



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

Twentieth Congress
Second Regular Session

HOUSE BILL NO. **10905**



Introduced by **REPRESENTATIVE KATRINA REIKO CHUA - TAI**

EXPLANATORY NOTE

The rapid development and widespread use of information and communications technologies have changed how Filipinos communicate, conduct business, access financial services, and transact daily. However, these advances have also created new opportunities for criminal activities. Cybercrime has become more prevalent, sophisticated, organized, and transnational, posing a serious and ongoing threat to the security, privacy, property, and welfare of every Filipino people.

Since the enactment of **Republic Act No. 10175**, known as the *“Cybercrime Prevention Act of 2012,”* the cyber threat landscape has evolved significantly. Criminals now exploit social media platforms, messaging applications, online marketplaces, electronic payment systems, digital banking, cryptocurrencies, virtual assets, and other internet-based technologies to commit fraud, unauthorized access, identity theft, online sexual exploitation, financial crimes, and other cyber-enabled offenses. Online scams, in particular, have become widespread, causing major financial losses and harm to individuals, businesses, and institutions.

The increasing sophistication of cybercriminal activities has exposed the need to strengthen investigative, enforcement, and asset-recovery mechanisms. Criminal proceeds can be transferred through multiple accounts, payment platforms, digital wallets, and virtual assets quickly, making timely access to information and the preservation and recovery of illicit proceeds essential for effective law enforcement. At the same time, the growing involvement of internet intermediaries, telecommunications entities, financial institutions, payment system providers, and digital services in the digital ecosystem requires clearer responsibilities and stronger cooperation with law enforcement authorities.

This proposed measure seeks to amend Republic Act No. 10175 to strengthen the country's legal and institutional framework against cybercrime and cyber-related or cyber-enabled offenses. It expands and clarifies relevant definitions, strengthens provisions on the misuse of devices and cybersex, establishes corporate liability where warranted, and provides mechanisms for the confiscation and forfeiture of proceeds and instruments derived from cybercrime. It also strengthens the investigative and digital forensic capabilities of the Philippine National Police Anti-Cybercrime Group and the National Bureau of Investigation Cybercrime Division, while granting appropriate authority to other law enforcement agencies within their mandates.

The measure further strengthens lawful mechanisms for obtaining computer, subscriber, traffic, content, and financial information relevant to cybercrime investigations. It provides for the temporary holding of funds, cryptocurrencies, and other virtual assets under investigation, subject to legal and judicial safeguards. It also enhances compliance with lawful investigative orders and offers mechanisms for the proper preservation, custody, and use of electronic evidence. This facilitates effective investigation and prosecution of cybercrime while maintaining the integrity and confidentiality of such evidence.

Considering the unprecedented growth of online scams, the bill provides for the creation of an Anti-Scam Hub under the supervision of the Cybercrime Investigation and Coordinating Center. The Anti-Scam Hub will serve as a coordinated mechanism among law enforcement agencies, government agencies, financial institutions, telecommunications companies, online marketplaces, financial technology companies, payment system operators, and other stakeholders. It will facilitate prompt investigation and disruption of scam operations, trace and recover illicit proceeds, and mitigate losses suffered by victims.

The proposed amendments recognize the transnational nature of cybercrime and the need for stronger cooperation between Philippine law enforcement and their foreign counterparts. Effective enforcement requires timely information sharing, coordinated investigations, technological capability, specialized personnel, and sustained investment in digital forensic and investigative resources. Accordingly, the measure provides augmented funding and training for the country's main cybercrime enforcement units and programs.

The State bears a solemn duty to protect its citizens and institutions from criminal activities that exploit modern technology. The proposed measure strengthens the powers and capabilities of law enforcement authorities while requiring them to exercise such powers in accordance with the Constitution, existing laws, judicial procedures, and fundamental rights. It seeks to enable law enforcement authorities to respond swiftly and effectively to rapidly evolving cyber threats while upholding the rule of law and protecting due process.

Cybercrime is no longer an emerging concern but an immediate and expanding threat to public safety, financial security, and confidence in the country's digital economy. The increasing frequency, scale, and advancement of cyberattacks, online scams, and other cyber-enabled offenses show the urgent need to update the legal framework and equip authorities with effective, modern, and coordinated tools for prevention, investigation, prosecution, and asset recovery.

