4 “System Interference” Section 4(a)(4) RA No. 10175

2.10 Definition. The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data messages, without right or authority, including the introduction or transmission of viruses.

2.11 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant (allege that the suspect committed the act without right or in excess of authority, or not covered by established legal defenses, excuses, court

orders, justifications, or relevant principles under the law);

- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of call logs, computer logs, network logs, and system logs;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- g. Affidavit of consent of the victim (owner of the computer);
- h. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- i. Affidavit/Certificate of preservation of evidence (manner of preservation);
- j. Case Referral (inquest) or Case Investigation Report (regular filing);
- k. NPS Investigation Data Form;

Additional requirements if the offended party is a juridical person:

- i. Board resolution for the company representative; and
- m. IT Report (fraud management report)/affidavit.

2.12 Notes

- a. Conduct of Vulnerability Assessment and Penetration Testing (VAPT) (if applicable);
- b. An example of System Interference is a “Denial of Service Attack (DoS attack)”, which interferes the systems by overwhelming servers and/or intermediaries (e.g., routers) with requests to prevent legitimate traffic from accessing a site and/or using a system. A “Distributed Denial of Service Attack (DDos attack)” refers to the use of multiple computers and other digital technologies to conduct coordinated attacks with the intention of overwhelming servers and/or intermediaries to prevent legitimate user’s access;
- c. Use of timestamp in preserving the online post. When using software tools that are freely available, use two applications for validation;
- d. Attribute the device with the suspect (description of the device, physical location,

IP addresses, domain names, other potential identifiers of digital devices, exact time);

- e. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- f. If the post had already been deleted when the case was reported to ACG, the complainant has to comply with the requirement stated under Sec. 2 Rule 11 in relation to Rule 5 on Rules of Electronic Evidence. (A.M. No. 01-07-01-SC;
- g. Proper collection, inventory, marking, and preservation of recovered/seized evidence; and
- h. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

Section 2-5 “Misuse of Device” Section 4(a)(5) RA No. 10175

2.13 Definition. The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

- a. A device, including a computer program, designed or adapted primarily for the

purpose of committing any of the offenses under this Act; or

- b. A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.
- c. The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section.

Provided, that no criminal liability shall attach when the use, production, sale, procurement, importation, distribution, otherwise making available, or possession of computer devices or data referred to in this section is for the authorized testing of a computer system.

2.14 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant (allege that the suspect committed the act without right or in excess of authority, or not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law);
- c. Affidavit of Witness;

- d. Print Screen and/or Screen Shots of call logs, computer logs, network logs, and system logs;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- g. Affidavit of consent of the victim (owner of the computer);
- h. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- i. Affidavit/Certificate of preservation of evidence (manner of preservation);
- j. Case Referral (inquest) or Case Investigation Report (regular filing);
- k. NPS Investigation Data Form;

Additional requirements if the offended party is a juridical person:

- l. Board resolution for the company representative; and

- m. IT Report (fraud management report)/affidavit.

2.15 Notes

- a. Use of timestamp in preserving the online post. When using software tools that are freely available, use two applications for validation;
- b. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- c. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- d. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- e. If the post had already been deleted when the case was reported to ACG, the complainant has to comply with the requirement stated under Sec. 2 Rule 11 in relation to Rule 5 on Rules of Electronic Evidence. (A.M. No. 01-07-01-SC;
- f. Proper collection, inventory, marking, and preservation of recovered/seized evidence;

- g. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian;
- h. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture); and
- i. Misuse of device can be filed even if the crime committed is not one of the core cybercrimes. On the other hand, the commission of a core cybercrime is necessary if the complaint filed for Misuse of Device is under Section 4 (a)(5)(ii), which punishes mere possession with intent to use said devices for the purpose of committing any of the offenses under Section 4 of R.A. No. 10175.

Section 2-6 “Cyber-Squatting” Section 4(a)(6) RA No. 10175

2.16 Definition. The acquisition of a domain name over the internet in a bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

- a. Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;
- b. Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and
- c. Acquired without right or with intellectual property interests in it.

2.17 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant (allege that the suspect committed the act without right or in excess of authority, or not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law);
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of the authentic website as certified by the representative of the company or by its owner;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Certificate of Extraction from Cyber Patroller/Investigator in relation to the

acquisition of domain name of the authentic website and its screen shots;

- g. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- h. Certificate of registration from SEC;
- i. For single proprietorship and partnership - DTI Certificate;
- j. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- k. Certificate of registration of hosting company (GoDaddy, Amazon web hosting etc.);
- l. Certificate of registration of domain name;
- m. Trademark Registration from IPO, if applicable;
- n. Case Referral (inquest) or Case Investigation Report (regular filing);
- o. NPS Investigation Data Form;

Additional requirements if the offended party is a juridical person:

- p. Board resolution for the company representative; and
- q. IT Report (fraud management report)/affidavit.

2.18 Notes

- a. Use of timestamp in preserving the online post. When using software tools that are freely available, use two applications for validation;
- b. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- c. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- d. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- e. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- f. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure

submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and

- g. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

Section 2-7 “Computer-Related Forgery” Section 4(b)(1) RA No. 10175

2.19 Definition

- a. The input, alteration, or deletion of any computer data without right resulting in inauthentic data with intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; or
- b. The act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

2.20 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant (allege that the suspect committed the act without right or in excess of authority, or not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law);
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of call logs, computer logs, network logs, emails, and system logs;
- e. For Video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- g. Affidavit of consent of the owner of the device;
- h. Copy of the original and forged data must be presented for comparison;

- i. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- j. Case Referral (inquest) or Case Investigation Report (regular filing);
- k. NPS Investigation Data Form;

Additional requirements if the offended party is a juridical person:

- l. Board resolution for the company representative; and
- m. IT Report (fraud management report)/affidavit.

2.21 Notes

- a. Use of timestamp in preserving the online post. When using software tools that are freely available, use two applications for validation;
- b. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- c. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;

- d. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- e. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- f. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and
- g. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

Section 2-8 “Computer-Related Fraud” Section 4(b)(2) RA No. 10175

2.22 Definition. The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent, *Provided*, that if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

2.23 Pieces of Evidence

- a. Incident Record Form;

- b. Affidavit of Complainant (allege that the suspect committed the act without right or in excess of authority, or not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law);
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of call logs, computer logs, network logs, emails, and system logs;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- g. Authenticated copy of bank statement/transactions (if applicable);
- h. Affidavit of consent of the victim (owner of the computer);
- i. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);

- j. Case Referral (inquest) or Case Investigation Report (regular filing);
- k. NPS Investigation Data Form;

Additional requirements if the offended party is a juridical person:

- l. Board resolution for the company representative; and
- m. IT Report (fraud management report)/affidavit.

2.24 Notes

- a. Computer-related fraud includes many online swindles that involve false or misleading promises of love and companionship, property (inheritance scams), and money and wealth (lottery scams, investment fraud, inheritance) by using social engineering, which is the practice of “manipulating, deceiving, influencing, or tricking individuals into divulging confidential information or performing acts that will benefit the social engineer in some way.” (source: UNODC Cybercrime Module);
- b. For cases involving crypto currency: Tracing/Tracking of cryptocurrency;
- c. Use of Timestamp in preserving the online post. When using software tools that are

freely available, use two applications for validation;

- d. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- e. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- f. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- g. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- h. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and
- i. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

**Section 2-9 “Computer-Related Identity Theft”
Section 4(b)(3) RA No. 10175**

2.25 Definition. The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: Provided, that if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

2.26 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant (allege that the suspect committed the act without right or in excess of authority, or not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law);
- c. Affidavit of Witness;
- d. Affidavit of Denial;
- e. Print Screen and/or Screen Shots of call logs, conversation, emails in PDF form;
- f. Print Screen and/or Screen Shots of the original (if applicable) and fake accounts;
- g. For video recordings, store in optical disk or flash drives and follow proper chain of custody;

- h. Social Media Exploitation Report;
- i. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- j. Authenticated copy of bank statement/transactions if used in committing fraudulent transactions;
- k. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- l. Case Referral (inquest) or Case Investigation Report (regular filing);
- m. NPS Investigation Data Form;

Additional requirements if the offended party is a juridical person:

- n. Board resolution for the company representative; and
- o. IT Report (fraud management report)/affidavit.

2.27 Notes

- a. Use of timestamp in preserving the online post. When using software tools that are

freely available, use two applications for validation;

- b. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- c. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- d. If the post has already been deleted when the case was reported to ACG, there must be compliance with *Sec. 2 Rule 11 in relation to Rule 5 on Rules of Electronic Evidence (Authentication of Electronic Evidence)*;
- e. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- f. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- g. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and
- h. Evaluate for possible Money Laundering investigation (conduct asset tracing and

recommend for freeze order, civil and criminal forfeiture).

Section 2-10 “Cybersex” Section 4(c)(1) RA No. 10175

2.28 Definition. The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

Cybersex involving a child shall be punished in accordance with the provision on child pornography of the Act.

Where the maintenance, control or operation of cybersex likewise constitutes an offense punishable under Republic Act No. 9208, as amended, a prosecution under the Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws, including R.A. No. 9208, consistent with Section 8 hereof. (IRR)

2.29 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant/ Deponent;
- c. Affidavit of Witness;
- d. Dispatch of poseur police operative;

- e. Names of the maintainer and employees;
- f. Approximate number of computers and other gadgets;
- g. SEC, DTI and LGU permits;
- h. Photographs of the vicinity/establishments;
- i. Payment records/proof of transaction;
- j. Printed images of the cybersex transaction;
- k. ISP records if available;
- l. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- m. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- n. Case Referral (inquest) or Case Investigation Report (regular filing);
- o. NPS Investigation Data Form; and
- p. Computers, tablets, mobile phones, and other devices seized pursuant to a WSSECD, if applicable.

2.30 Notes

- a. Check for other laws violated (SEC, FDA, etc.);

- b. Conduct of surveillance;
- c. Proper tagging of suspects vis-à-vis the device being used during WSSECD implementation;
- d. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- e. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- f. Submission of digital forensic examination result and affidavit of digital forensic examiner;
- g. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and
- h. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

NOTE: Repealed by RA No. 11930

**Section 2-11 “Child Pornography” Section 4(c)(2)
RA No. 10175**

2.31 Definition. The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: Provided, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

2.32 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of the Complainant (Parents/Guardian)/Nominal Representative;
- c. Affidavit of Witnesses;
- d. Birth Certificate of the Minor;
- e. Relevant conversation of the suspect and the victim in PDF form;
- f. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- g. Affidavit of Authentication of Electronic Evidence;
- h. Copy of Explicit Videos and Photos of the Victim;

- i. Affidavit of DSWD if the parents/guardian are not willing to file the case;
- j. National Center for Mental Health (NCMH) as the Institution-in-Charge for the Psychological assessment/examination of victim;
- k. Preservation, application of cybercrime warrant, court warrant and compliance (if applicable);
- l. Case Referral (inquest) or Case Investigation Report (regular filing); and
- m. NPS Investigation Data Form.

2.33 Notes

- a. ISPs are duty bound to report child pornography using it facility or server;
- b. ISPs are required to disclose data without a need for a WDCD;
- c. If the victim is outside the country, include the assessment from counterpart agencies;
- d. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;

- e. The complainant will execute the Affidavit of Authentication of Electronic Evidence if the post has already been deleted when the case was reported to ACG;
- f. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- g. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest and search warrant; Affidavit of Recording Officer; Affidavit of Data Custodian; and
- h. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

NOTE: Repealed by RA No. 11930

Section 2-12 “Libel” Section 4(c)(4) RA No. 10175

2.34 Definition. The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

This provision applies only to the original author of the post or online libel and not to others who simply receive the post and react to it.

- a. Imputation of a crime or a vice, or defect, real or imaginary or any act, omission, condition, status or circumstance tending to cause the dishonor, discredit or contempt of a natural or juridical person or to blacken the memory of one who is dead;
- b. Malice, either in law or in fact;
- c. Publication of the imputation and
- d. Identifiability of the victim.

2.35 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant;
- c. Affidavit of Witnesses (at least two witnesses);
- d. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- e. Affidavit of extraction as to the existence of FB account of the victim and the suspect;

- f. Print Screen and/or Screen Shots of the Libelous Post in PDF form;
- g. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- h. Affidavit/Certificate of preservation of evidence (manner of preservation);
- i. Case Referral (inquest) or Case Investigation Report (regular filing);
- j. NPS Investigation Data Form; and

Additional requirements if the offended party is a juridical person:

- k. Board resolution for the company representative.

2.36 Notes

- a. Cyber Libel should be filed to the place where the complainant resides at the time of the commission of the offense;
- b. In the Affidavit of the Complainant and Witness, indicate where the online post was discovered, to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- c. On WDCD against Facebook for Cyber Libel: Facebook will not comply with the cyber warrant since libel is not punishable in the

US, unless, there are other crimes committed such as terrorism or child pornography;

- d. For ISP located outside Philippines – the implementation of the cyber warrant should be endorsed by D, ACG to DOJ OOC;
- e. Affidavit/Certificate of Extraction – exclusive for cases handled by PNP ACG and other PNP Units;
- f. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian;

Section 2-13 “Other Offenses” Section 5, RA No. 10175

2.37 Definition

- a. Aiding or Abetting in the Commission of Cybercrime - Any person who willfully abets or aids, *or financially benefits* in the commission of any of the offenses enumerated in this Act, *except with respect to Sections 4 (c) (2) on Child Pornography and 4 (c) (4) on online Libel (IRR)*; and

- b. Attempt in the Commission of Cybercrime - Any person who willfully attempts to commit any of the offenses enumerated in this Act, except with respect to *Sections 4 (c) (2) on Child Pornography and 4 (c) (4) on online Libel (IRR)*.

2.38 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant;
- c. Affidavit of Witness;
- d. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- e. Job Description of Suspect/s;
- f. Case Referral (inquest) or Case Investigation Report (regular filing);
- g. NPS Investigation Data Form;

Additional requirements if the injured party is a juridical person:

- h. Board resolution for the company representative; and

- i. IT Report (fraud management report)/affidavit.

2.39 Notes

- a. Excluded: Online Libel and Child Pornography;
- b. In case of numerous suspects, proper tagging of suspects and devices;
- c. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- d. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- e. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture); and
- f. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian.

CHAPTER 3

CYBER-RELATED CRIMES

Section 3-1 “Unlawful Use of Means of Publication and Unlawful Utterance” (Art. 154, RPC)

3.1 Definition. Any person who by means of printing, lithography, or any other means of publication shall publish or cause to be published as news any false news which may endanger the public order, or cause damage to the interest or credit of the State.

(Committed by, through and with the use of information and communications technology.)

3.2 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant;
- c. Affidavit of Witnesses (at least two witnesses);
- d. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;

- e. Print Screen and/or Screen Shots as to the existence of FB account of the victim and the suspect;
- f. Print Screen and/or Screen Shots of the Fake News Post in PDF form;
- g. Affidavit/Certificate of preservation of evidence (manner of preservation);
- h. Certification from concerned government agencies (if applicable);
- i. Preservation, application of cybercrime warrant, court warrant and compliance (if applicable);
- j. Case Referral (inquest) or Case Investigation Report (regular filing); and
- k. NPS Investigation Data Form.

3.3 Notes

- a. If the fake news affects a government agency, there should be a nominal complainant from said agency;
- b. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;

- c. If the post has been deleted, *compliance with the requirement stated under Sec. 2 Rule 11 in relation to Rule 5 on Rules of Electronic Evidence (A.M. No. 01-07-01-SC) (Authentication of electronic evidence); and*
- d. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian.

Section 3-2 “Grave Threat” (Art. 282, RPC)

3.4 Definition. Any person who shall threaten another with the infliction upon the person, honor, or property of the latter or of his family of any wrong amounting to a crime.

If the threat demanding money or imposing any other condition, even though not unlawful, and said offender shall either have attained or not attained his purpose.

If the threat shall not have been made subject to a condition.

(Committed by, through and with the use of information and communications technology.)

3.5 Pieces of Evidence

- a. Incident Record Form;

- b. Affidavit of Complaint;
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of threatening post, online conversation, account used by the suspect in PDF form;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- g. Other related documents (police report, photographs, etc);
- h. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- i. Case Referral (inquest) or Case Investigation Report (regular filing); and
- j. NPS Investigation Data Form.

