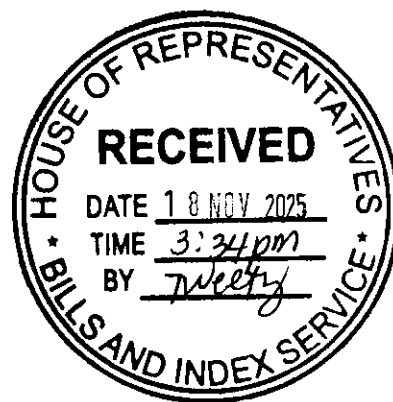




Republic of the Philippines  
**House of Representatives**  
Quezon City, Metro Manila

**TWENTIETH CONGRESS**  
First Regular Session

**HOUSE BILL NO. 6142**



---

Introduced by **REPRESENTATIVE CHEENO MIGUEL D. ALMARIO**

---

**EXPLANATORY NOTE**

The recent crisis brought about the Philippine Offshore Gaming Operators costed the Philippines P99.52 billion a year. In addition, the country also suffered unquantifiable losses such as human rights abuses of both domestic and foreign workers, the worsening of image of the Philippines in international community, and the addiction of local players to online gaming. One of the lessons we learned from this problem was that the Philippines was not prepared to tackle the ever evolving cybercrimes.

This measure seeks to make the government more proactive instead of being reactive. The additional legal power being given to the Philippine National Police and the National Bureau of Investigation will allow the government to tackle future problems in the field of cybercrime. Given how important it is to keep our laws updated to fight crimes which evolved with technology, this bill shall be seen as a priority.

Hence, the passage of this bill is earnestly sought.

  
**CHEENO MIGUEL D. ALMARIO**  
*Representative*  
2<sup>nd</sup> District, Davao Oriental



Republic of the Philippines  
**House of Representatives**  
Quezon City, Metro Manila

**TWENTIETH CONGRESS**  
First Regular Session

**HOUSE BILL NO. 6142**

---

Introduced by **REPRESENTATIVE CHEENO MIGUEL D. ALMARIO**

---

**AN ACT AMENDING REPUBLIC ACT NO. 10175 OTHERWISE KNOWN AS  
THE "CYBERCRIME PREVENTION ACT OF 2012", APPROPRIATING FUNDS  
THEREFOR, AND FOR OTHER PURPOSES**

*Be it enacted by the Senate and the House of Representatives of the Philippines in  
Congress assembled:*

**Section 1.** Section 3 of Republic Act No. 10175 is hereby amended to read as follows:

"Section 3. Definition of Terms. – xxx

(n) Service provider refers, BUT NOT LIMITED, TO THE  
FOLLOWING:

- (1) xxx
- (2) xxx
- (3) **PAYMENT SYSTEM PROVIDER (PSP) OR AN ENTITY  
ENGAGED IN ANY MONETARY TRANSACTION WHICH  
INCLUDES BANKS, FIAT OR DIGITAL MONEY SERVICE  
BUSINESSES INCLUDING CRYPTOCURRENCIES, CREDIT  
CARD COMPANIES, AND OTHER FINANCIAL  
INSTITUTIONS; AND**
- (4) **INTERNET INTERMEDIARIES AND INTERNET SERVICE  
PROVIDER AS DEFINED IN THIS ACT.**

(p) *Traffic data* or *non-content data* refers to any computer data other than the content of the communication including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

(q) INTERNET INTERMEDIARIES REFER TO PERSONS OR ENTITIES THAT PROVIDE INFRASTRUCTURE, PLATFORMS, ACCESS TO, AND HOST, TRANSMIT AND INDEX CONTENT, PRODUCTS AND SERVICES ORIGINATED BY THIRD PARTIES ON THE INTERNET. THESE INCLUDE, AMONG OTHERS:

- (1) INTERNET SERVICE PROVIDERS;
- (2) WEB HOSTING PROVIDERS INCLUDING DOMAIN NAME REGISTRARS;
- (3) INTERNET SEARCH ENGINES AND PORTALS;
- (4) E-COMMERCE INTERMEDIARIES;
- (5) INTERNET PAYMENT SYSTEM PROVIDERS; AND
- (6) PARTICIPATIVE NETWORK PLATFORM PROVIDERS INCLUDING SOCIAL MEDIA INTERMEDIARIES.