For these reasons, the immediate passage of this measure is earnestly sought. It is imperative that Philippine law keep pace with technological developments and that the State be properly equipped to protect the Filipino people, their property, and the integrity of the country's digital and financial systems against the growing menace of cybercrime.

In view of the foregoing, the immediate passage of this bill is earnestly sought.



KATRINA REIKO CHUA-TAI



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

Twentieth Congress
Second Regular Session

HOUSE BILL NO. **10905**

Introduced by **REPRESENTATIVE KATRINA REIKO CHUA-TAI**

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 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**

1 CRYPTOCURRENCIES, CREDIT CARD COMPANIES, AND OTHER
2 FINANCIAL INSTITUTIONS; *AND*

3 (4) INTERNET INTERMEDIARIES AND INTERNET
4 SERVICE PROVIDER AS DEFINED IN THIS ACT.

5 xxx

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

- 11 1) INTERNET SERVICE PROVIDERS;
- 12 2) WEB HOSTING PROVIDERS INCLUDING DOMAIN NAME
13 REGISTRARS;
- 14 3) INTERNET SEARCH ENGINES AND PORTALS;
- 15 4) E-COMMERCE INTERMEDIARIES;
- 16 5) INTERNET PAYMENT SYSTEM PROVIDERS; AND
- 17 6) PARTICIPATIVE NETWORK PLATFORM PROVIDERS
18 INCLUDING SOCIAL MEDIA INTERMEDIARIES

19 (R) INTERNET SERVICE PROVIDER (ISP) REFERS TO A PUBLIC
20 TELECOMMUNICATION ENTITY (PTE) OR VALUE-ADDED
21 SERVICE (VAS) PROVIDER DULY AUTHORIZED BY OR
22 REGISTERED WITH THE NATIONAL TELECOMMUNICATIONS
23 COMMISSION (NTC) THAT PROVIDES USERS OR OTHER ENTITIES
24 WITH DATA CONNECTION ALLOWING ACCESS TO THE INTERNET

1 **THROUGH PHYSICAL TRANSPORT INFRASTRUCTURE OR**
2 **SATELLITE INTERNET PROVIDERS, AND SUCH ACCESS IS**
3 **NECESSARY FOR INTERNET USERS TO ACCESS CONTENT AND**
4 **SERVICES ON THE INTERNET, AND FOR CONTENT PROVIDERS TO**
5 **PUBLISH OR DISTRIBUTE MATERIALS ONLINE.**

6 **(S) CORE CYBERCRIMES REFER TO THE SPECIFIC OFFENSES**
7 **ENUMERATED UNDER SECTION 4 OF R.A. NO. 10175.**

8 **(T) CYBER-RELATED/CYBER-ENABLED CRIME REFER TO**
9 **CRIMES DEFINED AND PENALIZED BY THE REVISED PENAL CODE,**
10 **AS AMENDED, AND SPECIAL LAWS, IF COMMITTED BY, THROUGH**
11 **AND WITH THE USE OF INFORMATION AND COMMUNICATIONS**
12 **TECHNOLOGIES.**

13 **(U) LAW ENFORCEMENT AUTHORITIES REFER TO THE PNP**
14 **AND NBI.**

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

22
23 SEC. 2. Section 4 of the same Act is hereby amended to read as follows:
24 “Section 4. Cybercrime Offenses. – Xxx.

1 (a) Xxx.

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

5 Xxx.

6 (5) Misuse of Devices.

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

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

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

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

23 **THERE IS PRESUMPTION AND PRIMA FACIE EVIDENCE**
24 **OF INTENT TO USE SAID DEVICES BY MERE POSSESSION,**

1 CONTROL OR CUSTODY BY A NATURAL PERSON OR
2 JURIDICAL PERSON WHOSE BUSINESS OR EMPLOYMENT
3 DOES NOT LAWFULLY DEAL WITH THE USE, PRODUCTION,
4 MANUFACTURE, PROCUREMENT, IMPORTATION, OR
5 DISTRIBUTION THEREOF OR NOT IN THE ORDINARY COURSE
6 OF THE POSSESSOR’S TRADE OR BUSINESS.

7 (c) Xxx.