3.6 Notes

- a. Affidavit/Certificate of Extraction – exclusive for cases handled by PNP ACG and other PNP Units;

- b. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- c. Proper collection, inventory, marking, and preservation of recovered/seized evidence; and
- d. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian.

Section 3-3 “Grave Coercion” (Art. 286, RPC)

3.7 Definition

- a. Any person who prevents another from doing something not prohibited by law;
- b. Any person who compels another to do something against his will be it right or wrong;
- c. The prevention or compulsion is effected by violence, threats, or intimidation;
- d. The offender had no right to do so; and
- e. Other analogous acts.

(Committed by, through and with the use of information and communications technology.)

3.8 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant;
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of threatening post, online conversation, account used by the suspect in PDF form;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- g. Affidavit/Certificate of preservation of evidence (manner of preservation);
- h. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);

- i. Other related documents (police report, photographs, etc);
- j. Case Referral (inquest) or Case Investigation Report (regular filing); and
- k. NPS Investigation Data Form.

3.9 Notes

- a. Affidavit/Certificate of Extraction – exclusive for cases handled by PNP ACG and other PNP Units;
- b. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- c. In case of entrapment, attached the booking/mugshot, medical examination result, affidavit of arrest and seizure, and inventory receipt of seized evidence;
- d. Proper collection, inventory, marking, and preservation of recovered/seized evidence; and
- e. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian.

Section 3-4 “Unjust Vexation” (Art. 287, RPC)

3.10 Definition

- a. The offender seizes anything from another;
- b. The purpose of seizure is to apply the same to the victim's debt; and
- c. Other analogous acts.

(Committed by, through and with the use of information and communications technology.)

3.11 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant;
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of threatening post, online conversation, account used by the suspect in PRINT SCREEN FORMAT and PDF FORMAT;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who

had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;

- g. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- h. Affidavit/Certificate of preservation of evidence (manner of preservation);
- i. Other related documents (police report, photographs, etc);
- j. Certificate to file Action is needed – if the victim and the suspect are residents of same barangay or residents of different barangay of the same city/municipality;
- k. Case Investigation Report (regular filing); and
- l. NPS Investigation Data Form.

3.12 Notes

- a. Accomplished National Telecommunications Commission Complaint Form if the complainant intends to request for the take down of mobile numbers;
- b. Affidavit/Certificate of Extraction – exclusive for cases handled by PNP ACG and other PNP Units;
- c. In the Affidavit of the Complainant and Witness, indicate the place of the

commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor; and

- d. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian.

Section 3-5 “Swindling/Estafa” (Art. 315, RPC) as amended by RA 10175

3.13 Definition

- a. There is deceit;
- b. There is damage or prejudice to the offended party;
- c. The deceit is through unfaithfulness or abuse of confidence;
- d. Some by means of false pretenses or fraudulent acts or means; and
- e. Other analogous acts.

(Committed by, through and with the use of information and communications technology.)

3.14 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant;
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of online conversation, account used by the suspect, acknowledgement of payments in PRINT SCREEN and PDF form;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Certificate of extraction as to the existence of the account used by perpetrator;
- g. Proof of Transactions;
- h. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- i. Authenticated copy of Statement of Account (if applicable);
- j. Bank Dispute Reports (if applicable);

- k. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- l. Case Referral (inquest) or Case Investigation Report (regular filing);
- m. NPS Investigation Data Form;

Additional requirement if Crypto-currency (Portal of Subject Platform):

- n. Screen shot of wallet address; and
- o. Tracing methods made by the IOC.

3.15 Notes

- a. Affidavit/Certificate of Extraction – exclusive for cases handled by PNP ACG and other PNP Units;
- b. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- c. Section 3, Rule 131, Revised Rules on Evidence (2019);

Disputable Presumption: xxx

- (f) *That money paid by one to another was due to the latter;*

xxx

- (j) *That a person found in possession of a thing taken in the doing of a recent wrongful act is the taker and the doer of the whole act; otherwise, that things which a person possesses, or exercises acts of ownership over, are owned by him or her;*

xxx

- d. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- e. If the amount does not exceed Php200,000.00, attached a barangay certificate to file action and minutes of the meeting. (2019 Rules on Mediation in the National Prosecution Service);
- f. Accomplished National Telecommunications Commission Complaint Form if the complainant intends to request for the take down of mobile numbers;
- g. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture);
- h. For Estafa cases, only those cases involving 4.4 million and up will be handled by the DOJ-Task Force on Cybercrime; and

- i. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian.

Section 3-6 “Robbery with Intimidation of Persons” (Art. 294, RPC)

3.16 Definition

- a. The personal property belongs to another;
- b. The unlawful taking of that property;
- c. With intent to gain (animus lucrandi);
- d. Violence against or intimidation of any person or force upon things;
- e. The offense can be committed by a band or with the use of firearms on a street, road or alley or by attacking a moving train, street car, motor vehicle or airship or by entering or taking the passenger conveyance by surprise; and
- f. Other analogous act.

(Committed by, through and with the use of information and communications technology.)

3.17 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant;
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of threatening post, online conversation, account used by the suspect in PRINT SCREEN and PDF form;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- g. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- h. Affidavit/Certificate of preservation of evidence (manner of preservation);
- i. Other related documents (police report, photographs, photocopy of money etc.);
- j. Coordinate with FG for the powder dusting of marked Money and request for UV immediately after the conduct of operation;

- k. Case Referral (inquest) or Case Investigation Report (regular filing); and
- l. NPS Investigation Data Form.

3.18 Notes

- a. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- b. If the post has been deleted, *compliance with the requirement stated under Sec. 2 Rule 11 in relation to Rule 5 on Rules of Electronic Evidence (A.M. No. 01-07-01-SC) (Authentication of electronic evidence)*;
- c. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- d. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and
- e. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

Section 3-7 “Access Device Regulation Act” (RA No. 8484)

3.19 Definition

Section 9. Prohibited Acts.

xxx

- (b) trafficking in one or more unauthorized access devices or access devices fraudulently applied for;

xxx

- (e) possessing one or more counterfeit access devices or access devices fraudulently applied for;

xxx

- (g) inducing, enticing, permitting or in any manner allowing another, for consideration or otherwise to produce, use, traffic in counterfeit access devices, unauthorized access devices or access devices;

xxx

- (k) having in one’s possession, without authority from the owner of the access device or the access device company, an access device, or any material, such as slips, carbon paper, or any other medium, on which the access

device is written, printed, embossed, or otherwise indicated;

xxx

- (n) effecting transaction, with one or more access devices issued to another person or persons, to receive payment or any other thing of value.

xxx

(Committed by, through and with the use of information and communications technology.)

3.20 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant;
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of online conversation, email or lick sent, text messages, call logs and account used by the suspect;
- e. Acknowledgement of payments in PRINT SCREEN and PDF form;
- f. For video recordings, store in optical disk or flash drives and follow proper chain of custody;

- g. Print Screen and/or Screen Shots of call logs, computer logs, network logs, emails, links;
- h. Proof of transactions;
- i. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- j. Authenticated copy of Statement of Account;
- k. Bank Dispute Reports;
- l. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- m. Other related documents (police report, photographs of access device, etc);
- n. Case Referral (inquest) or Case Investigation Report (regular filing); and
- o. NPS Investigation Data Form.

3.21 Notes

- a. For Phishing, Vishing, Smishing: File also a case violation of Sec. 4 (b-2) Computer Related Fraud, RA No. 10175;

- b. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- c. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- d. Section 14 of RA 8484. Presumption and prima facie evidence of intent to defraud. – The mere possession, control or custody of:
 - 1) *An access device, without permission of the owner or without any lawful authority;*
 - 2) A counterfeit access device;
 - 3) Access device fraudulently applied for;
 - 4) Any device-making or altering equipment by any person whose business or employment does not lawfully deal with the manufacture, issuance, or distribution of access device;
 - 5) An access device or medium on which an access device is written, not in the ordinary course of the possessor's trade or business; or

- 6) A genuine access device, not in the name of the possessor, or not in the ordinary course of the possessor's trade or business, shall be prima facie evidence that such device or equipment is intended to be used to defraud.
- e. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian.

Section 3-8 “Access Devices Regulation Act” as amended (RA 11449)

3.22 Definition

- a. Accessing, with or without authority, any application, online banking account, credit card account, ATM account, debit card account, in a fraudulent manner, regardless of whether or not it will result in monetary loss to the account holder; and
- b. Hacking refers to the unauthorized access into or interference in a computer system/server, or information and communication system, or any access in order to corrupt, alter, steal, or destroy using

a computer or other similar information and communication devices without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like resulting in the corruption, destruction, alteration, theft, or loss of electronic data messages or electronic documents.

(Committed by, through and with the use of information and communications technology.)

3.23 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of complainant;
- c. Affidavit of witness;
- d. Print Screen and/or Screen Shots of online conversation, account used by the suspect, acknowledgement of payments in PDF form;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Print Screen and/or Screen Shots of call logs, computer logs, network logs, emails, links;
- g. Proof of transactions;

- h. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- i. Authenticated copy of Statement of Account;
- j. Bank Dispute Reports;
- k. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- l. Other related documents (police report, photographs of access device, etc);
- m. Case Referral (inquest) or Case Investigation Report (regular filing); and
- n. NPS Investigation Data Form.

3.24 Notes

- a. For Phishing, Vishing, Smishing: File also a case violation of Sec. 4 (b-2) Computer Related Fraud, RA No. 10175;
- b. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- c. In the Affidavit of the Complainant and Witness, indicate the place of the

commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;

- d. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- e. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture);
- f. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and
- g. Section 14 of RA 8484. Presumption and prima facie evidence of intent to defraud. – The mere possession, control or custody of:
 - 1) *An access device, without permission of the owner or without any lawful authority;*
 - 2) A counterfeit access device;
 - 3) Access device fraudulently applied for;
 - 4) Any device-making or altering equipment by any person whose business or employment does not lawfully deal with the manufacture,

issuance, or distribution of access device;

- 5) An access device or medium on which an access device is written, not in the ordinary course of the possessor's trade or business; or
- 6) A genuine access device, not in the name of the possessor, or not in the ordinary course of the possessor's trade or business, shall be prima facie evidence that such device or equipment is intended to be used to defraud.

Section 3-9 "Anti-Photo and Video Voyeurism" (RA No. 9995)

3.25 Definition

- a. To take photo or video coverage of a person or group of persons performing sexual act or any similar activity or to capture an image of the private area of a person/s such as the naked or undergarment clad genitals, public area, buttocks or female breast without the consent of the person/s involved and under circumstances in which the person/s has/have a reasonable expectation of privacy;

- b. To copy or reproduce, or to cause to be copied or reproduced, such photo or video or recording of sexual act or any similar activity with or without consideration;
- c. To sell or distribute, or cause to be sold or distributed, such photo or video or recording of sexual act, whether it be the original copy or reproduction thereof; or
- d. To publish or broadcast, or cause to be published or broadcast, whether in print or broadcast media, or show or exhibit the photo or video coverage or recordings of such sexual act or any similar activity through VCD/DVD, internet, cellular phones and other similar means or device.

(Committed by, through and with the use of information and communications technology.)

3.26 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of the Complainant;
- c. Affidavit of Witnesses;
- d. Relevant conversation of the suspect and the victim in PRINT SCREEN and PDF form;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;

- f. Affidavit of Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- g. Copy of Explicit Videos and Photos of the victim;
- h. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- i. Case Referral (inquest) or Case Investigation Report (regular filing); and
- j. NPS Investigation Data Form.

3.27 Notes

- a. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- b. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- c. Proper collection, inventory, marking, and preservation of recovered/seized evidence;

- d. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian; and
- e. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

Section 3-10 “Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) And Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act” (RA No. 11930)

3.28 Definition. Online Sexual Abuse or Exploitation of Children (OSAEC) refers to the use of ICT as a means to abuse and/or exploit children sexually, which include cases in which offline child abuse and/or exploitation is combined with an online component. This can include, but is not limited to:

- a. The production, dissemination and possession of CSAEM;
- b. Online grooming of children for sexual purposes;
- c. Sexual extortion of children;

- d. Sharing image-based sexual abuse;
- e. Commercial sexual exploitation of children;
- f. Exploitation of children through online prostitution; and
- g. Live-streaming of sexual abuse.

With or without the consent of the victim: Provided, That OSAEC may be used interchangeably with online child sexual exploitation or abuse (OCSEA).

3.29 Unlawful or Prohibited Acts (Sec. 4) - Regardless of the consent of the child, it shall be unlawful for any person to commit the following acts through online or offline means or a combination of both:

- a. To hire, employ, use, persuade, induce, extort, engage, or coerce a child to perform or participate in whatever way in the creation or production of any form of OSAEC and CSAEM;
- b. To produce, direct, manufacturer, facilitate, or create any form of CSAEM, or participate in the production, direction, manufacture, facilitation or creation of the same;
- c. To offer, sell, distribute, advertise, promote, export, or import, by any means, any form of CSAEM;
- d. To knowingly publish, transmit and broadcast, by any means, any form of CSAEM;

- e. To permit or influence the child to engage, participate or assist in any form of CSAEM;
- f. To produce, direct, create, hire, employ or pay a facilitator to stream or livestream acts of child sexual abuse or exploitation;
- g. To stream or live-stream acts of, or any form of, child sexual abuse and exploitation;
- h. To recruit, transport, transfer, harbor, provide, or receive a child or to induce or influence the same, for the purpose of violating this act;
- i. To introduce or match a child to a foreign national or to any person for the purpose of committing any of the offences under this act;
- j. For film distributor, theaters and ICT services by themselves or in cooperation with other entities, to distribute any form of CSAEM or to facilitate the commission of any of the offences under this act;
- k. To knowingly benefit from, financial or otherwise, the commission of any of the offences of this act;
- l. To provide a venue for the commission of prohibited acts under this section such as dens, private rooms, cubicles, cinemas, houses, private homes, or other establishment;

- m. To engage in the luring or grooming of a child: Provided, that grooming taking place offline as a prelude to violating under this act shall also be penalized;
- n. To sexualize children by presenting them as objects of sexual fantasy, or making them conversational subjects of sexual fantasies, in any online or digital platform;
- o. To engage in pandering as defined under this act;
- p. To willfully subscribe, join, donate to, or support an internet site that host OSAEC or the streaming or live-streaming of child sexual abuse and exploitation;
- q. To advertise, publish, print, broadcast or distribute, or cause the advertisement, publication, printing, broadcasting or distribution by any means of any brochure, flyer, or any material that promotes OSAEC and child sexual abuse or exploitation;
- r. To possess any form of CSAEM: Provided, that possession of three (3) or more CSAEM is prima facie evidence of the intent to sell, distribute, publish or broadcast;
- s. To willfully access any form of CSAEM; and
- t. To conspire to commit any of the prohibited acts stated in this section.

3.30 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of the Complainant (Parents/Guardian)/Nominal Representative;
- c. Affidavit of Witnesses;
- d. Birth Certificate of the Minor;
- e. Relevant conversation of the suspect and the victim in PDF form;
- f. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- g. Copy of Explicit Videos and Photos of the Victim must be authenticated through an Affidavit of Authentication of Electronic Evidence which must be executed by either the party to the communication or person who had the direct knowledge about the videos or photos in compliance with *A.M. No. 01-07-01-SC*;
- h. Affidavit of DSWD if the parents/guardian are not willing to file the case;
- i. National Center for Mental Health (NCMH) as the Institution-in-Charge for the Psychological assessment/examination of victim;

- j. Preservation, application of cybercrime warrant, court warrant and compliance (if applicable);
- k. Case Referral (inquest) or Case Investigation Report (regular filing);
- l. NPS Investigation Data Form;
- m. Computers, tablets, mobile phones, and other devices seized pursuant to a WSSECD; and
- n. Affidavit of Investigator regarding the National Center for Missing and Exploited Children (NCMEC) CyberTipline Report (CTR), with attached DOJ endorsement, if applicable.

3.31 Notes

- a. ISPs are duty bound to report child pornography using it facility or server;
- b. ISPs are required to disclose data without a need for a WDCD;
- c. If the victim is outside the country, include the assessment from counterpart agencies;
- d. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;

- e. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- f. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian;
- g. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture); and
- h. **RA No. 11930** (Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act) expressly repealed RA No. 9775 and Section 4 (c) (2) of RA No. 10175.