(r) INTERNET SERVICE PROVIDER (ISP) REFERS TO A PUBLIC TELECOMMUNICATION ENTITY (PTE) OR VALUE-ADDED SERVICE (VAS) PROVIDER DULY AUTHORIZED BY OR REGISTERED WITH THE NATIONAL TELECOMMUNICATIONS COMMISSION (NTC) THAT PROVIDES USERS OR OTHER ENTITIES WITH DATA CONNECTION ALLOWING ACCESS TO THE INTERNET THROUGH PHYSICAL TRANSPORT INFRASTRUCTURE OR **SATELLITE INTERNET PROVIDERS**, AND SUCH ACCESS IS NECESSARY FOR INTERNET USERS TO ACCESS CONTENT AND SERVICES ON THE INTERNET, AND FOR CONTENT PROVIDERS TO PUBLISH OR DISTRIBUTE MATERIALS ONLINE.

(s) CORE CYBERCRIMES REFER TO THE SPECIFIC OFFENSES ENUMERATED UNDER SECTION 4 OF R.A. NO. 10175.

(u) CYBER-RELATED/CYBER-ENABLED CRIME REFER TO 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.

(v) LAW ENFORCEMENT AUTHORITIES REFER TO THE PNP AND NBI.

(w) OTHER LAW ENFORCEMENT AGENCIES REFER TO LAW ENFORCEMENT AGENCIES, OTHER THAN THE PNP AND NBI, THAT ARE VESTED BY LAW WITH THE AUTHORITY TO INVESTIGATE, ENFORCE, OR PROSECUTE SPECIFIC VIOLATIONS OF LAW, AND WHICH MAY, IN CONNECTION WITH SUCH AUTHORITY, ISSUE PRESERVATION ORDERS AND APPLY FOR CYBERCRIME WARRANTS IN ACCORDANCE WITH THEIR RESPECTIVE MANDATES.

**Section 2.** Section 4 of the same Act is hereby amended to read as follows:

“Section 4. Cybercrime Offenses. – Xxx

(a) xxx

(1) Illegal Access. – The access to the whole or any part of a COMPUTER, ~~OR~~ computer system, OR ACCOUNT, WHETHER ONLINE OR OFFLINE, without right.

xxx

(5) Misuse of Devices.

(i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

(aa) A device OR ANY HARDWARE COMPONENT SUCH AS ANY ELECTRONIC GADGET OR EQUIPMENT, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or

(bb) A computer password, **EMAIL PASSWORD**<sup>1</sup> access code, APPLICATION, MALWARE or similar data, or ANY HARDWARE COMPONENT SUCH AS ANY ELECTRONIC GADGET OR EQUIPMENT by which the whole or any part of a computer system is capable of being accessed with **THE** intent that it be used for the purpose of committing any of the offenses under this Act.

(ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above USED IN, OR with intent to use said devices for the purpose of, committing any of the offenses under this section."

THERE IS PRESUMPTION AND PRIMA FACIE EVIDENCE OF INTENT TO USE SAID DEVICES BY MERE POSSESSION, CONTROL OR CUSTODY BY A NATURAL PERSON OR JURIDICAL PERSON WHOSE BUSINESS OR EMPLOYMENT DOES NOT LAWFULLY DEAL WITH THE USE, PRODUCTION, MANUFACTURE, PROCUREMENT, IMPORTATION, OR DISTRIBUTION THEREOF OR NOT IN THE ORDINARY COURSE OF THE POSSESSOR'S TRADE OR BUSINESS.