8 (1) CYBERSEX. — ~~The willful engagement, maintenance, control, or~~
9 ~~operation, directly or indirectly, of any lascivious exhibition of sexual organs or~~
10 ~~sexual activity, with the aid of a computer system, for favor or consideration~~ ANY
11 PERSON OR ENTITY WHO WILLFULLY ENGAGE, PROMOTE,
12 SOLICIT, MAINTAIN, CONTROL, OR OPERATE, DIRECTLY OR
13 INDIRECTLY, OF ANY LASCIVIOUS EXHIBITION OF SEXUAL ORGANS
14 OR SEXUAL ACTIVITY, WITH THE AID OF A COMPUTER SYSTEM, OR
15 THROUGH THE USE SOCIAL MEDIA PLATFORMS, OR ANY OTHER
16 SOFTWARE, TOOLS, OR PROGRAMS, EITHER FOR FAVOR OR
17 CONSIDERATION SHALL BE LIABLE FOR CYBERSEX. IT SHALL
18 INCLUDE INTERACTIVE PROSTITUTION AND PORNOGRAPHY SUCH
19 AS LIVE SHOWS OR INTERACTIVE METHODS WITH THE GOAL OF
20 SEXUAL AROUSAL, CONSTITUTING OBSCENITY AND
21 INDECENCY.

22 PROVIDED, THAT THE TESTIMONY OF THE CYBERSEX’
23 CLIENTS SHALL NOT BE A PRE-REQUISITE FOR THE PROSECUTION
24 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.

SEC. 3. 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

1 SEC. 4. Section 10 of the same Act is hereby amended to read as follows:

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

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

19
20 SEC. 5. Section 11 of the same Act shall be renumbered as Section 14 and a new
21 Section 11 is hereby inserted to read as follows:

22 **“SECTION 11. CONFISCATION AND FORFEITURE OF THE**
23 **PROCEEDS AND INSTRUMENTS DERIVED FROM CYBERCRIME OR**

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

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

SEC. 6. Section 11 of the same Act is renumbered as Section 14 and is hereby amended to read as follows:

“Section ~~11~~ **14. 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**

1 **OF AN INVESTIGATION WITHIN A PERIOD NOT EXCEEDING**
2 **THIRTY (30) CALENDAR DAYS, UNLESS OTHERWISE**
3 **EXTENDED BY A COURT OF COMPETENT JURISDICTION;**

4 **e. FORMULATE GUIDELINES IN INVESTIGATION, FORENSIC**
5 **EVIDENCE RECOVERY, AND FORENSIC DATA ANALYSIS**
6 **CONSISTENT WITH INDUSTRY STANDARD PRACTICES;**

7 **f. DEVELOP PUBLIC, PRIVATE SECTOR, AND LAW**
8 **ENFORCEMENT AGENCY RELATIONS IN ADDRESSING**
9 **CYBERCRIMES;**

10 **g. MAINTAIN NECESSARY AND RELEVANT DATABASES FOR**
11 **STATISTICAL AND/OR MONITORING PURPOSES;**

12 **h. DEVELOP CAPACITY WITHIN THEIR ORGANIZATIONS IN**
13 **ORDER TO PERFORM SUCH DUTIES NECESSARY FOR THE**
14 **ENFORCEMENT OF ANTI-CYBERCRIME LAWS;**

15 **i. SUPPORT THE FORMULATION AND ENFORCEMENT OF THE**
16 **NATIONAL CYBERSECURITY PLAN; AND**

17 **j. PERFORM OTHER FUNCTIONS AS MAY BE REQUIRED BY**
18 **LAW.**

19 **MOREOVER, THE HEADS OF THE NBI AND PNP CYBERCRIME UNITS**
20 **SHALL HAVE THE POWER TO ADMINISTER OATH, AND ISSUE SUBPOENA**
21 **AND SUBPOENA DUCES TECUM IN RELATION TO ITS INVESTIGATION.**
22 **THE SUBPOENA SHALL STATE THE NATURE AND PURPOSE OF**
23 **INVESTIGATION, SHALL BE DIRECTED TO THE PERSON OR SERVICE**

1 PROVIDER WHOSE ATTENDANCE IS REQUIRED, AND IN THE CASE OF A
2 SUBPOENA DUCES TECUM, IT SHALL ALSO CONTAIN A REASONABLE
3 DESCRIPTION OF THE BOOKS, DOCUMENTS, OR THINGS DEMANDED
4 WHICH MUST BE RELEVANT TO THE INVESTIGATION. FAILURE TO
5 COMPLY WITH SUBPOENA AND SUBPOENA DUCES TECUM SHALL
6 AUTHORIZE THE FILING OF A CASE FOR INDIRECT CONTEMPT UNDER
7 THE RULES OF COURT WITH THE REGIONAL TRIAL COURT AND
8 OBSTRUCTION OF JUSTICE UNDER SEC. 20 OF THIS ACT.”