Section 3-11 “Anti-Violence Against Women and Children” (RA No. 9262)

3.32 Definition

- a. Causing physical harm to the woman or her child;
- b. Threatening to cause the woman or her child physical harm;

- c. Attempting to cause the woman or her child physical harm;
- d. Placing the woman or her child in fear of imminent physical harm;
- e. Attempting to compel or compelling the woman or her child to engage in conduct which the woman or her child has the right to desist from or to desist from conduct which the woman or her child has the right to engage in, or attempting to restrict or restricting the woman's or her child's freedom of movement or conduct by force or threat of force, physical or other harm or threat of physical or other harm, or intimidation directed against the woman or her child;
- f. Threatening to deprive or actually depriving the woman or her child of custody or access to her/his family;
- g. Depriving or threatening to deprive the woman or her children of financial support legally due her or her family, or deliberately providing the woman's children insufficient financial support;
- h. Depriving or threatening to deprive the woman or her child of a legal right;
- i. Preventing the woman from engaging in any legitimate profession, occupation, business or activity, or controlling the victim's own

money or properties, or solely controlling the conjugal or common money, or properties;

- j. Inflicting or threatening to inflict physical harm on oneself for the purpose of controlling her actions or decisions;
- k. Causing or attempting to cause the woman or her child to engage in any sexual activity which does not constitute rape, by force or threat of force, physical harm, or through intimidation directed against the woman or her child or her/his immediate family;
- l. Engaging in purposeful, knowing, or reckless conduct, personally or through another that alarms or causes substantial emotional or psychological distress to the woman or her child such as stalking or following the woman or her child in public or private places; peering in the window or lingering outside the residence of the woman or her child; entering or remaining in the dwelling or on the property of the woman or her child against her/his will; destroying the property and personal belongings or inflicting harm to animals or pets of the woman or her child; engaging in any form of harassment or violence;
- m. Causing mental or emotional anguish, public ridicule or humiliation to the woman or her child, including, but not limited to, repeated verbal and emotional abuse, and denial of financial support or custody of minor children

or denial of access to the woman's child/children;

- n. Any acts in violation of confidentiality of records; and
- o. Other analogous acts.

(Committed by, through and with the use of information and communications technology.)

3.33 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of the Complainant;
- c. Affidavit of Witnesses;
- d. Birth Certificate of the Minor; Marriage Certificate (if applicable);
- e. Proof of intimate or past relationship;
- f. Relevant conversation of the suspect and the victim in PRINT SCREEN AND PDF form;
- g. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- h. Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;

- i. Preservation, application of cybercrime warrant, court warrant and compliance (if applicable);
- j. Other related documents (police report, photographs, etc);
- k. Case Referral (inquest) or Case Investigation Report (regular filing); and
- l. NPS Investigation Data Form.

3.34 Notes

- a. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;
- b. Proper collection, inventory, marking, and preservation of recovered/seized evidence; and
- c. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian.

Section 3-12 “Special Protection against Child Abuse, Exploitation and Discrimination, and for Other Purposes” (RA No. 7610)

3.35 Definition

- a. **Child Prostitution and Other Sexual Abuse.** Children, whether male or female, who for money, profit, or any other consideration or due to the coercion or influence of any adult, syndicate or group, indulge in sexual intercourse or lascivious conduct, are deemed to be children exploited in prostitution and other sexual abuse.

- b. **Attempt to Commit Child Prostitution.** There is an attempt to commit child prostitution under Section 5, paragraph (a) hereof when any person who, not being a relative of a child, is found alone with the said child inside the room or cubicle of a house, an inn, hotel, motel, pension house, apartelle or other similar establishments, vessel, vehicle or any other hidden or secluded area under circumstances which would lead a reasonable person to believe that the child is about to be exploited in prostitution and other sexual abuse.

- xxx

- e. **Obscene Publications and Indecent Shows.** Any person who shall hire, employ, use, persuade, induce or coerce a child to

perform in obscene exhibitions and indecent shows, whether live or in video, or model in obscene publications or pornographic materials or to sell or distribute the said materials.

- f. **Other Acts of Neglect, Abuse, Cruelty or Exploitation and Other Conditions Prejudicial to the Child's Development.** Any person who shall commit any other acts of child abuse, cruelty or exploitation or to be responsible for other conditions prejudicial to the child's development including those covered by Article 59 of Presidential Decree No. 603, as amended, but not covered by the Revised Penal Code, as amended.

(Committed by, through and with the use of information and communications technology.)

3.36 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of the Complainant;
- c. Affidavit of Witnesses;
- d. Birth Certificate of the Minor;
- e. Relevant conversation of the suspect and the victim in PDF form;
- f. Authentication of Electronic Evidence must be executed by either the party to the

communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;

- g. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- h. Psychological Assessment/ Examination of the victim from DSWD/ NCMH (if available);
- i. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);
- j. Other related documents (police report, photographs, etc);
- k. Case Referral (inquest) or Case Investigation Report (regular filing); and
- l. NPS Investigation Data Form.

3.37 Notes

- a. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time);
- b. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor;

- c. Proper collection, inventory, marking, and preservation of recovered/seized evidence; and
- d. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest, conduct of entrapment operation and implementation of WSSECD. Ensure submission of Affidavit of Recording Officer and Affidavit of Data Custodian.

Section 3-13 “Safe Spaces Act” (RA No. 11313)

3.38 Definition. Use of information and communications technology in terrorizing and intimidating victims:

- a. through physical, psychological, and emotional threats;
- b. unwanted sexual misogynistic, transphobic, homophobic and sexist remarks and comments online whether publicly or through direct and private messages;
- c. invasion of victim’s privacy through cyberstalking and incessant messaging;
- d. uploading and sharing without the consent of the victim, any form of media that contains photos, voice or video with sexual content;

- e. any unauthorized recording and sharing of any of the victim's photos, videos, or any information online;
- f. impersonating identities of victims online;
- g. posting lies about victims to harm their reputation; and
- h. filing false abuse reports to online platforms to silence victims.

3.39 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of the Complainant;
- c. Affidavit of Witnesses;
- d. Relevant conversation of the suspect and the victim in PDF form;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Screen shots/extraction of the Post in PRINT SCREEN and PDF form;
- g. Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;

- h. Preservation, application of cybercrime warrant, court warrant and compliance (if applicable);
- i. Other related documents (police report, photographs, etc);
- j. Case Referral (inquest) or Case Investigation Report (regular filing); and
- k. NPS Investigation Data Form.

3.40 Notes

- a. In investigating GBOSH, refer to the procedures established under the DOJ Guideline in Gathering Evidence and Case Build-up: Gender-Based Online Sexual Harassment;
- b. Attribute the device with the suspect (description of the device, physical location, IP addresses, domain names, other potential identifiers of digital devices, exact time); and
- c. In the Affidavit of the Complainant and Witness, indicate the place of the commission of the offense to ensure that the elements of the offense are within the territorial jurisdiction of the Prosecutor.

**Section 3-14 “Migrant Workers and Overseas
Filipino Act of 1995, amended xx” (RA No. 8042 as
amended by RA 10022)**

3.41 Definition. Committed by, through and with the use of information and communications technology.

xxx

- p. That the victim was recruited by a person who has no license or authority to recruit workers;
- q. Suspect through false pretenses and fraudulent representations created an impression that he/she can facilitate or has the capacity to deploy the victim abroad for employment;
- r. Recruitment is defined as any act of canvassing, enlisting, contracting, transporting, utilizing, hiring or procuring workers, and includes referrals, contract services, promising or advertising for employment, locally or abroad, whether for profit or not: Provided, that any person or entity which, in any manner, offers or promises for a fee, employment to two or more persons shall be deemed engaged in recruitment and placement;
- s. It shall likewise include the following acts, whether committed by any person, whether

a non-licensee, non-holder, licensee or holder of authority:

- 1) To charge or accept directly or indirectly any amount greater than that specified in the schedule of allowable fees prescribed by the Secretary of Labor and Employment, or to make a worker pay or acknowledge any amount greater than that actually received by him as a loan or advance;
- 2) To furnish or publish any false notice or information or document in relation to recruitment or employment;
- 3) To give any false notice, testimony, information or document or commit any act of misrepresentation for the purpose of securing a license or authority under the Labor Code, or for the purpose of documenting hired workers with the POEA, which include the act of reprocessing workers through a job order that pertains to nonexistent work, work different from the actual overseas work, or work with a different employer whether registered or not with the POEA;
- 4) To include or attempt to induce a worker already employed to quit his employment in order to offer him another unless the transfer is

designed to liberate a worker from oppressive terms and conditions of employment;

- 5) To influence or attempt to influence any person or entity not to employ any worker who has not applied for employment through his agency or who has formed, joined or supported, or has contacted or is supported by any union or workers' organization;
- 6) To engage in the recruitment or placement of workers in jobs harmful to public health or morality or to the dignity of the Republic of the Philippines;
- 7) To fail to submit reports on the status of employment, placement vacancies, remittance of foreign exchange earnings, separation from jobs, departures and such other matters or information as may be required by the Secretary of Labor and Employment;
- 8) To substitute or alter to the prejudice of the worker, employment contracts approved and verified by the Department of Labor and Employment from the time of actual signing thereof by the parties up to and including the period of the expiration of the same without the

approval of the Department of Labor and Employment;

- 9) For an officer or agent of a recruitment or placement agency to become an officer or member of the Board of any corporation engaged in travel agency or to be engaged directly or indirectly in the management of travel agency;
- 10) To withhold or deny travel documents from applicant workers before departure for monetary or financial considerations, or for any other reasons, other than those authorized under the Labor Code and its implementing rules and regulations;
- 11) Failure to actually deploy a contracted worker without valid reason as determined by the Department of Labor and Employment; and
- 12) Failure to reimburse expenses incurred by the worker in connection with his documentation and processing for purposes of deployment, in cases where the deployment does not actually take place without the worker's fault. Illegal recruitment when committed by a syndicate or in large scale shall be considered an offense involving economic sabotage.

3.42 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of the Complainant;
- c. Affidavit of Witnesses;
- d. Relevant conversation of the suspect and the victim in PRINT SCREEN AND PDF form;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Screenshot of proof of payment;
- g. Screenshot of acknowledgement of payment;
- h. Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- i. Certification from POEA/Department of Migrant Workers that the recruiter has no authority to recruit;
- j. Other related documents (police report, photographs, etc.);
- k. Preservation, application for cybercrime warrant, court warrant and compliance (if applicable);

- l. Case Referral (inquest) or Case Investigation Report (regular filing); and
- m. NPS Investigation Data Form.

3.43 Notes

- a. As to the venue of the filing of the case, under the law, the victim/complainant has the option to file the case either in his/her residence or to the place where the crime was committed;
- b. The complainant or his/her witness will execute the Affidavit of Authentication of Electronic Evidence if the post has already been deleted when the case was reported to ACG;
- c. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- d. Illegal Recruitment case may be filed together with Article 315 (ESTAFSA) of the Revised Penal Code, as amended;
- e. Illegal recruitment is deemed committed by a syndicate if carried out by a group of three (3) or more persons conspiring or confederating with one another. It is deemed committed in large scale if committed against three (3) or more persons individually or as a group;

- f. Use of Body-worn camera or Alternative Recording Device in implementing warrant of arrest and search warrant; Affidavit of Recording Officer; Affidavit of Data Custodian; and
- g. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

Section 3-15 “Intellectual Property Code of the Philippines” (RA No. 8293)

3.44 Definition. *Committed by, through and with the use of information and communications technology.*

a. Infringement of Trademarks

a) Section 155.1 Use in commerce:

- a) Any reproduction, counterfeit, copy or colorable imitation of a registered mark or the same container or a dominant feature thereof;
- b) In connection with the sale, offering for sale, distribution, advertising of any goods or services, including preparatory steps necessary

to carry out the sale of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or

- c) Without the consent of the owner of the registered mark.

b) Section 155.2 Reproduce, counterfeit, copy or colorably imitate a registered mark or a dominant feature thereof:

- a) Apply the same to labels, signs, prints, packages, wrappers, receptacles, or advertisement;
- b) Labels, signs, prints, packages are intended to be used for;
- c) In commerce upon or;
- d) In connection with the sale, offering for sale, distribution, or advertising of goods or services on or;
- e) In connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or
- f) Without the consent of the owner of the registered mark.

c) Section 168.2 Any person (Natural or Juridical):

- a) Who manufactures, or deals in certain goods, or engages in business, or offers services;
- b) Employs deception or any other means contrary to good faith, or commits any acts, calculated to result in; or
- c) Passing off the goods manufactures by him or in which he deals, or his business, or services for those of the one having established such good will, or who shall produce said result.

d) Section 168.3 (a) Any person, natural or juridical:

- a) Who sells his goods and gives them the general appearance of goods of another manufacturer or dealer, either as to the goods themselves or in the wrapping of the packages in which they are contained, or the devices or works thereon, or in any other feature of their appearance;

- b) Which would be likely to influence purchasers to believe that the goods offered are those of a manufacturer or dealer other than the actual manufacturer or dealer; or
 - c) Otherwise clothes the goods with such appearance as shall deceive the public and defraud another of his legitimate trade or any subsequent vendor of such goods or any agent of any vendor engaged in selling such goods with a like purpose.
- e) **Section 168.3 (b) and (c)** Any person, natural or juridical, who:
- a) Employs any artifice, or device, or any other means calculated to induce the false belief that such person is offering the services of another;
 - b) Who has identified such services in the mind of the public;
 - c) Make any false statement in the course of trade;

- d) Who shall commit any other act contrary to good faith of a nature; or
- e) Calculated to discredit the goods, business or services of another.

b. **False Designation of Origin; False Description or Representation**

a) **Section 169.1 (a)** A person, natural or juridical:

- a) Who uses in commerce;
- b) Any word, term, name, symbol or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact;
- c) On or in connection with any goods or services, or any container for goods; or
- d) Which is likely to cause confusion, or mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of

his or her goods, services, or commercial activities by another person.

b) Section 169.1 (b) A person, natural or juridical:

- a) Who uses in commerce;
- b) Any word, term, name, symbol or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact;
- c) On or in connection with any goods or services, or any container for goods; or
- d) In commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographical origin of his or her or another person' goods, services or commercial activities.

c. Copyright

- a) Section 177** Copyright or economic rights shall consist of the exclusive right to carry out, authorize or prevent the following:

- a) Acts of reproduction of the work or substantial portion of the work (177.1);
- b) Dramatization, translation, adaptation, abridgment, arrangement or other transformation of the work (177.2);
- c) First public distribution of the original and each copy of the work by sale or other forms of transfer of ownership (177.3);
- d) Rental of the original or a copy of an audiovisual or cinematographic work, a work embodied in a sound recording, a computer program, a compilation of data and other materials or a musical work in graphic form, irrespective of the ownership of the original or the copy which is the subject of the rental (177.4);
- e) Public display of the original or a copy of the work (177.5);
- f) Public performance of the work (177.6); or
- g) Other communication to the public of the work (177.7).

- b) Section 217.1. Infringement** Any person, natural or juridical:
- a) Infringing any of the right secured provisions of Part IV of this Act, or
 - b) Aiding or abetting such infringement.
- c) Section 217.3. Possession** Any person, natural or juridical, who has in his possession an article:
- a) Which he knows, or ought to know, to be an infringing copy of the work;
 - b) For the purpose of selling, letting for hire, or by way of trade, offering or exposing for sale, or hire, the article;
 - c) Distributing the article for purpose of trade, or for any other purpose to an extent that will prejudice the rights of the copyright owner in the work; or
 - d) Trade exhibit of the article in public at the time when copyright subsists in the work.

3.45 Pieces of Evidence

- a. Incident Record Form;
- b. Affidavit of Complainant;
- c. Affidavit of Witness;
- d. Print Screen and/or Screen Shots of text messages from the alleged fraudster/scammer, email/s and phishing link in PRINT SCREEN and PDF form;
- e. For video recordings, store in optical disk or flash drives and follow proper chain of custody;
- f. Authentication of Electronic Evidence must be executed by either the party to the communication or person who had the direct knowledge about the online communication in compliance with *A.M. No. 01-07-01-SC*;
- g. SEC, DTI or LGU permits;
- h. Proper collection, inventory, marking, and preservation of recovered/seized evidence;
- i. Photograph the counterfeit products confiscated during the seizure operation;
- j. IPO Certificate's regarding as follows:
 - 1) Trademark;
 - 2) Patent;

- 3) Industrial Design; and
- 4) Copyright.
- k. Official/delivery receipts during test-buy operations (if any);
- l. Sample of the genuine product and the counterfeit product;
- m. Board resolution for the company representative;
- n. Certifications issued by the product expert/laboratory technicians/certified technical expert attesting to the fact that the item seized is fake;
- o. Preservation, application of cybercrime warrant, court warrant and compliance (if applicable);
- p. Case Referral (inquest) or Case Investigation Report (regular filing); and
- q. NPS Investigation Data Form.