(c) xxxx

- (1) CYBERSEX. — ANY PERSON OR ENTITY WHO WILLFULLY ENGAGE, PROMOTE, SOLICIT, MAINTAIN, CONTROL, OR OPERATE, DIRECTLY OR INDIRECTLY, OF ANY LASCIVIOUS EXHIBITION OF SEXUAL ORGANS OR SEXUAL ACTIVITY, WITH THE AID OF A COMPUTER SYSTEM, OR THROUGH THE USE SOCIAL MEDIA PLATFORMS, OR ANY OTHER SOFTWARE, TOOLS, OR PROGRAMS, EITHER FOR FAVOR OR CONSIDERATION SHALL BE LIABLE FOR CYBERSEX. IT SHALL INCLUDE INTERACTIVE PROSTITUTION AND PORNOGRAPHY SUCH AS LIVE SHOWS OR INTERACTIVE METHODS WITH THE GOAL OF SEXUAL AROUSAL, CONSTITUTING OBSCENITY AND INDECENCY.

PROVIDED, THAT THE TESTIMONY OF THE CYBERSEX' CLIENTS SHALL NOT BE A PRE-REQUISITE FOR THE PROSECUTION OF THE CASE AND PROOF OF PAYMENT/S FOR THE CYBERSEX SERVICES MAY BE DETERMINED

DURING THE CONDUCT OF DIGITAL FORENSIC EXAMINATION BY LAW ENFORCEMENT AUTHORITIES.

PROVIDED FURTHER, THAT THE OWNER OF THE PROPERTY OR ESTABLISHMENT WHERE THE CYBERSEX ACTIVITY IS CONDUCTED SHALL BE LIABLE FOR AIDING OR ABETTING THE COMMISSION OF CYBERCRIME AND SHALL BE PUNISHABLE UNDER THIS ACT.

**Section 3.** A NEW SECTION IS HEREBY INSERTED TO READ AS FOLLOWS:

***“SECTION 8-A. - CONFISCATION AND FORFEITURE OF THE PROCEEDS AND INSTRUMENTS DERIVED FROM CYBERCRIME OR CYBER-RELATED OFFENSES. – IN ADDITION TO THE PENALTY IMPOSED FOR THE VIOLATION OF THIS ACT, THE COURT SHALL ORDER THE CONFISCATION AND FORFEITURE, OF ALL THE PROCEEDS AND PROPERTIES DERIVED FROM THE COMMISSION OF THE CRIME, IN FAVOR OF THE GOVERNMENT TO BE INCLUDED IN THE TRUST FUND CREATED UNDER THIS ACT, UNLESS THEY ARE THE PROPERTY OF A THIRD PERSON NOT LIABLE FOR THE UNLAWFUL ACT; PROVIDED, HOWEVER, THAT ALL AWARDS FOR DAMAGES SHALL BE TAKEN FROM THE PERSONAL AND SEPARATE PROPERTIES OF THE OFFENDER; PROVIDED, FURTHER, THAT IF SUCH PROPERTIES ARE INSUFFICIENT, THE BALANCE SHALL BE TAKEN FROM THE CONFISCATED AND FORFEITED PROPERTIES.***

WHEN THE PROCEEDS, PROPERTIES AND INSTRUMENTS OF THE OFFENSE HAVE BEEN DESTROYED, DIMINISHED IN VALUE OR OTHERWISE RENDERED WORTHLESS BY ANY ACT OR OMISSION, DIRECTLY OR INDIRECTLY, OF THE OFFENDER, OR IT HAS BEEN CONCEALED, REMOVED, CONVERTED OR TRANSFERRED TO PREVENT THE SAME FROM BEING FOUND OR TO AVOID FORFEITURE OR CONFISCATION, THE OFFENDER SHALL BE ORDERED TO PAY THE AMOUNT EQUAL TO THE VALUE OF THE PROCEEDS, PROPERTY OR INSTRUMENTS OF THE OFFENSE.”