3.46 Notes

- a. In IPR prosecution, the item or product claimed to have been the subject of forgery should be presented;
- b. Coordinate with IPO as to product certification (e.g. Business Software Alliance certification);

- c. For counterfeit drugs, coordinate with FDA for the conduct of laboratory test, License to Operate status, and product verification;
- d. The complainant or his/her witness will execute the Affidavit of Authentication of Electronic Evidence if the post has already been deleted when the case was reported to ACG; and
- e. Evaluate for possible Money Laundering investigation (conduct asset tracing and recommend for freeze order, civil and criminal forfeiture).

Section 3-16 “Obstruction of Justice” (PD No. 1829) in relation to RA 10175 and Sec. 27 of A.M. 17-11-03 (Rule on Cybercrime Warrant)

3.47 Definition. Section 1. Any person who knowingly or willfully obstructs, impedes, frustrates or delays the apprehension of suspects and the investigation and prosecution of criminal cases by committing any of the following acts:

xxx

- e. Delaying the prosecution of criminal cases by obstructing the service of process or court orders or disturbing proceedings in the fiscal's offices, in Tanodbayan, or in the courts;

3.48 Pieces of Evidence

- a. Incident Record Form;
- b. Complaint-Affidavit of the Investigator-on Case/Applicant of the WDCD;
- c. Copy of the Court Order approving the Warrant to Disclose Computer Data;
- d. Copy of Production/Compliance order received by the authorized representative of the service provider; and
- e. Copy of the Final Return filed in court stating the failure of the service provider to reply/comply within the allowable period.

3.49 Notes

- a. Section 20 of RA No. 10175 states that:

“Noncompliance - Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 with imprisonment of prision correccional in its maximum period or a fine of One Hundred Thousand Pesos (Php100,000.00) or both, for each and every noncompliance with an order issued by law enforcement authorities.”
- b. Section 2.7, Rule on Cybercrime Warrants provides that:

“Obstruction of Justice for Non-Compliance; Where to File- Pursuant to Section 20, Chapter IV of RA 10175, failure to comply with the provisions of Chapter IV, specifically the orders from law enforcement authorities, shall be punished as a violation of Presidential Decree No. 1829, entitled “Penalizing Obstruction of Apprehension and Prosecution of Criminal Offenders.”

The criminal charge for obstruction of justice shall be filed before the designated cybercrime court that has jurisdiction over the place where the non-compliance was committed.”

- c. The case must be filed by the Investigator-on-Case/applicant of the cybercrime warrant to the Prosecutor’s Office having jurisdiction over the place where the ORDER was serve

APPENDIX

Section 2.10 Cybercrime and Cyber-Related Incident Response Operations (2021 Revised PNP Operational Procedures, Page 73)

- a. Cybercrime Response. Cybercrime Response is the actual police intervention in a cybercrime or cyber-related incident where the acquisition of matters of evidentiary value is traceable within the computer's hardware, software and its network.
- b. Guidelines in Responding to Cybercrime and Cyber-Related Incidents
 - 1. When responding to a cybercrime incident, or to a crime scene where Information and Communication Technology (ICT) equipment (e.g. computers, digital storage devices, and other electronic devices or equipment) are present, it is imperative for the First Responder (FR) to protect and preserve the crime scene and seek the assistance of the station IOC to identify potential evidence such as the following:
 - a. Contraband or fruits of a crime;
 - b. Tools used for the commission of the crime; and/or
 - c. Other items that may be used in the commission of the crime

2. The FR shall immediately coordinate with the nearest ACG office, through the station TOC or the IOC, for assistance. Upon arrival of the ACG personnel, they shall immediately conduct the “bag and tag” procedure on the digital evidence and turn over to the IOC.
3. The concerned investigating unit shall secure and submit a court order and necessary legal requirements for the ACG to conduct digital forensic examination that is in accordance with the rule on cybercrime warrants. The evidence seized shall then be subjected to digital forensic examination by the PNP ACG. The result of the forensic examination, as well as the testimony of the forensic expert, shall be made available during the trial.

c. Preservation of Seized Computer

Upon determination of how the computer was utilized in the commission of the crime, and once the legal requirements have been complied with, the following are the guidelines in the preservation of the seized computer:

1. Secure the Scene:
 - a.) Officer's safety is always paramount.
 - b.) Preserve the area for potential fingerprints.
 - c.) Immediately restrict access to the computer.

- d.) Disable the internet connection to restrict remote access to the computer.

2. Secure the computer as evidence.

- a) If the computer is "OFF", do not turn it "ON".
- b) If the computer is "ON", do not turn it "OFF", nor touch its mouse or its keyboard.

3. For stand-alone connection or single area connection computers (not-networked).

- a) Consult a Digital Forensic Examiner.
- b) If a Digital Forensic Examiner is not available, the station IOC shall perform the following:
 - i. Photograph screen and disconnect all power sources and plugs including those at the back of the computer;
 - ii. Cover or put a tape over each drive slot;
 - iii. Photograph (or make a diagram) and label parts located at the back of the computer including its connections;
 - iv. Label all connectors and cable end to allow reassembly as needed (Example:

“Socket” marked “A” and the “cable End” also marked “A”);

- v. If transport is required, pack the components as “fragile cargo” prior to transport;
 - vi. Keep it away from magnets, radio transmitters, and from other hostile environment; and
 - vii. Ensure that only the Digital Forensic Examiner conducts the search for any evidence contained in the computer hardware.
4. For Networked Computers (or business computers)
- i. Consult a Digital Forensic Examiner for assistance.
 - ii. Do not immediately pull the plug to prevent the following:
 - 1. Severe damage to the system;
 - 2. Disrupting the legitimate business; and
 - 3. Possible liability of the police officers.
5. For Ransomware or Malware Attack on a Computer
- i. Consult a computer specialist for assistance;

- ii. Immediately disconnect the computer from the network to avoid the spread of malware to other computers on the same network; and
 - iii. Do not immediately pull the plug and wait for the computer specialist to arrive.
- d. Guidelines in the Treatment of Other Electronic Data Storage Devices

The IOC should understand that other electronic devices may contain viable evidence associated with the crime. The IOC must ensure that the device should not be accessed unless a warrant has been issued.

- e. Preservation of Seized Mobile Communication Devices

Upon determination of how the mobile communication device was utilized in the commission of the crime the following are the guidelines to be followed:

1. If the device is turned "ON", do not turn it "OFF" as it could activate lockout feature
 - a.) Take a photograph of the screen display and write down all information therein;
 - b.) If possible, turn on airplane/flight mode or use a signal blocking container, if available, and record the steps undertaken;

- c.) If the device is locked, do not attempt to unlock it; and
 - d.) Bring the power supply cord of the seized device found at the scene.
2. If the device is TURNED "OFF", leave it "OFF" AS IT could alter evidence in the device.
- f. Preservation of Seized Facsimile or Fax Machine or Similar Devices

If the fax machine is "ON", do not turn it "OFF" as it may cause the loss of the last number dialed or other stored fax numbers. If possible, all manuals should be seized along with the machine. Photographs of the machine and its display shall be taken.

- g. Preservation of Seized Caller ID Devices and Other Similar Devices
- 1. The IOC should be able to recognize potential evidence contained in caller ID devices such as telephone numbers and subscriber's information from incoming phone calls.
 - 2. The IOC should remember that interruption of the power supply of the caller ID device may cause loss of data if not protected by an internal battery back-up.
- h. Guidelines in the Treatment of Seized Digital Video Recording (DVR) Devices
- 1. The IOC should be able to recognize potential evidence contained in DVR devices such as the date and time of occurrence and the

persons viewed on the video captured by the Audio and Video Recorder (AVR) and camera devices; and

2. The IOC should secure a warrant for the conduct of forensic examination/enhancement of audio video recorded by the DVR device.
- i. Acquiring the DVR Devices and/or their Footages/Recording
 - a. The IOC shall send a Preservation Letter (Annex "Y") addressed to the DVR device owner directing him/her to keep, retain and preserve the footages/recordings; and
 - b. A court order or a notarized affidavit of consent together with the photocopy of valid ID from the DVR device owner or authorized administrator must be secured to obtain the original and/or duplicate copies of footages/recordings.

ANNEXES

“A”	Format for Case Investigation Report	118
“B”	Affidavit of Examination by Digital Forensic Examiner	120
“C”	Affidavit of Preservation by Investigator-on-Case (IOC) /Cyber Patroller	124
“D”	Affidavit of Authentication of Electronic Evidence by Complainant	127
“E”	Affidavit of Disinterested Party	129
“F”	Affidavit of IOC re: Non-appearance of complainant	131
“G”	Affidavit of Recording Officer	134
“H”	Affidavit of Data Custodian	137
“I”	Affidavit of Seizing Officer	140
“J”	Certificate of Extraction by IOC/ Cyber Patroller	142
“K”	Preservation Request (Banks, Telephone Company, Internet Service Providers, Social Media Platforms, Money Service Business, Other Private Entities)	144
“L”	Sample Request for Digital Forensic Examination	146
“M”	Sample Application for WDCD	148
“N”	Sample Application for WECD	160
“O”	Sample Application for WSSECD	170
“P”	Production/Compliance Order for Service Providers	187
“Q”	Initial Return of Cybercrime Warrant	189
“R”	Final Return of Cybercrime Warrant	193

Annex “A”



Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City



To: Hon. Investigating Prosecutor
Quezon City, Metro Manila.

Subject: Case Investigation Report (Alleged Estafa under
Article 315 of the Revised Penal Code, as amended in
relation to sec. 6 of R.A. 10175

Date:

CASE INVESTIGATION REPORT

I

BRIEF BACKGROUND OF THE CASE

- a) *NAME OF THE VICTIM;*
- b) *NAME OF THE SUSPECT;*
- c) *DTPO;*
- d) *MODUS OPERANDI; and*
- e) *SCREEN SHOTS OF ONLINE CONVERSATION IN PDF FORM*

II

LAWS VIOLATED

III

.ACTION TAKEN/ RESULT

- a) *Application for WDCD- CITE the complete details of WDCD;*
- b) *Compliance of WDCD;*

- c) Preservation Order; and*
- d) Verification as to the existence of the person disclosed under the WDCD.*

IV
RECOMMENDATION

INVESTIGATOR ON CASE
CEL. NO. OR EMAIL.

Annexes-

- A. IRF;
- B. SWORN STATEMENT;
- C. SCREEN SHOTS OF ONLINE CONVERSATION;
- D. PRESERVATION ORDER; and
- E. APPLICATION OF WDCD.

Annex “B”

Republic of the Philippines)
Quezon City) S.S.
X-----X

AFFIDAVIT OF DIGITAL FORENSIC EXAMINER

I, (Rank and Name of Digital Forensic Examiner), Filipino, of legal age, member of the Philippine National Police, presently assigned at Digital Forensic Unit, PNP Anti-Cybercrime Group, Camp Crame, Quezon City, do hereby depose and state that:

1. On March 15, 2023, this Unit received a memorandum from _____, Officer-in-Charge, Cyber Response Unit, Anti-Cybercrime Group (CRU, ACG), Camp BGen Rafael T Crame, Quezon City, requesting for Digital Forensic Examination dated _____ in relation to the investigation for Violation of Section 4 (b) (c) (d) of Republic Act 9995 “Anti-Photo and Video Voyeurism Act of 2009” in relation to Section 6 of Republic Act 10175, otherwise known as “Cybercrime Prevention Act of 2012”. The said request is supported by a Warrant to Search, Seize, and Examine Computer Data (WSSECD) No _____ issued by Hon. _____, Presiding Judge, Branch __, Regional Trial Court, _____ dated _____.
2. On the same day, (Rank and Name of IOC), Investigator-on-Case (IOC), submitted the following pieces of digital evidence:

Evidence Number	Quantity	Full Description
001	1	Vivo 20s (g) (Blue) with tag ("Cellphone #1, WSSECD NO. _____, VIOLATION OF SEC. 4 OF RA 9995 in rel to sec 6 of RA 10175, March 9, 2023") tagged as "Evidence 001".
002	1	DITO TELECOMMUNITY SIM Card with Reference _____ tagged as "Evidence 002" (Note: Pulled out from SIM Slot1 of Evidence 001)
003	1	Smart 5G SIM Card with Reference _____ tagged as "Evidence 003" (Note: Pulled out from SIM Slot2 of Evidence 001)

3. On _____, I started my examination on the submitted pieces of evidence and completed my examination on _____.
4. I examined the submitted pieces of evidence using Cellebrite UFED Camera version 7.40.0.85 and Cellebrite UFED TOUCH version 7.45.1.43.

5. The names and positions of the law enforcement authorities who may be allowed to access the deposited data:
 - d. (Rank and Name of Digital Forensic Examiner), Filipino, of legal age, member of the Philippine National Police, presently assigned at PNP Anti-Cybercrime Group, Camp BGen Rafael T Crame, Quezon City.
 - e. (Rank and Name of IOC), Investigator-on-Case, Filipino, of legal age, member of the Philippine National Police, presently assigned at PNP Anti-Cybercrime Group, Camp BGen Rafael T Crame, Quezon City.
 - f. Attached is the hard copy of my Digital Forensic Report together with a storage media (USB Flashdrive), tagged as "Evidence Number 004," containing extracted data and reports from the submitted evidence.
6. I certify that the submitted pieces of evidence, digital forensic report, and storage media (USB Flashdrive) are included in the sealed package.

IN WITNESS WHEREOF, I have here unto affixed my signature this ____ day of _____ at Camp BGen Rafael T Crame, Quezon City, Philippines.

Rank and Name of Digital Forensic Examiner
Affiant

RESTRICTED

PNP ID No: _____
Valid Until: _____

SUBSCRIBED and SWORN to before me this _____ at Camp BGen Rafael T Crame, Quezon City, Philippines. I HEREBY CERTIFY that I have personally examined the affiants and I am fully convinced that they voluntarily and freely executed this affidavit and understood the same.

Administering Officer

Annex “C”

Republic of the Philippines)
_____) S.S.
X -----X

AFFIDAVIT OF PRESERVATION

I, _____, of legal age, single, an Investigation PNCO presently assigned at Philippine National Police, Anti-Cybercrime Group (PNP-ACG), _____, after having been duly sworn to in accordance with law, hereby depose and state, that:

1. I am a recipient of a Cybercop Badge, a competency badge issued by the Philippine National Police after I completed four (4) mandatory courses conducted by the PNP-ACG to wit: Introduction to Cybercrime Investigation Course (ICIC); Identification and Seizure of Digital Evidence (ISDE); Proactive Internet Investigation Course (PIIC) and Introduction to Digital Forensic Investigation (IDFI);

2. From these courses, I learned how to capture and preserve social media content in a sound manner through the use of available application tools;

3. I am the Officer who preserved computer data to support the complaint of _____, legal age, female, a resident of _____ against _____, legal age, a resident of _____ for Violation of _____ in relation to RA 10175 (Cybercrime Prevention Act of 2012);

4. On _____, complainant _____ signed the “Consent to Access Social Networking Site Account” and gave me authority to open her Facebook Account _____ with URL/FB ID _____ and to examine, capture, preserve, save and print the conversation that she had with Facebook account name _____ with URL/FB ID _____;

5. I viewed, examined, captured and preserved the Facebook accounts of _____ and _____ using ***Snipping Tool***, a screenshot utility that can take screen shots of an open window, rectangular areas, a free-form area, or the entire screen. Snips can then be annotated using a mouse or a tablet, stored as an image file (PNG, GIF, or JPEG file) or an MHTML file, or e-mailed and PDF File Format. I also viewed, examined, captured and preserved the conversation of the complainant with Facebook Account _____ in PDF File Format;

6. I saved the preserved snips of the two Facebook accounts and the conversation under file name/s _____ and obtained the hash value of each of them with the following information:

- a. Screenshot 1:
- b. Screenshot 2:
- c. Saved PDF file of conversation:

7. I stored the preserved conversation in a DVD-R under file name _____, marked as Annex “_____”. I also made printed copies of the said screen shots and preserved conversation consisting of ____ pages, and attached as Annex “_____”; and

8. The Facebook screen shots and messenger conversation that I preserved form part of the evidence in this case.

IN WITNESS WHEREOF, I have hereunto set my hand and affix my signature this _____ day of _____ 2023 at _____, Philippines.