**Section 4.** Section 9 of the same Act is hereby amended to read as follows:

**"Section 9. Corporate Liability.** — When any of the punishable acts herein defined, INCLUDING CYBER-RELATED/ICT-ENABLED OFFENSES, are ~~knowingly~~ committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on: (a) a power of representation of the juridical person provided the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person: *Provided*, That the act committed falls within the scope of such authority; or (c) an authority to exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten million pesos (PhP10,000,000.00)."

xxx

**Section 5.** A NEW SECTION IS HEREBY INSERTED TO READ AS FOLLOWS:

**"SECTION 8-B. - TRUST FUND.** - ALL FINES IMPOSED UNDER THIS ACT AND THE PROCEEDS AND PROPERTIES FORFEITED AND CONFISCATED PURSUANT TO SECTION 9-A HEREOF, AS WELL AS THOSE COLLECTED BY THE AMLC, SHALL ACCRUE TO A TRUST FUND TO BE ADMINISTERED AND MANAGED BY THE CICC EXECUTIVE COMMITTEE TO BE USED EXCLUSIVELY FOR ANTI-CYBERCRIME PROGRAMS AND UPGRADING OF CAPABILITIES OF THE PNP ACG AND NBI CCD."

**Section 6.** Section 10 of the same Act is hereby amended to read as follows:

**"Section 10. Law Enforcement Authorities.** — The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act. FURTHER, SAID CYBERCRIME UNITS ARE AUTHORIZED TO STRENGTHEN AND UPGRADE THEIR ORGANIZATIONAL STRUCTURE AND STAFFING PATTERNS TO ADDRESS THE COMPLEXITY AND CHALLENGES ON CYBERCRIME INVESTIGATION.

THE PNP ANTI-CYBERCRIME GROUP CREATED BY VIRTUE OF THIS ACT SHALL BE HEADED BY A DIRECTOR WITH THE RANK OF POLICE MAJOR GENERAL. THE DIRECTOR SHALL BE ASSISTED BY A COMMAND GROUP COMPOSED OF A DEPUTY DIRECTOR FOR ADMINISTRATION AND DEPUTY DIRECTOR FOR OPERATIONS, BOTH WITH THE RANK OF POLICE BRIGADIER GENERAL, AND A CHIEF OF STAFF WITH THE RANK OF POLICE COLONEL.

**Section 7.** A NEW SECTION 10-A IS HEREBY INSERTED TO READ AS FOLLOWS:

**SECTION 10-A. AUTHORITY OF OTHER UNITS OF THE PNP AND NBI AND OTHER LAW ENFORCEMENT AGENCIES.** — OTHER UNITS OF THE PNP AND NBI SHALL HAVE THE AUTHORITY TO INVESTIGATE CYBER-RELATED OFFENSES, ISSUE PRESERVATION ORDERS, AND APPLY FOR CYBERCRIME WARRANTS IN RELATION TO THEIR INVESTIGATION.

LIKewise, OTHER LAW ENFORCEMENT AGENCIES SHALL HAVE THE AUTHORITY TO ISSUE PRESERVATION ORDERS, APPLY FOR CYBERCRIME WARRANTS AND TO CONDUCT DIGITAL FORENSIC EXAMINATION, PROVIDED THAT SUCH AUTHORITY IS EXERCISED IN RELATION TO OFFENSES FALLING WITHIN THE MANDATE OF THE RESPECTIVE AGENCY UNDER EXISTING LAWS.

**Section 8.** Section 11 of the same Act is hereby amended to read as follows:

**“Section 11. Duties, POWERS, AND FUNCTIONS of Law Enforcement Authorities.** — To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to submit ~~timely and regular~~ reports ~~including pre-operation, post-operation and investigation results and such other documents~~ as may be required to the Department of Justice (DOJ) for review and monitoring.

THE PNP ANTI-CYBERCRIME GROUP AND THE NBI CYBERCRIME DIVISION SHALL HAVE THE FOLLOWING

POWERS

AND

FUNCTIONS:

- a. INVESTIGATE ALL CYBERCRIMES AND CYBER-RELATED CRIMES;
- b. CONDUCT DATA RECOVERY AND FORENSIC ANALYSIS ON COMPUTERS, COMPUTER SYSTEMS AND OTHER ELECTRONIC DEVICES IN RELATION TO A CRIMINAL INVESTIGATION;
- c. PROVIDE TECHNICAL AND INVESTIGATIVE ASSISTANCE TO OTHER INVESTIGATING UNITS WITHIN THE PNP AND NBI TO INCLUDE REFERRALS FROM OTHER GOVERNMENT AGENCIES FOR PURPOSES OF CRIMINAL INVESTIGATION;
- d. **ORDER THE TEMPORARY HOLDING OF FUNDS, CRYPTOCURRENCY AND OTHER VIRTUAL ASSETS SUBJECT OF AN INVESTIGATION WITHIN A PERIOD NOT EXCEEDING THIRTY (30) CALENDAR DAYS, UNLESS OTHERWISE EXTENDED BY A COURT OF COMPETENT JURISDICTION;**
- e. FORMULATE GUIDELINES IN INVESTIGATION, FORENSIC EVIDENCE RECOVERY, AND FORENSIC DATA ANALYSIS CONSISTENT WITH INDUSTRY STANDARD PRACTICES;
- f. DEVELOP PUBLIC, PRIVATE SECTOR, AND LAW ENFORCEMENT AGENCY RELATIONS IN ADDRESSING CYBERCRIMES;
- g. MAINTAIN NECESSARY AND RELEVANT DATABASES FOR STATISTICAL AND/OR MONITORING PURPOSES;
- h. DEVELOP CAPACITY WITHIN THEIR ORGANIZATIONS IN ORDER TO PERFORM SUCH DUTIES NECESSARY FOR THE ENFORCEMENT OF ANTI-CYBERCRIME LAWS;
- i. SUPPORT THE FORMULATION AND ENFORCEMENT OF THE NATIONAL CYBERSECURITY PLAN; AND
- j. PERFORM OTHER FUNCTIONS AS MAY BE REQUIRED BY LAW.

MOREOVER, THE HEADS OF THE NBI AND PNP CYBERCRIME UNITS SHALL HAVE THE POWER TO ADMINISTER OATH, AND ISSUE *SUBPOENA* AND *SUBPOENA DUCES TECUM* IN RELATION TO ITS INVESTIGATION. THE *SUBPOENA* SHALL STATE THE NATURE AND PURPOSE OF INVESTIGATION, SHALL BE DIRECTED TO THE PERSON OR SERVICE PROVIDER WHOSE ATTENDANCE IS

REQUIRED, AND IN THE CASE OF A *SUBPOENA DUCES TECUM*, IT SHALL ALSO CONTAIN A REASONABLE DESCRIPTION OF THE BOOKS, DOCUMENTS, OR THINGS DEMANDED WHICH MUST BE RELEVANT TO THE INVESTIGATION.

FAILURE TO COMPLY WITH *SUBPOENA* AND *SUBPOENA DUCES TECUM* SHALL AUTHORIZE THE FILING OF A CASE FOR INDIRECT CONTEMPT UNDER THE RULES OF COURT WITH THE REGIONAL TRIAL COURT AND OBSTRUCTION OF JUSTICE UNDER SEC. 20 OF THIS ACT."

RECOGNIZING THE TRANSNATIONAL NATURE OF CYBERCRIME, THE PNP AND NBI SHALL ENDEAVOR TO ESTABLISH COOPERATION ARRANGEMENTS WITH FOREIGN LAW ENFORCEMENT AGENCIES FOR FASTER EXCHANGE OF INFORMATION, BEST PRACTICES, AND JOINT INVESTIGATIONS OF CYBERCRIMES.

**Section 9.** A NEW SECTION IS INSERTED TO READ AS FOLLOWS:

**SECTION \_\_. FILING A COMPLAINT** <sup>1</sup>  
NOTWITHSTANDING ANY EXISTING LAWS AND PROCEDURES, IN VIEW OF THE NATURE OF CYBERCRIME, COMPLAINTS ON ANY OFFENSE PUNISHABLE UNDER THIS ACT MAY BE FILED BY THE FOLLOWING:

- (1) PRIVATE COMPLAINANT WHICH INCLUDES ALL THE SERVICE PROVIDERS AS DEFINED IN SECTION 3(N) AS AMENDED INCLUDING THOSE PROVIDING BUSINESS PROCESS OUTSOURCING AND SIMILAR SERVICES. FILING MADE UNDER THIS SUBSECTION (1) SHALL NOT REQUIRE ANY PREREQUISITE ACTION INCLUDING THAT THE SAME BE PRECEDED BY A REPORT FILED WITH A LAW ENFORCEMENT AGENCY<sup>2</sup>; OR
- (2) ANY LAW ENFORCEMENT OFFICER IN CASES WHERE THE PRIVATE COMPLAINANT IS LOCATED OUTSIDE THE

---

<sup>1</sup> Inputs from IBPAP

<sup>2</sup> Inputs from IBPAP

PHILIPPINES AND IS UNABLE TO APPEAR BEFORE THE PROSECUTOR'S OFFICE OR THE COURT."

**Section 10.** Section 14 of Republic Act No. 10175 is hereby amended to read as follows:

**"Section 14. *Disclosure of Computer Data.*** — Law enforcement authorities, THROUGH A SUBPOENA OR upon securing a court warrant, shall issue an order requiring any person or service provider, **OR ANY SOCIAL MEDIA PLATFORMS, MESSAGING CHANNELS, OR WEBSITES<sup>3</sup>**, to disclose or submit subscriber's information, traffic data, CONTENT DATA, or any relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation BEFORE THE LAW ENFORCEMENT AGENCY and the disclosure is necessary and relevant for the purpose of investigation.

FOR PURPOSES OF THIS ACT AND NOTWITHSTANDING THE PROVISIONS OF REPUBLIC ACT NO. 1405, OTHERWISE KNOWN AS THE "BANK SECRECY LAW", AS AMENDED; REPUBLIC ACT NO. 6426, OTHERWISE KNOWN AS THE "FOREIGN CURRENCY DEPOSIT ACT OF THE PHILIPPINES", AS AMENDED; REPUBLIC ACT NO. 8791, OTHERWISE KNOWN AS "THE GENERAL BANKING LAW OF 2000" AND OTHER LAWS, THE NBI AND PNP CYBERCRIME UNITS ARE HEREBY AUTHORIZED TO REQUIRE THROUGH A SUBPOENA OR COURT ORDER VALIDLY ISSUED IN ACCORDANCE WITH THIS SECTION, ANY BANKING INSTITUTION OR NON-BANK FINANCIAL INSTITUTION AND THEIR SUBSIDIARIES AND AFFILIATES, FINANCIAL INTERMEDIARIES, INTERNET PAYMENT SYSTEM PROVIDERS (PSP), PAYMENT SERVICE PROVIDERS, AND OTHER FINANCIAL FACILITATORS, THE DISCLOSURE OF BANK ACCOUNT OWNER'S INFORMATION SUCH AS NAME, HOME/DELIVERY ADDRESS, EMAIL ADDRESS, MOBILE OR OTHER CONTACT DETAILS WHEN IT HAS BEEN ESTABLISHED THAT THERE IS REASONABLE GROUND TO BELIEVE THAT THE DEPOSIT OR INVESTMENT ARE RECIPIENTS OF OR USED

---

<sup>3</sup> Inputs from IBPAP

IN THE COMMISSION OF CYBERCRIMES OR CYBER-RELATED OFFENSES.”

**Section 11.** Section 16 of the same Act is hereby amended to read as follows:

**“Section 16. Custody of Computer Data.** — All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data. ~~The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made.~~ PROVIDED THAT, LAW ENFORCEMENT AUTHORITIES ARE AUTHORIZED TO RETAIN AND USE A COPY OF THE COMPUTER DATA AS EVIDENCE FOR PURPOSES OF FILING A COMPLAINT BEFORE THE PROSECUTOR’S OFFICE OR DURING THE PENDENCY OF A CASE BEFORE THE COURT AND FOR RECORD KEEPING WHICH SHALL BE CONSIDERED CONFIDENTIAL IN NATURE.