Affiant

SUBSCRIBED AND SWORN TO before me this _____ of _____ at _____, after affiant showed me her _____ ID with Card Number _____. I hereby certify that I personally examined the herein affiant and am convinced and satisfied that she executed this affidavit voluntarily, freely and fully understood the contents hereof.

Administering Officer

Annex “D”

Republic of the Philippines)
Quezon City) S.S.
X-----X

**AFFIDAVIT OF AUTHENTICATION OF ELECTRONIC
EVIDENCE**

I, _____, _____ years old, _____,
Filipino and a resident of _____, under oath,
hereby depose and state the following that:

1. I am executing this AFFIDAVIT in support to the case against _____ for violation of _____ in relation to Sec. 6 of RA 10175 also known as Cybercrime Prevention Act of 2012.
2. I have caused the faithful reproduction of my conversation with _____ which was downloaded and recorded to _____. The same was transferred to CD-ROM marked as Annex __ with markings, date and signature.
3. The said conversation transpired on _____ at around _____ in relation to _____.
4. The said recordings and print outs are not altered and still stored in my laptop (or mobile device) described as _____.
5. I am executing this AFFIDAVIT not for the purpose of fraud nor perpetuate injustice; and

6. That I executed this AFFIDAVIT in compliance with the rule of admissibility of electronic evidence.

AFFIANT FURTHER SAYETH NAUGHT.

Affiant

SUBSCRIBED AND SWORN TO BEFORE ME, this _____ day of _____ in the City of _____, affiant personally known to me as the same person who signed the foregoing AFFIDAVIT as his free own act and deed.

Doc No. : _____

Page No.: _____

Book No.: _____

Series of 2023

Annex “E”

Republic of the Philippines)
Quezon City) S.S.
X-----X

AFFIDAVIT OF DISINTERESTED PARTY

I _____, (Status) _____, _____ years old
_____ (citizenship) _____ (gender) with occupation of
_____ and _____ presently residing at
_____ do hereby depose and state that:

- 1 On _____ (date) at _____ (time), I personally appeared at the Philippine National Police Anti-Cybercrime Group (PNP ACG) to report the following incident which transpired on _____ (date) in violation of _____ with the following information as follows:

- 2 The aforementioned incident is reported to PNP ACG for blotter purposes only as I am no longer interested to pursue the case against the suspect _____ (name/account number if any) based on the following:

- ☐ Only interested to deactivate the fake/dummy account or similar social Media account
- ☐ Only interested to delete the pornographic picture and/or videos in Website
- ☐ No available time to attend hearings

RESTRICTED

- ☐ No available fund to attend hearings or travel to and from concerned government agencies
- ☐ Affiant or victim is an OFW or about to travel abroad
- ☐ Other reasons:
- _____

- 3 I am executing this Affidavit to attest to the truthfulness of the foregoing facts and circumstances in relation to the above-mentioned incident/s.

FURTHER SAYETH NAUGHT

IN WITNESS WHEREOF, I have hereunto affixed my signature signed this ___ day of _____ 2023', at Camp BGen Rafael T Crame, Quezon City, Philippines.

Affiant

Valid ID: _____
ID No. : _____

SUBSCRIBED AND SWORN to before me this ___ day of ___ 2023 by the affiant who exhibited his / her valid ID indicated above.

Administering Officer

Annex “F”

Republic of the Philippines)
Quezon City) S.S.
X-----X

**AFFIDAVIT OF INVESTIGATOR-ON-CASE
(Non-Appearance of Complainant)**

I, _____, _____ (Status)
_____ years old _____ (citizenship) bona fide member of
Philippine National Police and presently assigned at
_____ do hereby depose and state that:

1. I am the investigator-on-case in the alleged Identity Theft wherein the complainant is certain _____, (Status) _____ years old _____ (citizenship) native of _____ and a resident of _____;
2. On _____ at around _____ PM, above named complainant personally appeared at Regional Anti-Cybercrime Unit 4B, and narrated the following incidents as follow:
 - a. Nature of the incident: Viol; of Sec. 4 of R.A 10175 (_____);
 - b. Name of Suspect: _____;
 - c. Time and Date: _____;
 - d. Place of occurrence: _____;
 - e. Name of witness/es if any: _____;
 - f. Pieces of evidence presented: _____; and
 - g. Brief narration of the facts (Why and How).

3. In response to that complaint, the undersigned affiant took the following actions: (EXAMPLES)
 - a. Made the complainant to fill-up the IRF;
 - b. Put his/her complaint in the PB with entry No. _____ dated _____;
 - c. Prepared the preservation order;
 - d. Advice the complainant to bring _____ or produce _____; and
 - e. Etc.
4. The Disposition of the Case: (ei. Under investigation/For follow-up operation/For entrapment operation);
5. Herein affiant has exerted efforts to contact and coordinate with the complaint by:
 - i. Visiting the given address at _____ on _____ but the complaint was not present; and
 - ii. Calling the given mobile number _____ on _____ or three consecutive times, however _____ (indicate if you were able to talk/refusal/not answering)
 - a. From the foregoing, the complainant _____(name) showed his/her lack of interest to pursue and prosecute the case.

- b. I am executing this Affidavit to attest to the truthfulness of the foregoing fact and circumstances in relation to the above-mentioned incidents/s.

FURTHER SAYETH NAUGHT

IN WITNESS WHEREOF, I have hereunto affixed my signature signed this ____ day of _____ 2023, at Camp BGen Rafael T Crame, Quezon City, Philippines.

Affiant

Valid ID: _____

ID No. _____

SUBSCRIBED AND SWORN to before me this day of 2023 by the affiant who exhibited his / her valid ID indicated above.

Administering Officer
By Authority: Sec. 50, R.A 6975 as amended

Annex “G”

Republic of the Philippines)
City of _____) S.S.
X-----X

AFFIDAVIT OF RECORDING OFFICER

(In Compliance to Section 4 of A.M. NO. 21-06-08 SC)

I, _____, of legal age, PNP member presently assigned with the PNP Ant-Cybercrime Group, under oath, hereby depose and state the following:

1. I am the officer assigned to record the arrest of _____ with the following information:

a. Prior to the arrest, I notified the person to be arrested that the arrest is being recorded. I positioned myself in a location where I will have the maximum ability to record the arrest.

b. Camera used:

Body-Worn Camera (BWC) ____ Alternative Recording Device (ARD)____

Reason for use of ARD: Non-availability of PNP-issued BWC

Attached as **Annex A** is the Certificate from the PNP ACG Logistics Officer.

Standard Specifications	ARD Specifications
Brand name/Serial No.	

Video Resolution	
Frame Rate	
Audio	
Data and time stamping	
GPS	
Battery life	
Storage	
Low-light recording	

- c. The ARD was placed in a conspicuous location which maximizes the ability to capture the recording of the arrest.
- d. Date, time and duration of recording:
_____.
- e. Place of recording:
_____.
- f. Date and time of turn-over of ARD to the Data Custodian _____.

Attached as **Annex B** is the Turn-Over Slip.

- g. Name of Data Custodian conducting the download through an external storage device:
_____.
- h. The Data Custodian mentioned above will deliver the recordings to the Court (for Warrant of Arrest) or to the Prosecutor's Office (for Warrantless Arrest).

RESTRICTED

2. I execute this Affidavit to attest to the truth of the foregoing facts and in compliance to the Rules of the Use of Body-Worn Cameras in the Execution of Warrants.

NAME/RANK

Affiant

Subscribed and sworn to before me, this _____ day of _____ 2023. Affiants personally appeared before me and signed the foregoing affidavit as their free own act and deed.

Administering Officer

Annex “H”

Republic of the Philippines
Quezon City, Metro Manila

AFFIDAVIT OF DATA CUSTODIAN

I, _____, bonafide member of Philippine National Police, presently assigned with Anti-Cybercrime Group, with address at _____ and presently designated as _____, hereby depose and state the following:

1. On _____, on or about _____, (describe briefly the conduct of operation);
2. That, I took part in the said operation as one of the operatives designated as back -up security within the perimeter;
3. That prior to the launching of the said operation, we went to our Supply Accountable Officer for the issuance of two alternative recording devices (ARD) in the absence of issued-PNP body-worn camera to the PNP ACG;
4. That the said operation was properly documented by PCpl _____ who used ARD No. 1 and Pat _____ who used ARD No. 2 to take the video recording of the said operation;
5. At about 3:00 PM of the same date, immediately after the arrest, we went back to our office, I prepared the external hard drive for the transfer of the video recordings which is described as follows:

**STATE THE DESCRIPTION OF THE EXTERNAL
HARD DRIVE**

6. That on 3:05 PM of the said date, in the presence of the accused and the Complainant, I started to transfer the video recording of ARD No. 1 and ARD No. 2 to the external hard drive and by 3:30 PM of the same date, the data was successfully transferred.
7. I redacted the personal identifiers such as _____ to protect the privacy of the _____.
(depends on the case)
8. After downloading the data from the ARDs, I encrypted the data and preserved the same.
9. Thereafter, I placed it in a sealed transparent plastic envelope. I wrote the DTPO. Further, I marked it with the initials of the suspect, and I signed it.
10. Thereafter, I placed the external hard drive it in a secured cabinet inside our office prior to delivering the same to the court.
11. That, I am executing this AFFIDAVIT in compliance with the requirements of A.M. No. 21-06-08-SC (Rules on the Use of Body-Worn Cameras in the Execution of Warrants).

AFFIANT FURTHER SAYETH NAUGHT.

_____(date)_____(place).

RESTRICTED

Affiant

Subscribed and sworn to before me, this____ day of _____.

Affiant personally appeared and signed the foregoing affidavit as his free own act and deed.

Administering Officer

Annex “I”

Republic of the Philippines)
 Quezon City) S.S.
 X-----X

AFFIDAVIT OF SEIZING OFFICER

I, _____, of legal age, member of Philippine National Police and presently assigned at Anti-Cybercrime Group, Camp Crame, Quezon City after having been duly sworn to in accordance with the law do hereby depose and states, that;

1. I am designated as seizing officer during the entrapment operation at _____ that resulted to the arrest of ____ suspect identified as _____ and presently residing at _____ for violation of _____ in relation to Section 6 of Republic Act No. 10175 otherwise known as “Cybercrime Prevention Act of 2012”.
2. On _____, at about _____, personnel of PNP Anti-Cybercrime Group (ACG) _____ Unit led by _____, together with the _____ Police Station led by _____, COP conducted an entrapment operation at _____ that resulted to the arrest of _____.
3. During the conduct of entrapment operation, the undersigned while in the conduct of the arrest of the two persons, confiscated/recovered the items mentioned in the Inventory of Evidence.

The seized items were brought to the office of the PNP Anti-Cybercrime Group for temporary safekeeping; **(Inventory Receipt ANNEX “A”)**

4. The above information and circumstances will support the filing of violation of _____ in relation to Section 6 of Republic Act 10175 otherwise known as “Cybercrime Prevention Act of 2012” against the above-mentioned suspects.

FURTHER SAYETH NAUGHT:

IN WITNESS WHEREOF, I, hereunto signed this Affidavit of Seizing Officer this ____ day of _____ at _____, Philippines.

Affiant

SUBSCRIBED AND SWORN to before me this ____ day of _____ 2023, here at PNP ACG Camp BGen Rafael T Crame Quezon City and I am hereby certifying that I have personally examined the affiant and I am convinced that they voluntarily executed and understood the content of their sworn affidavit.

Administering Officer

Annex “J”



Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City



CERTIFICATION ON DATA
PRESERVATION/EXTRACTION
OF SOCIAL MEDIA/ONLINE CORRESPONDENCE

THIS IS TO CERTIFY that the following Facebook (FB) Accounts with Universal Resources Locator (URL) were authentic being saved/preserved at the Desktop Computer of this unit upon personal appearance of complainant _____ to file a formal complaint for **Sec. 4(c) 4, RA 10175 (Online Libel)** against _____ and said hard copy/printout of FB Accounts are being used in filing the aforesaid case were all certified true copy from the original online documents:

1. Facebook Account named _____ with URL _____ with User ID _____ containing post, saved and preserved on _____;

Likewise, Facebook account of complainant and witness/es were saved and preserved to wit:

2. Facebook _____ Account _____ named _____ with _____ URL _____ with User ID _____, saved and preserved on _____;

3. Facebook Account named _____ with URL _____
_____, with User ID _____
_____, saved and
preserved on _____;
4. Facebook Messenger Conversation between _____ and _____
_____ with message thread _____
_____, saved and
preserved on _____; and
5. Facebook Account named _____ with URL _____
_____ with User ID _____
_____, saved and
preserved on _____.

THIS CERTIFICATION is issued for filing of case for
Sec. 4(c) 4, RA 10175 (Online Libel) against
_____.

Issued this ____ day of ____ 2023 at ACG Regional
Anti-Cybercrime Unit __, Camp _____.

(Rank and Name of IOC)
Police Staff Sergeant
Invest PNCO

Annex “K”



Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City



(date)

PRESERVATION REQUEST

Dear _____:

This pertains to the investigation being conducted by this Group on alleged violation of Article 315 (Swindling/Estafa) of the *Revised Penal Code in relation to Section 6 of Republic Act No. 10175 otherwise known as the “Cybercrime Prevention Act of 2012”*.

Relative thereto, Section 13 of RA 10175 provides for the authority of PNP-ACG to request from the concerned service provider the preservation of computer data involved in the commission of the aforesaid offense. Reciprocally, it further states for the responsibility of your Office to preserve the integrity of traffic data and the subscriber’s information in relation with your provided communication services.

In view thereof, we would like to request your good office to preserve the traffic and subscriber’s data as well as other available information related to the mobile number listed below:

RESTRICTED

Mobile Number	Date and Time Stamp
0906xxxxxxx	03/10/2023-10:00AM-06:30PM
	03/15/2023-11:00AM-07:33PM

Kindly furnish this Group with the result/s of your action taken. This will serve as our reference in applying for the court order necessary for the release of the requested data. We will appreciate your deed of ensuring the confidentiality of this investigation by not notifying the subscriber concerned.

Should you have any concerns, kindly contact us through telephone numbers 723-0401 local 3562 and 414-1560 or e-mail address pnpacgcfcu@gmail.com citing reference number _____.

We look forward to your utmost cooperation on this matter.

Very truly yours,

Chief, RACU _____

Annex “L”



National Police Commission
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City



MEMORANDUM

FOR : Director, Anti-Cybercrime
Group
(Attn: Digital Forensic Unit)

FROM : Head of Office

SUBJECT : Request for Digital
Forensic Examination

DATE :

1. Reference:

2. This pertains to the request for the conduct of digital forensic examination on the accompanying digital evidence specifically describe on the attached Digital Forensic Examination Request Form which is owned by the ____ (*victim, witness or suspect*).

3. Background of the case with the following information:

- a) NATURE OF CASE:
- b) VICTIM:
- c) SUSPECT:
- d) T D P O:

4. The facts of the case are as follows:

5. Attached is the required storage media necessary for the digital forensic examination:

Submitted Digital Media for Digital Forensic Examination	Required Destination Storage Media
(if) One (1) Cellular Phone	<i>USB Flash Drive</i> , which capacity must be twice the capacity of the Cellular Phone's storage media.
(if) One (1) Computer System Unit / Hard Drive and other storage media.	<i>External Storage Media or Hard Drive</i> , which capacity must be twice the capacity of evidence submitted storage media.

6. The bearer of this request is (Rank Name/ Mobile Number) investigator-on case.

Note:

- a. *(For cases from Region 3, 4a, and NCR must be delivered personally by the investigator-on case.); and*
- b. *(For cases from other Regions preferably delivered by investigator-on case or official Liaison Officer).*

7. Further request that this Office be furnished a copy of the ACG digital forensic examination result for our reference.

(Head of Office)

Annex “M”

Republic of the Philippines
National Capital Judicial Region
REGIONAL TRIAL COURT
Branch _____
Pasig City

**RE: IN THE MATTER OF THE
ISSUANCE OF WARRANT TO
DISCLOSE COMPUTER DATA
(WDCD) DIRECTING UNION BANK
TO DISCLOSE TRAFFIC DATA,
SUBSCRIBER’S INFORMATION,
AND OTHER RELEVANT DATA
RELATIVE TO UNION BANK
ACCOUNT NUMBER _____
UNDER THE NAME OF
_____**

WDCD No. _____

**FOR: _____
in relation to Sec. 6 of RA
10175**

PNP Anti-Cybercrime Group
(ACG), Cyber Financial Crime
Unit represented by
_____, Officer-On-
Case

Applicant,

vs.

UNIONBANK

Respondent.

X-----X

**APPLICATION FOR THE ISSUANCE
OF A COURT WARRANT TO
DISCLOSE COMPUTER DATA (WDCD)**

The Philippine National Police, Anti-Cybercrime Group (**PNP-ACG** for brevity), represented herein by the undersigned, _____, under oath, hereby depose and state that:

1. The applicant is the Officer-On-Case (OOC) of Cyber Financial Crime Unit, Philippine National Police Anti-Cybercrime Group (ACG), and may be served with orders, notices/summons and resolutions of this Honorable Court at PNP-ACG, National Headquarters, Camp BGen Rafael T Crame, Quezon City.
2. The applicant is duly authorized by _____, OIC, PNP Anti-Cybercrime Group in applying this Warrant to Disclose Computer Data (WDCD). **Attached is the copy of the Authorization as Annex "A"**
3. The applicant has sufficient reasons to believe that respondent **UNIONBANK OF THE PHILIPPINES** possesses and controls information/data pertaining to UNIONBANK Account No. _____ **UNDER THE NAME OF** _____ which was used in a fraudulent transaction.

4. The undersigned believes that this Application is in compliant with the essential facts necessary for the issuance of a WDCD under Section 4.3 of A.M. No. 17-11-03-SC dated July 3, 2018 entitled "Rule on Cybercrime Warrant", in the following manner.

I. Facts of the Case

5. On March 15, 2023 at around 09:41 PM, the complainant _____ at _____ personally appeared before the office of PNP ACG to file a formal complaint for violations of _____ in relation to Section 6 of R.A. No. 10175 also known as "Cybercrime Prevention Act of 2012".

- **Please see Affidavit of complaint attached as Annex "B"**

6. Herein Applicant was designated as the Officer-On-Case (OOC) wherein, said complainant was assisted by _____ Investigator-On-Case (IOC) and officially recorded for investigation under blotter number: **2023-06-87**.

- **Please see attached copy of Incident Record Form (IRF) as Annex "C"**
- **Please see attached copy of Affidavit of Deposition of _____, IOC as Annex "D"**

7. Accordingly, on March 13, 2023, _____ the sister of the victim received a phone call from unregistered number _____. The caller

introduced himself as _____, a staff of the Chinese Embassy and spoke in Mandarin language. Since _____ did not know how to speak in Mandarin she gave the phone to her sister _____.

Attached is the screenshot of the call logs as Annex “E”

8. The caller _____ relayed to the complainant _____ that her sister _____ had a pending case in China regarding Money Laundering that needs to be settled. The complainant was surprised since her sister was residing here in the Philippines.
9. However, believing that it was true, the victim asked the caller on how to settle the case. Thereafter, _____ informed her that he will transfer the line to Shanghai Police Department. On the same date, the victim was able to talk with a certain _____ who pretended to be from the Shanghai Police Department and informed the victim that they will clear the name of _____.
10. Relatedly, _____ asked the Viber account of the victim _____ to talk about the case of her sister. On March 14, 2023, _____ called _____ and narrated that it was not her sister who has a pending case but her.
11. On March 14, 2023, _____ endorsed the victim to another person who

pretended to be _____ which according to _____ will help the victim.

12. On the same date, _____ called the victim using Viber account _____ and said that the victim needs to pay _____ to clear her name in Court. The said _____ provided the bank account details where the money should be deposited. Believing it was true, the victim deposited _____ to **Unionbank** account No. _____.

- **Please see photocopy of deposit slip attached as Annex “F”**
- **Please see copy of conversation attached as Annex “G”**

13. After sending the said money, _____ instructed the victim that he will give update of the case on the following day.
14. On March 15, 2023, _____ sent a message to the victim that he already went to the Chinese Notary Office and he was informed that the _____ was not enough to clear the name of the victim.
15. _____ further stated in his message that the victim needs to pay _____. On the same date, _____ instructed the victim to open a Unionbank Bank account. In which, on March 15, 2023 the victim proceeded to Unionbank United Nation Ave. branch and open a bank account.

Attached is the screenshot of the conversation as Annex ____

16. On March 16, 2023, _____ demanded and instructed the victim to forward the user and password of the Online banking account of the victim. After the victim forwarded the above-mentioned information of her bank account, she noticed that her Union bank account had multiple illegal/unauthorized transactions amounting to _____ made by the unknown perpetrator.

- **Please see copy of Statement of Account attached as Annex “H”**
- **Please see photocopy of text message notification Annex “I”.**

17. Based on the foregoing facts, the unknown perpetrator was able to illegally and unlawfully access the Union Bank account of the herein victim and fraudulently transferred it thru the **UNIONBANK with account numbers** _____ with the total amount of _____ was transferred to above-mentioned Bank of the Philippine Island (BPI) account.

Attached is the Bank Dispute Report as Annex ____

18. Based on the foregoing facts, the unauthorized fund transfers were made thru the **UNIONBANK** account numbers _____ under the name of _____ with the total amount of _____ (Php_____).

II. Relevance and Necessity:

19. Despite the conduct of social media exploitation and online investigation, the ACG could not determine the identity of the mobile numbers used in creating the viber account involved including the bank account owner which was being used by an unknown perpetrator/s involved in the fraudulent transactions.
20. On the basis of the above facts, there is *prima facie* evidence showing that the person behind the subject UNIONBANK Account numbers committed acts that constitute violations of _____ in relation to Section 6 of R.A. No. 10175 also known as "Cybercrime Prevention Act of 2012".
21. However, herein applicant could not successfully prepare and refer the case for preliminary investigation unless the identity of the unknown suspect/s behind the aforementioned **UNIONBANK** account numbers are known.
22. It is the humble belief of herein Applicant that the account details (such as name and address), and other relevant information, which is in the possession of UNIONBANK account will surely be led to the identification of the person/s responsible for the fraudulent transactions.

III. NAMES OF INDIVIDUALS WHOSE DATA ARE SOUGHT TO BE DISCLOSED:

23. The _____ transaction amounting to _____ (Php _____) was

illegally/fraudulently transferred to the following
UNIONBANK account numbers:

UNION BANK Account No.	Date of Transaction	Account Name	Amount

**IV. PARTICULAR DESCRIPTION OF THE DATA
SOUGHT TO BE DISCLOSED**

24. The data sought to be disclosed will aid the applicant in the identification of the person/persons responsible for the fraudulent transactions using the aforementioned **UNIONBANK** account, to wit:
- a. Account information such as full name, personal information, and address of the account owner;
 - b. Submitted verification ID when applying the subject bank accounts;
 - c. Results of Know Your Customer (KYC) verification regarding the submitted proof of identity and other documents when applying the subject bank accounts;
 - d. Contact details (Internet Protocol (IP) address, Email address, landline phone or cellular number; and
 - e. Any other relevant information that will lead to the identity of the alleged suspect.

25. This application will not cover the disclosure of financial transactions or bank deposits but merely requests for information that could establish the identity and address of the account holder which is authorized pursuant to Section 14 of R.A. No. 10175 (Cybercrime Prevention Act) and Section 4 of the Rule on Cybercrime Warrants.

V. PLACE AND MANNER BY WHICH DISCLOSURE IS TO BE CARRIED OUT:

26. The data in printed form/hard copy, duly authenticated by the authorized person who made the report/disclosure may be disclosed and provided to ACG through herein applicant.

**UNIONBANK
ADDRESS**

VI. LEGAL BASIS:

27. This Application for Warrant to Disclose Computer Data is filed before this Honorable Court in accordance with Section 2.2 of the A.M. No. 17-11-03-SC or the Rules on Cybercrime Warrants which states that:

**“Section 2.2”. *Where to File an Application for a Warrant.* –
xxx**

On the other hand, an application for a warrant under this Rule for violation of Section 6, Chapter II of RA 10175 (all crimes defined and penalized by the Revised Penal

Code, as amended, and other special laws, if committed by, through, and with the use of ICT) shall be filed by the law enforcement authorities with the regular or other specialized regional trial courts, as the case may be, within its territorial jurisdiction in the places above-described.”

28. This Honorable Court has authority and jurisdiction to issue a WDCD on this case.

P R A Y E R

WHEREFORE, premises considered, it is respectfully prayed for unto this Honorable Court that a WARRANT TO DISCLOSE COMPUTER DATA be issued directing **UNIONBANK of the PHILIPPINES with office address at _____** to release preserved data /information pertaining UNIONBANK account numbers which were the recipients of the illegally access account of the victim, to wit:

UNION BANK Account No.	Date of Transaction	Account Name	Amount

- a. Account information such as full name, personal information, and address of the account owner;
- b. Submitted verification ID when applying the subject bank accounts;

- c. Results of Know Your Customer (KYC) verification regarding the submitted proof of identity and other documents when applying the subject bank accounts;
- d. Contact details (Internet Protocol (IP) address, Email address, landline phone or cellular number;) and
- e. Any other relevant information that will lead to the identity of the alleged suspect.

Other reliefs, which are just and equitable under the premises, are likewise prayed for.

Quezon City, Philippines ____ day of March 2023.

Officer-On-Case, CFCU

SUBSCRIBED AND SWORN to before me this ____ day of March 2023 at Quezon City.

Administering Officer

CERTIFICATION AND VERIFICATION

I, _____, Investigator of Cyber Financial Crime Unit, Philippine National Police Anti-Cybercrime Group, of legal age, single, with office address located at Camp BGen. Rafael T. Crame, Quezon City after being duly sworn, hereby depose and state that:

- a. I am the Applicant in the above-captioned case;

- b. I have caused the preparation and filing of the foregoing Application;
- c. I have read and understood the content of the said Pleading and attest that the content thereof are true and correct based on my own personal knowledge or Authentic records;
- d. I further certify that:
 - d1. I have not commenced any other proceeding involving the same issues subject matter of this pleading in the Supreme Court, Court of Appeals or the different Divisions thereof, the Regional Trial Court, or any judicial tribunal or agency in the Philippines, and that to the best of my knowledge no such Action is pending; and
 - d2. In the event that I should learn that a similar action or Proceeding has been filed or is pending before the Supreme Court, Court Appeals, or the different divisions thereof, the Regional Trial Court, or any other tribunal or agency, I undertake to promptly inform this Honorable Office of that fact within five days there from.

Other reliefs just and equitable under circumstance are similarly prayed for.

Quezon City, Philippines ____ day of March 2023.

Affiant

SUBSCRIBED AND SWORN to before me this ____ of March 2023 at Quezon City, Philippines.

Administering Office

Annex “N”

**REPUBLIC OF THE PHILIPPINES
REGIONAL TRIAL COURT
BRANCH _____
Pasig City**

**IN THE MATTER OF THE ISSUANCE OF
A COURT WARRANT DIRECTING THE
EASTERN DISTRICT ANTI-
CYBERCRIME TEAM TO CONDUCT
DIGITAL FORENSICT EXAMINATION TO
(DESCRIPTION OF GADGET WITH SIM
CARD)
WECD NO. _____**

**FOR: Violation of Art. 248
of the Revised Penal
Code.**

Eastern Police District,
Pasig City Police as represented
by _____,

Applicant,

x-----x

**APPLICATION FOR ISSUANCE OF COURT
WARRANT TO
EXAMINE COMPUTER DATA**

The Eastern Police District, Pasig City Police Station, with office address at C. Raymundo Ave., Brgy. Caniogan, Pasig City, represented herein by the undersigned, _____, under oath, hereby depose and state that:

1. Herein Applicant is a member of the Eastern Police District, Pasig City Police presently assigned at Pasig City Police Station, and may be served with orders, notices/summons and resolutions of this Honorable Court at C. Raymundo Ave., Brgy. Caniogan, Pasig City.
2. The undersigned is the Investigator on Case and authorized by the Team Leader, Eastern District Anti-Cybercrime Team (EDACT), PNP Anti-Cybercrime Group to file this Application for the issuance of a Warrant to Examine Computer Data (WECD) before this Honorable Court which is attached as **Annex A**;
3. The applicant has sufficient reasons to believe that the mobile device recovered during the surrender of the suspect contains relevant information/data to be used as evidence in the prosecution of case against _____ and cohorts for violation of Art. 248 RPC. Attached is the Affidavit of Arrest as **Annex "B"**;
4. This Application complies with the essential facts necessary for the issuance of a WECD under Sections 4.3 and 6.9 of A.M. No. 17-11-03-SC dated July 3, 2018 entitled "Rule on Cybercrime Warrant", as follows:

I. Antecedent Facts

5. This pertains to the shooting incident that transpired at around 5:45 PM of March 15, 2023, in front of _____ located at _____ which resulted in the death of _____

_____, 37 years of age, married and resident of _____, and a member of the Sangguniang Barangay of _____.

6. During the investigation, it revealed that the victim was then sitting and talking with witness _____ and _____ when the suspect approached and shot the victim's head at close range before fleeing the scene of incident on board a motorcycle driven by his cohort and parked along the nearby Ortigas Ave., Extension. The victim was brought by the members of the Barangay _____ Emergency/Rescue Unit on board an ambulance to the Medical City for treatment but he was pronounced DOA by the attending physician.
7. The crime scene was processed by the EPD Crime Laboratory Office's SOCO Team and one fired cartridge case of caliber .45 was recovered and now being subjected to ballistic examination.
8. Victim was very active in supporting law enforcers in their operations in Brgy. Rosario specially in anti-illegal drug operations and this might have been the primary reason for his shooting incident.
9. Based on the several CCTV footage gathered by the Special Investigation Task Group (SITG) relative to this case, the trigger/gun man was aided by at least three other persons specifically as follows: one unidentified driver and/or passenger of a Mitsubishi Montero SUV

with fake license plate number and seen at the Jollibee food store near the scene of incident; one unidentified driver of the get-away motorcycle; and one of the lookouts.

10. During the continuous follow-up operation of the Pasig City Police Station on the case, the suspect who shot the victim at close range was identified as _____.
11. That on October 26, 2023 at around 1:00 PM, the suspect _____ out of fear for his family voluntarily surrendered at _____ and he was subsequently placed under the custody of this station to give protection. Attached copy of blotter/any document to support his voluntary surrender as Annex ____.
12. Upon surrender, _____ voluntarily submitted his cellphone to give aid to the investigation being conducted by the Pasig City Police Station.
13. The case for violation of Art. 248 (Murder) of the Revised Penal Code against **suspect** _____ is being prepared before the city prosecutor office.

II. Relevance and Necessity

14. On the basis of the above facts and circumstances, the Applicant believes that the recovered mobile device from _____ during his surrender is relevant and material for his prosecution including his cohorts for

violation of Art. 248 of the RPC. It will corroborate the pieces of evidence at hand and it will ratify and confirm that the respondent indeed committed the crime stated.

15. Thus, there is a need for the conduct of digital forensic examination on the recovered devices to examine computer data mentioned in paragraph 19, in order to support the prosecution of the aforementioned violations of law against _____.

III. Computer Device Sought to be Examined

16. The herein Applicant is also the Evidence Custodian of the following **mobile device** that was voluntarily surrendered by the suspect as **Annex "C"**

1 blue Huawei Android phone marked as
_____ with Smart sim card number _____
Globe Sim card number _____.

IV. Particular Description of the Data Sought to be Examined

17. The data sought to be examined will aid the Applicant in the prosecution of cases against the suspects and the identification of the other person/persons, conspirators that are responsible for the offense committed:
 - a. Name, personal information, photos and address of the person/s who are involved in the illegal activities;

- b. Email logs/conversation/multimedia files;
- c. SMS, Multimedia and Chat Messages;
- d. Call logs; and
- e. Any other relevant information necessary to support the prosecution of the case against the suspect/s.