~~The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or then contents revealed, except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.”~~

**Section 12.** Section 19 of the same Act is hereby reinstated to read as follows:

**“Restricting or Blocking Access to Computer Data.** — When a computer data is prima facie found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data. ”

**Section 13.** Section 20 of the same Act is hereby amended to read as follows:

**“Section 20. Noncompliance.** — Failure OF A SERVICE PROVIDER 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 correctional* in its maximum period or a fine of ~~One hundred thousand pesos (PHP100,000.00)~~ ONE MILLION PESOS (PHP1,000,000.00) or both, for each and every noncompliance with an order issued by law enforcement authorities WITHOUT PREJUDICE TO THE PROVISIONS OF PRESIDENTIAL DECREE NO. 1829."

**Section 14. A NEW SECTION IS INSERTED TO READ AS FOLLOWS:**

**"SECTION 24-A. - CREATION OF THE ANTI-SCAM HUB. -** WITHIN SIX (6) MONTHS AFTER THE EFFECTIVITY OF THIS ACT, THE ANTI-SCAM HUB, HEREINAFTER REFERRED TO AS THE "ASH", SHALL BE CREATED UNDER THE CONTROL AND SUPERVISION OF THE CYBERCRIME INVESTIGATION AND COORDINATING CENTER (CICC) EXECUTIVE COMMITTEE TO CENTRALIZE INVESTIGATIONS OF SCAM-RELATED CRIMES, DISRUPT SCAMMERS' OPERATIONS, AND HELP MITIGATE VICTIMS' LOSSES.

THE ASH SHALL BE A COLLABORATION BETWEEN THE LAW ENFORCEMENT AGENCIES, OTHER GOVERNMENT AGENCIES (DTI, BSP, NTC, NPC, ETC.) CONCERNED, BANKS, TELECOMMUNICATION COMPANIES, ONLINE MARKETPLACES, FINANCIAL TECHNOLOGY COMPANIES, OPERATORS OF PAYMENT SYSTEMS, AMONG OTHERS.

THE COMPOSITION, FUNCTIONS, AND MECHANISM ON HOW THE ASH WILL WORK SHALL BE LAID DOWN IN THE IMPLEMENTING RULES AND REGULATIONS.

**Section 15. Section 27 of Republic Act No. 10175 is hereby amended to read as follows:**

**"Section 27. Appropriations.** The amount of Fifty million pesos (PhP50,000,000.00) shall be appropriated annually for the implementation of this Act.

MOREOVER, THE CAPABILITY AND CAPACITY ENHANCEMENT FOR THE PNP ANTI-CYBERCRIME GROUP AND NBI CYBERCRIME DIVISION SHALL BE

INCLUDED IN THE ANNUAL GENERAL APPROPRIATIONS ACT.

PROVIDED FURTHER THAT, THE AMOUNT NECESSARY TO CREATE THE ANTI-SCAM HUB SHALL BE CHARGED AGAINST THE CURRENT YEAR'S APPROPRIATIONS OF THE AGENCIES CONCERNED. IN ADDITION, THE AMOUNT OF ONE HUNDRED MILLION PESOS (PHP100,000,000.00) AS INITIAL FUNDING FOR THE ANTI-SCAM HUB TO BE CHARGED AGAINST THE UNEXPENDED CONTINGENCY FUND OF THE OFFICE OF THE PRESIDENT IS HEREBY APPROPRIATED. THEREAFTER, THE AMOUNT NEEDED FOR THE IMPLEMENTATION OF THE HUB SHALL BE INCLUDED IN THE ANNUAL GENERAL APPROPRIATIONS ACT"

**Section 16. Implementing Rules and Regulations.** The Department of Justice and the Department of Information and Communication Technology, Cybercrime Investigation and Coordinating Center, Philippine National Police, and the National Bureau of Investigation shall jointly formulate the necessary rules and regulations within ninety (90) days from the approval of this Act for its effective implementation.

**Section 17. Separability Clause.** The declaration of invalidity of any provision of this Act or part thereof shall not affect the validity of the remaining provisions.

**Section 18. Repealing Clause.** All laws, decrees, executive orders, proclamations, rules and regulations, and issuances or parts thereof which are inconsistent with the provisions of the Act are hereby repealed or modified accordingly.

**Section 19. Effectivity.** This Act shall take effect after fifteen (15) days following its complete publication in the Official Gazette.

*Approved,*