V. Legal Basis

18. The recovered devices as described in paragraph 19 hereof were made pursuant to a voluntary surrender of the suspect, hence, may be subject to the issuance of a *Warrant to Examine Computer Data* under Section 6.9 of A.M. No. 17-11-03-SC which provides that:

Section 6.9. *Examination where lawful possession of device is obtained; Warrant to Examine Computer Data (WECD).* - Upon acquiring possession of a computer device or computer system via a lawful warrantless arrest, or by any other lawful method, law enforcement authorities shall first apply for a warrant before searching the said computer device or computer system for the purpose of obtaining for forensic examination the computer data contained therein. The warrant therefore shall be denominated as a Warrant to Examine Computer Data (WECD).

x x x

19. This Application for Warrant to Examine Computer Data is filed before this Honorable Court in accordance with Section 2.2 of the A.M. No. 17-11-03-SC or the Rules on Cybercrime Warrants which states that:

“xxx On the other hand, an application for a warrant under this Rule for violation of Section 6, Chapter II of RA 10175 (all crimes defined and penalized by the Revised Penal Code, as amended, and other special laws, if committed by, through, and with the use of ICT) shall be filed by the law enforcement authorities with the regular or other specialized regional trial courts, as the case may be, within its territorial jurisdiction in the places above-described.”

20. This Honorable Court has authority and jurisdiction to issue a WECD on this case.

P R A Y E R

WHEREFORE, premises considered, the undersigned most respectfully prays for:

- a. The issuance of a **WARRANT TO EXAMINE COMPUTER DATA** on the following devices listed below:

1 blue Huawei Android phone marked as _____
with Smart sim card number _____
Globe Sim card number _____.

b. To direct the Digital Forensic Examiner of Eastern District Anti-Cybercrime Team in coordination with the Digital Forensic Unit, PNP Anti-Cybercrime Group with office address at Camp BGen Rafael T Crame, Quezon City to examine the computer data on the above-mentioned digital devices:

- b.1. Name, personal information, photos and address of the person/s who are involved in the illegal activities;
- b.2. Email logs/conversation/multimedia files;
- b.3. SMS, Multimedia and Chat Messages;
- b.4. Call logs; and
- b.5. Any other relevant information necessary to support the prosecution of the case against the suspect/s.

Other reliefs, which are just and equitable under the premises, are likewise prayed for.

This ____ of _____, 2023 at Pasig City, Philippines.

Applicant

SUBSCRIBED AND SWORN to before me this ____ of _____, 2023 at Pasig City, Philippines.

Administering Officer

CERTIFICATION AND VERIFICATION

I, _____, member of the Eastern Police District, Pasig City Police Station, currently assigned as Investigator of Pasig City Police, with office address at C. Raymundo Ave., Brgy. Caniogan, Pasig City, after being duly sworn, hereby depose and state that:

- a. I am the Applicant in the above-captioned Application for a Court Warrant to Examine Computer data (WECD);
- b. I have caused the preparation and filing of the foregoing Application;
- c. I have read and understood the content of the said Application and attest that the content thereof are true and correct based on my own personal knowledge or Authentic records;
- d. I further certify that:
 - d1. I have not commenced any other proceeding involving the same issues subject matter of this pleading in the Supreme Court, Court of Appeals or the different Divisions thereof, the Regional Trial Court, or any judicial tribunal or agency in the Philippines, and that to the best of my knowledge no such Action is pending; and

d2. In the event that I should learn that a similar action or Proceeding has been filed or is pending before the Supreme Court, Court Appeals, or the different divisions thereof, the Regional Trial Court, or any other tribunal or agency, I undertake to promptly inform this Honorable Office of that fact within five days there from.

Other reliefs just and equitable under circumstance are similarly prayed for.

Pasig City, Philippines ____ day of _____ 2023.

Affiant

SUBSCRIBED AND SWORN to before me this ____ of _____, 2023 at Pasig City, Philippines.

Administering Officer

Annex “O”

**Republic of the Philippines
National Capital Judicial Region
REGIONAL TRIAL COURT
Branch ____,
MANILA**

**Philippine National
Police, Anti-
Cybercrime Group,
Cyber Response
Unit, as represented
by _____,**

Applicant,

versus

**_____ or other
managers, team
supervisors, team
leaders, operators,
and all occupants of
branches**

**_____ located
at _____ for
violation of 4 (a) (5)
[Misuse of Device]
of Republic Act No.
10175 (Cybercrime
Prevention Act of
2012).**

Respondents,

**WSSECD
NO. _____
FOR Violation
Section 4 (a) (5)
(i) (ii) (Misuse
of Device) of
Republic Act
10175
otherwise
known as the
“Cybercrime
prevention
Act” of 2012**

X ----- X

**APPLICATION FOR WARRANT TO
SEARCH, SEIZE, AND EXAMINE COMPUTER DATA
(WSSECD)
(Pursuant to Section 15 of RA No. 10175 and Section 6
of A.M. No. 17-11-03-SC)**

The Philippine National Police, Anti-Cybercrime Group (PNP ACG) represented herein by _____, under oath, do hereby depose and states, that:

1. The Applicant is designated as the Team Leader and presently assigned at PNP ACG Cyber Response Unit (CRU), and may be served with orders, notices/summons and resolutions of this Honorable Court at PNP ACG Compound, Camp BGen Rafael T Crame, Quezon City.
2. The Applicant is duly authorized by the Director, ACG, to file this instant application for a Warrant to Search, Seize and Examine Computer Data (WSSECD) for Violation Section 4 (a) (5) (i) (ii) (Misuse of Device) Republic Act No. 10175 (Cybercrime Prevention Act of 2012) Attached is the Letter Endorsement from the Director, ACG dated March 6, 2023, hereto attached as **Annex "A"** and made as an integral portion of this Application.
3. I and my deponent verily believed and have personal knowledge gained from the conduct of physical surveillance and verification that _____ alias "_____" and _____ or other managers, supervisors, team leaders, operators, and all occupants of the branches of _____ located at _____ for violation of

Section 4 (a) (5) [Misuse of Device] of Republic Act No. 10175 (Cybercrime Prevention Act of 2012).

4. By virtue of the said acts, the undersigned applicant and my deponent have reasonable grounds to believe that _____ or other managers, supervisors, team leaders, operators, and all occupants of the branch of _____ located at _____ were engaged in illegal online activity which constitutes violation of Section 4 (a) (5) [Misuse of Device] of Republic Act No. 10175 (Cybercrime Prevention Act of 2012).

I. FACTS OF THE CASE

5. On February 17, 2023, an informant with alias name “_____”, appeared to this Group and reported that the office where he was working was engaged in illegal activities by sending link to acquire victims’ personal information which was operated by their company name “_____”.
6. Accordingly, the Circalis Marketing Services company was owned by a certain _____ or other managers, supervisors, team leaders, operators, and all occupants of branches of _____ located at _____.
7. On February 23, 2023 at around 11:00 AM, personnel of this Unit led by _____, under direct supervision of _____ conducted a surveillance operation on February 24, 2023 at _____.
8. On the same day, the team arrived at _____ and one of the operating team _____ was tasked to infiltrate the said Office by applying as

agent. _____ was approached by a concern person for recruitment and asked several questions regarding the vacant position. When Pat _____ entered in the said office, she noticed multiple desktops and laptops which were used by the agents. After several minutes, she was called by the person who approached her and stated that she needs to follow-up her application next week and on that week, she will be subject to orientation about her job. **(See Attached _____ as ANNEX “___”)**
indicate what document is being attached

9. Thereafter, the team drove to the next target area located at Unit 2, 3rd Floor, 167 Place RCBCON Building, Don Mariano Marcos, Commonwealth Avenue Quezon City. One of the operating team _____ was also tasked to infiltrate the said Office by applying as agent.
10. When _____ reached the glass door, _____ immediately informed the guard that she will apply for a vacant position. When Pat _____ entered the main room, she spotted numerous sets of desktop and other agents working in their station. She also noticed the white board attached to the wall with written date, names and shapes. The area has three (3) small rooms for other transaction and one (1) well lighted room which was allegedly occupied by more or less 25 agents. **(See Attached _____ as ANNEX “___”)**
11. During the conduct of surveillance of _____ inside the said office, she was catered by a certain _____ as well as the other agent _____ and started to asked questions in relation to the job description she had in the past

employments. They started the conduct of initial orientation. Thereafter, _____ was assisted by _____ and was asked if she was willing to accept the job after the initial orientation on the office policy. An initial demonstration on how they talked to foreigners using models' identity was also shown to her. _____ stated that if _____ wants the job, she just needs to return and bring with her an additional 2x2 picture.

12. On February 28, 2023, team led by _____ together with _____ and _____ conducted a follow-up surveillance at _____ to check if the office are still in the building and for additional gathering of information.
13. On the same day, the team arrived at _____ to drop-off _____ for the follow-up of her application and orientation. _____ proceeded in the said office and was again approached by the same person. _____ was introduced to another agent who started to orient her on how to work as agent. First, _____ was instructed to make a social media account which will be used to engage and look for a client and next was to make a pioneer account with "_____" and "_____" which will be used to get links of sensitive site.
14. Once _____ was able to have a client, she needs to seduce it to enter into a site provided by a pioneer account ("circularischat.com" and "powercastcash.com"). Once the victim clicks the said link, they will be required to fill-out verification process form, in which the client would encode his card details and once it is done, the assigned team

leader will immediately shake his handbell which will indicate that access to the client's bank account was already done.

15. Provide facts that access to the client's bank account would constitute Misuse of Device.
16. On the same day, at around _____, the team arrived at _____ to drop-off _____ for her orientation. During the orientation, she was assisted by Jason to create a social media account and pioneer accounts. Jason also showed her how to make conversation to the foreign client via Instagram wherein, he/she later forwarded a pornographic link from alleged pioneer account ("circularchat.com" and "supreme chatter"). Therein, the agent then instructed his client to click the forwarded link and fill-out the verification process form, in which the client would encode his card details and once it is done, the assigned team leader will ring the bell to indicate that access to the client's bank account was already done. **(See Attached _____ as ANNEX "_____")**
17. While _____ was walking inside the said office, she was able to discreetly took photos and videos. She was able to observed that there were more or less 24 units of complete desktops which were installed for the agents and allegedly used for their operation. _____ also noticed the white board attached on the wall where the names of agents were indicated and two (2) separate desks besides the wall allegedly allocated only for the team leaders. The Team Leaders has their own complete set of desktop, handbell, telephones, router and other equipment. **(See Attached _____ as ANNEX "D")**

18. *Provide facts that access to the client's bank account would constitute Misuse of Device.*

19. Moreover, _____ saw a brown board attached to the wall with pinned documents. Upon close examination, it was a Statement of Account from Philippine Long Distance Telephone Company (PLDT) with account Number _____ dated _____ under the name of _____ with its address. **(See Attached _____ as ANNEX "E")**

20. On the basis of the above facts, there is prima facie evidence showing that _____ and _____ or other managers, supervisors, team leaders, operators, and all occupants of branches of _____ located at _____ and _____ has in their possession devices used and intended to be used in online illegal activities for violation of 4 (a) (5) [Misuse of Device] of Republic Act No. 10175 (Cybercrime Prevention Act of 2012) as mentioned in Paragraph 13 hereof.

21. Taking into custody and examining the items listed in paragraph 23 hereof which are being used in online illegal activities are essential to held _____ or other managers, supervisors, team leaders, operators, and all occupants of the offices liable for the aforementioned illegal act.

II. NAMES OF INDIVIDUALS WHO HAVE CONTROL, POSSESSION TO THE COMPUTER DEVICES

22. The place sought to be searched, seized and examined for violation of Section 4 (a) (5) [Misuse of Device] of Republic Act No. 10175 (Cybercrime Prevention Act of 2012) is owned/operated by:

_____ or other managers, supervisors, team leaders, operators, and all occupants of branches _____ located at:

- a. _____; and
- b. _____.

III. PLACE AND MANNER BY WHICH THE SEARCH, SEIZURE AND EXAMINATION IS TO BE CARRIED OUT

23. The computer devices may be searched, seized, and examined at the _____ at branch offices which are located at:

- a. _____; and
- b. _____.

24. During the implementation of WSSECD, both on-site and off-site examinations will be conducted. The report/disclosure will be authenticated by the person who made the examination on the subject devices.

IV. PARTICULAR DESCRIPTION OF THE COMPUTER DEVICES

25. The search, seizure and examination of the items being used in committing Misuse of Devices are concealed at the above-mentioned premises, to wit:

Desktop computers and its peripherals (connected or remote);
Laptops and its peripherals (connected or remote);
Modem/routers (connected either by cable or remote);

Other communication/electronic devices (connected or remote);
Digital storage devices such as SD cards, thumb drives, and external drives, or webcams;
Smart Phones;
iPods/Tablets;
Cameras/Video cameras;
Bank Transactions, bank books, transaction receipts and other documents used in the Online Lending operations; and
CCTV/Hard drive.

V. RESULT OF CASING AND SURVEILLANCE

26. The Operatives of Cyber Response Unit (CRU) conducted verification and surveillance operation at the above-mentioned address of the suspects in a building located at _____.

After Surveillance Report dated _____ as ANNEX _____

Attach are pictures of the areas as Annex ____ and Annex ____

Attach is the Sketch/Floor Plan as Annex ____

27. The surveillance operatives had successfully confirmed that the subject of the surveillance operation and personally witnessed that the employees of the above-mentioned company is indeed involved in alleged sending link to acquired victims' personal information.

28. Based on the foregoing, herein Applicant have reasons to believe that the respondents _____ or other managers, supervisors, team leaders, operators, and all occupants of branches of _____ and _____ committed acts in

violation of 4 (a) (5) [Misuse of Device] of Republic Act No. 10175 (Cybercrime Prevention Act of 2012).

29. Herein Applicant have verified the information given by alias _____ through a series of surveillance operations conducted by the operatives of Cyber Response Unit, Anti Cybercrime Group. Thus, the Applicant believes that there is sufficient probable cause for this Honorable Court to authorize the undersigned or any agent of the law to conduct search, seizure and digital forensic examination on the electronic and digital pieces of evidence on the premises where _____ or other managers, supervisors, team leaders, operators, and all occupants of branches of _____ which are located at _____ and _____ for violation of Section 4 (a) (5) [Misuse of Device] of Republic Act No. 10175 (Cybercrime Prevention Act of 2012).

VI- COMPLIANCE TO THE RULES ON THE USE OF BODY-WORN CAMERAS IN THE EXECUTION OF WARRANTS PURSUANT TO SC AM No. 21-06-08-S

30. For information of this Honorable Court, in view of the limited PNP-issued Body-Worn Camera (BWC), resort to the use of two Alternative Recording Devices (ARD) will be made with the following specifications:

Standard Requirements	ADR No. 1	ADR No. 2
Brand name/Serial No.	XXXXXXX XXXX	XXXXXXXXXX

RESTRICTED

Video Resolution	720p and Higher	720p and Higher
Frame Rate	30 – 60 frame per Second	30 – 60 frame per Second
Audio	Built-in	Built-in
Data and time stamping	Built-in	Built-in
GPS	Built-in	Built-in
Battery life	8hrs continuous with Power Bank	8hrs continuous with Power Bank
Storage	Capable of 8hrs continuous audio video footage	Capable of 8hrs continuous audio video footage
Low-light recording	Built-in	Built-in

Standard Requirements	ADR No. 3
Brand name/Serial No.	Realme 7i/XXXXXXXXXXXX
Video Resolution	720p and Higher
Frame Rate	30 – 60 frame per Second
Audio	Built-in
Data and time stamping	Built-in

GPS	Built-in
Battery life	8hrs continuous with Power Bank
Storage	Capable of 8hrs continuous audio video footage
Low-light recording	Built-in

31. Attached is the Certification from the PNP ACG Logistics Section which states that no BWC was issued to PNP ACG, herein attached as **Annex “__”**.
32. In view thereof, the Applicant is seeking the imprimatur of this Honorable Court to use the aforementioned ADRs in the execution of the WSSECD.

VII. LEGAL BASIS

33. Section 6 on the “Rule of Cybercrime Warrants” in relation to Section 15, Chapter IV of RA 10175 provides the authority for law enforcement authorities, to secure a Warrant to Search, Seize and Examine Computer Data (WSSECD).
34. This Application is filed before this Honorable Court pursuant to the Rule on Warrants which states that:

“Section 2.2. Where to File an Application for a Warrant.

“An application for a warrant under this Rule concerning a violation of Section 4 (Cybercrime Offenses) and/or Section 5 (Other Offenses), Chapter II of RA 10175 shall be filed by the law

enforcement authorities before any of the designated cybercrime courts of the province or the city where the offense or any of its elements has been committed, is being committed, or is about to be committed, or where any part of the computer system used is situated, or where any of the damage caused to a natural or juridical person took place. However, the cybercrime courts in Quezon City, the City of Manila, Makati City, Pasig City, Cebu City, Iloilo City, Davao City and Cagayan De Oro City shall have the special authority to act on applications and issue warrants which shall be enforceable nationwide and outside the Philippines.

On the other hand, an application for a warrant under this Rule for violation of Section 6, Chapter II of RA 10175 (all crimes defined and penalized by the Revised Penal Code, as amended, and other special laws, if committed by, through and with the use of ICT) shall be filed by the law enforcement authorities with ¹the regular or other specialized regional trial courts, as the case may be, within its territorial jurisdiction in the places above-described.”

This application is being filed before this honorable court to avoid leakages of this application for WSSECD considering the information obtained during the investigation that the subjects of this warrant have connections in the local government Offices, Law Enforcements and court personnel in Quezon City.

35. This Honorable Court has authority and jurisdiction to issue a WSSECD on this case.

PRAYER

WHEREFORE, the undersigned applicant respectfully prays that:

1. The Honorable Court cause the immediate issuance of a Warrant to Search, Seize, and Examine Computer Data commanding any Police Officer to conduct a search on the above-described premises and seize all items described above and examine computer data and be dealt with as the law directs;
2. To include in the WSSECD an express authority to serve the warrant at any time of the day or night including Saturdays and Sundays, including holidays and weekends, and to break open to and from the premises should the owner refuse entry inside the premises or is not in there;
3. To include in the WSSECD an express authority to immediately conduct onsite digital forensic examination, if possible, of the content of the

digital devices by trained examiners of PNP Anti-Cybercrime Group;

4. To include in the WSSECD an express authority for PNP Anti-Cybercrime Group, Digital Forensic Laboratory in Camp BGen Rafael T Crame, Quezon City to conduct a full forensic examination of the seized digital, electronic, or storage devices within the period allowed by the rules;
5. To include in the WSSECD the express authority to intercept communications and computer data reasonably related to the Respondent's activities in relation to the Misuse of Devices and other related acts during the implementation of the WSSECD;
6. To Include in the WSSECD the express authority for the Applicant to retain and utilize the seized and examined computer data, including the result of the onsite and offsite computer forensic examination, in the investigation and the subsequent filing of Violation Section 4 (a) (5) (i) (ii) (Misuse of Device) of Republic Act 10175 against Respondent and his cohorts; and
7. To include in the WSSECD an express authority for PNP-Anti-Cybercrime Group operating personnel to use the Alternative Recording Device (ARD) for the reason that this Group has not yet received the allotted Body Worn Cameras in compliance with section 4 of A.M No. 21-06-08 SC.

Other reliefs, which are just and equitable under the premises, are likewise prayed for.

_____, Philippines ____ day of March 2023.

Applicant

SUBSCRIBED AND SWORN to before me this ____ day of March 2023 at _____, Philippines.

Administering Officer

**VERIFICATION AND
CERTIFICATION OF NON-FORUM SHOPPING**

I, THE UNDERSIGNED, under oath, deposes and says that:

I am the applicant of the above-entitled application for a Warrant to Search, Seize and Examine Computer Data (WSSECD);

I personally caused the preparation of the foregoing application for WSSECD and have read its content and the allegations therein, which are true and correct to my own personal knowledge and belief.

I further certify that (a) I have not therefore commenced or filed any application for a WSSECD involving the same issues in any court, tribunal or quasi-judicial agency and to the best of my knowledge, no such

RESTRICTED

other application for WSSECD is pending therein; (b) if there is such other pending application for WSSECD, I will therefore inform this Honorable Court of the present status thereof; (c) if I should thereafter learn that the same and similar application for WSSECD has been filed or its pending, I shall report that fact within five (5) days there from to this Honorable Court, wherein the aforesaid application for WSSECD has been filed.

Applicant

SUBSCRIBED AND SWORN to before me this ____
day of March 2023 at _____
Philippines.

Administering Officer

Annex “P”



Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

[Date]

[INSERT NAME OF SERVICE PROVIDER (SP)]
[Insert Address of SP]

ORDER FOR THE DISCLOSURE OF COMPUTER DATA

Dear Sir/Ma'am:

Pursuant to Section 14 of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 and Section 4.1. Disclosure of Computer Data of Administrative Matter No. 17-11-03-SC or the Rule on Cybercrime Warrants issued by the Philippine Supreme Court, attached is a copy of a Warrant for the Disclosure of Computer Data (WDCD) with No. _____ which was issued by Honorable [INSERT NAME OF JUDICIAL AUTHORITY], Presiding Judge, Branch [___], Regional Trial Court, [_____, Philippines dated _____. The WDCD authorizes the PNP Anti-Cybercrime Group, Regional Anti-Cybercrime Unit __ to issue this Order requiring [INSERT NAME OF SP] for the disclosure of computer data on a _____ account with the following details:

1. _____;
2. The requested data was preserved in accordance with an earlier request for preservation issued by [indicate the authority,

RESTRICTED

and, if available, the date of transmission of request and reference number].

In view of the foregoing, you are hereby ordered to release, within seventy-two (72) hours from receipt of this Order, the following information:

(sample only, it would depend on what is indicated in the court order)

- a. Account information such as full name, personal information, and address of the account holder;
- b. Submitted verification ID when the account was opened;
- c. Contact details (Phone or cellular number;)
- d. Any other relevant information that will lead to the identity of the account holder; and
- e. A statement or affidavit authenticating that the electronic evidence requested is under _____ management, control and custody.

All questions and compliance in relation to this Order must be sent to [NAME OF AUTHORIZED PERSON, CONTACT INFORMATION including official email address, phone number with international code.]

We look forward to your utmost cooperation on this matter.

Very truly yours,

PCOL _____
Chief, RACU _

Annex “Q”

Republic of the Philippines
REGIONAL TRIAL COURT
Branch --
---Judicial Region
_____ City

*RE: Application for a
Warrant to Disclose
Computer
Data under Section
15 of Republic Act
No. 10175*

WDCD No.

(Name of IOC)

Representing the
Philippine National
Police
Anti-Cybercrime
Group
Regional Anti-
Cybercrime Unit
___Applicant,

X-----X

**COMPLIANCE/INITIAL RETURN OF WARRANT TO
DISCLOSE COMPUTER DATA (WDCD) with MOTION
FOR EXTENSION OF TIME TO SUBMIT COMPUTER
DATA**

COMES NOW, the undersigned applicant, _____,
Investigator On Case presently assigned with PNP Anti-
Cybercrime Group, Regional Anti-Cybercrime Unit ____
(RACU __) with office address at Camp _____,

most respectfully return unto this Honorable Court the above-described Warrant To Disclose Computer Data (WDCD) dated March 15, 2023, with the following information:

1. On _____, a Warrant to Disclose Computer Data (WDCD) No. _____ was issued by the Court signed by Honorable _____ Presiding Judge, Regional Trial Court __, Branch __, _____ City. The said order authorizes RACU -- as represented by the undersigned to issue an order compelling _____ located at _____ to disclose computer data pertaining _____ Account No. 0999xxxxxx, 0967xxxxxxx and 0928xxxxxx. A Copy of WDCD No. 1 is hereto attached as **"Annex A"**;
2. Relative thereto, the undersigned received the WDCD _____ on _____. Thereafter, RACU ____ through the Undersigned, prepared the Compliance Order dated _____ addressed to _____ hereto attached as **"Annex B"**;
3. On _____, at about _____, this unit requested for assistance from Southern District Anti-Cybercrime Team (SDACT) located at 2nd Floor SPD Building Fort Bonifacio, Taguig City, Metro Manila, Philippines to serve the Compliance Order. The same was sent via electronic mail in their email address pnnp.sdact@gmail.com the copy of the Order and the WDCD _____.

4. On _____, at about _____, a hard copy of the order was sent via JRS Express with tracking number _____ dated _____. On the same date, at about _____ personnel of SDACT implemented the said Order at _____ at the address _____. *A copy of sent email, received order by BDO and LBC Receipt are hereto attached as Annexes “C”, “D”, and “E”, respectively.*
5. In view thereof, the undersigned would like to file this Initial Return in compliance to Section 4.5 of the Rule on Cybercrime Warrant. Further, the Undersigned is respectfully requesting for an extension of ten (10) days reckon from the time this Honorable Court issue an order granting the request in order to give the respondent (GCash) ample time to search and process the requested records of the computer data.

PRAYER

WHEREFORE, premises considered, the undersigned Applicant prays that:

- a. This Return be noted and admitted; and
- b. The effectivity of _____ be extended for another ten (10) days from today, to give _____ ample time to process the preserve the computer data.

Other reliefs and remedies, just and equitable under the premises are likewise prayed for.

RESTRICTED

Done this _____ day of _____ at Camp
_____.

(Name of IOC)

Applicant

SUBSCRIBED AND SWORN to before me
this _____ of _____ at _____.

VERIFICATION

Republic of the Philippines)
_____) S.S.
X-----X

I, _____, applicant in this Warrant, under
oath, depose and say that:

I have caused the preparation of this Initial
Return/Compliance, read and signed the same; and all the
contents/allegations thereof are true and correct of my own
personal knowledge or based on authentic records.

(Name of IOC)

Applicant

SUBSCRIBED AND SWORN to before me this
_____ day of _____ at _____.

Administering Officer

Annex “R”

Republic of the Philippines
REGIONAL TRIAL COURT
Branch ____
____ Judicial Region
____ City

*RE: Application for a Warrant
to Disclose Computer
Data under Section 14 of Republic Act
No. 10175*

WDCD No.

(Name of IOC)

Representing the Philippine National
Police
Anti-Cybercrime Group
Regional Anti-Cybercrime Unit ____
Applicant,

X-----X

**COMPLIANCE/FINAL RETURN OF WARRANT TO
DISCLOSE COMPUTER DATA (WDCD)**

COMES NOW, the undersigned applicant,
_____, Investigator and presently assigned at the
PNP Anti-Cybercrime Group, Regional Anti-Cybercrime
Unit ____ (RACU ____) with office address at Camp
_____, most respectfully return unto this Honorable
Court the above-described Warrant to Disclose Computer
Data (WDCD) dated _____, with the following
information:

1. On _____, a Warrant to Disclose
Computer Data (WDCD) No. _____ was issued

by the Court signed by Honorable _____,
Presiding Judge, Regional Trial Court ____,
Branch ____, _____ City authorizing RACU ____
represented by the undersigned to issue an
order compelling _____ located at
_____ to disclose computer data
pertaining _____ Account No.
0999xxxxxxx, 0928xxxxxxx and 0906xxxxxxx.
A Copy of WDCD No. _____ is hereto attached
as “**Annex A**”;

2. Relative thereto, the undersigned received the
WDCD _____ on _____ and prepared the
Compliance Order dated _____ addressed
to _____ hereto attached as “**Annex
B**”;
3. On _____, at about _____, this unit
requested for assistance from Southern District
Anti-Cybercrime Team (SDACT) located at 2nd
Floor SPD Building Fort Bonifacio, Taguig City,
Metro Manila, Philippines to serve the
Compliance Order and was sent through their
email address pnnp.sdact@gmail.com the copy of
the Order and the _____;
4. On _____ at about _____ personnel of
SDACT implemented the said Order at _____ at
the address _____. On the same day, at
about _____, a hard copy of the order was sent
via JRS Express with tracking number _____
dated _____. *A copy of sent email, received
order by BDO and LBC Receipt are hereto
attached as Annexes “C”, “D”, and “E”,
respectively;*

5. On _____ at around _____, the undersigned made an Initial Return of the WDCD No. _____ with motion for extension of time to submit computer data. The said Initial Return was noted by the court, attached herein as Annex ____;
6. On _____ at around _____, _____, Legal Counsel of _____ forwarded to our Email their compliance to the Disclosure of Computer Data wherein it stated the information pertaining to the _____ Account no. 0999xxxxxxx, 0928xxxxxxx and 0906xxxxxxx. Attached is the compliance letter from _____ and the bank statement of the said account as **Annexes "G" and H"** respectively;
7. Further, the aforementioned disclosed computer data will be retained by the Applicant for purposes of case build-up/preliminary investigation which shall be kept strictly confidential and shall be labelled accordingly; and
8. In view of the foregoing, the undersigned would like to file this full and final Return, as Applicant of this Warrant and on behalf of the RACU __, PNP ACG, in compliance to Section 4.5 of the Supreme Court Rule on Cybercrime Warrant.

PRAYER

Premises considered; the undersigned Applicant prays that this Compliance/Final Return be admitted.

Other reliefs and remedies, just and equitable under the premises are likewise prayed for.

RESTRICTED

Done this ____ day of _____ at Camp
_____.

(Name of IOC)

Applicant

SUBSCRIBED AND SWORN to before me this
_____ day of _____ at _____.

VERIFICATION

REPUBLIC OF THE PHILIPPINES)
_____) S.S.
X-----X

I, _____, applicant in this Warrant,
under oath, depose and say that:

I have caused the preparation of this Final
Return/Compliance, read and signed the same; and all the
contents/allegations thereof are true and correct of my own
personal knowledge or based on authentic records.

(Name of IOC)

Applicant

SUBSCRIBED AND SWORN to before me this
_____ day of _____ at _____.

REFERENCES

RA No. 10175 (Cybercrime Prevention Act of 2012)

IRR of RA No. 10175

Rule on Cybercrime Warrants

Rules on the Use of Body-Worn Cameras in the Execution of Warrants

Philippine National Police Manual (PNPM-DO-D-0-2-13-21)
[Revised POP 2021]

Philippine National Police Manual (PNP-DIDM-DS-9-1)
[Criminal Investigation Manual Revised 2011]

Case Digest: DISINI vs. SECRETARY OF JUSTICE
(Discussed the Constitutionality of the Provisions of RA 10175)

PNP MC No. 2021-141 (Guidelines and Procedures in Reporting, Recording, Monitoring, and Disposition of Cybercrime and Cyber-related Incidents)

PNP ACG AOM Requirements on the Conduct of Digital Forensic Examination

TECHNICAL WORKING GROUP

PCOL VILLAMOR Q TULIAO (DDO, ACG)
Chairman

PCOL VINA H GUZMAN (CS, ACG)
Vice-Chairman

Members

PCOL REYNALDO SG DELA CRUZ
(C, ARMD)

PCOL DOMINGO S SORIANO
(C, OMD)

PCOL ALEJANDREA G SILVIO
(C, ID)

PCOL NOVA G DE CASTRO-AGLIPAY
(C, LAD)

PCOL RHODORA D MAYLAS
(C, WCCPU)

PCOL IRENE C CENA
(C, DFU)

PCOL FERDINAND S RAYMUNDO
(C, CSU)

PLTCOL DEODENNIS JOY E MARMOL
(AC, CPIU)

RESTRICTED

PLTCOL JAY D GUILLERMO
(AC, CRU)

PLTCOL ROBERT D BONGAYON JR
(OIC, CFCU)

TWG Secretariat

PCPT JULIUS VINCENT T LIBANG
Head Secretariat

TWG Members

PCpl Esteban E Belarmino
Case Monitoring PNCO, ID

Pat John Paulo S Manganti
Investigation PNCO, ID

Pat Marc Christian A Del Rosario
Legal Research PNCO, LAD

PNP ACG HOTLINE NUMBERS

PNP ACG Complaint Center Local 7491

PNP ACG TOC Local 7483

Regional Anti-Cybercrime Units (RACU)

RACU 1 09498819643

RACU 2 09551888421

RACU 3 09985988102

RACU 4A 09985988103

RACU 4B 09988558382

RACU 5 09985988104

RACU 6 09209702647

RACU 7 09985988105

RACU 8 09985716064

RACU 9 09985988106

RACU 10 09985988107

RACU 11 09985988108

RACU 12 09985988109

RESTRICTED

RACU 13	09088144981
RACU BAR	09989761930
RACU COR	09088180211

District Anti-Cybercrime Teams

QCDACT	09664000073
MDACT	09959732432
EDACT	09974197214
NDACT	09255128074
SDACT	09563440075



Published by:
Anti-Cybercrime Group
Philippine National Police
2023