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

14
15 SEC. 7. Section 12 of the same Act shall be renumbered as Section 15 and a new Section
16 12 is hereby inserted to read as follows:

17 “SECTION 12. AUTHORITY OF OTHER UNITS OF THE PNP AND NBI
18 AND OTHER LAW ENFORCEMENT AGENCIES. - OTHER UNITS OF THE PNP
19 AND NBI SHALL HAVE THE AUTHORITY TO INVESTIGATE CYBER-
20 RELATED OFFENSES ISSUE PRESERVATION ORDERS, AND
21 APPLY FOR CYBERCRIME WARRANTS IN RELATION TO
22 THEIR INVESTIGATION.

23 LIKEWISE, OTHER LAW ENFORCEMENT AGENCIES SHALL HAVE
24 THE AUTHORITY TO ISSUE PRESERVATION ORDERS, APPLY FOR
25 CYBERCRIME WARRANTS AND TO CONDUCT DIGITAL FORENSIC

1 **EXAMINATION, PROVIDED THAT SUCH AUTHORITY IS EXERCISED IN**
2 **RELATION TO OFFENSES FALLING WITHIN THE MANDATE OF THE**
3 **RESPECTIVE AGENCY UNDER EXISTING LAWS.”**

4
5 SEC. 8. Section 13 of the same Act shall be renumbered as Section 16 and A new Section
6 13 is hereby inserted to read as follows:

7 **“SECTION 13. TRUST FUND. – ALL FINES IMPOSED UNDER THIS ACT**
8 **AND THE PROCEEDS AND PROPERTIES FORFEITED AND CONFISCATED**
9 **PURSUANT TO SECTION 10 HEREOF, AS WELL AS THOSE COLLECTED BY**
10 **THE AMLC, SHALL ACCRUE TO A TRUST FUND TO BE ADMINISTERED AND**
11 **MANAGED BY THE CICC EXECUTIVE COMMITTEE TO BE USED**
12 **EXCLUSIVELY FOR ANTI-CYBERCRIME PROGRAMS AND UPGRADING OF**
13 **CAPABILITIES OF THE PNP ACG AND NBI CCD.”**

14 SEC. 9. Section 17 of the same Act shall be renumbered as Section 18 and a new Section
15 17 is hereby inserted to read as follows:

16 **“SECTION 17. FILING A COMPLAINT - NOTWITHSTANDING ANY**
17 **EXISTING LAWS AND PROCEDURES, IN VIEW OF THE NATURE OF**
18 **CYBERCRIME COMPLAINTS ON ANY OFFENSE PUNISHABLE**
19 **UNDER THIS ACT MAY BE FILED BY THE FOLLOWING:**

20 **(1) PRIVATE COMPLAINANT WHICH INCLUDES ALL THE SERVICE**
21 **PROVIDERS AS DEFINED IN SECTION 3(N) AS AMENDED INCLUDING**
22 **THOSE PROVIDING BUSINESS PROCESS OUTSOURCING AND**
23 **SIMILAR SERVICES. FILING MADE UNDER THIS SUBSECTION (1) SHALL**
24 **NOT REQUIRE ANY PREREQUISITE ACTION INCLUDING THAT THE SAME**

1 **BE PRECEDED BY A REPORT FILED WITH A LAW ENFORCEMENT AGENCY;**
2 **OR**

3 **(2) ANY LAW ENFORCEMENT OFFICER IN CASES WHERE THE**
4 **PRIVATE COMPLAINANT IS LOCATED OUTSIDE THE PHILIPPINES AND IS**
5 **UNABLE TO APPEAR BEFORE THE PROSECUTOR’S OFFICE OR THE**
6 **COURT.”**

7 SEC. 10. Section 14 of the same Act shall be renumbered as Section 19 and is hereby
8 amended to read as follows:

9 “Section 14 **19. Disclosure of Computer Data.** — Law enforcement authorities,
10 **THROUGH A SUBPOENA OR** upon securing a court warrant, shall issue an order
11 requiring any person or service provider, **OR ANY SOCIAL MEDIA PLATFORMS,**
12 **MESSAGING CHANNELS, OR WEBSITES,** to disclose or submit subscriber’s
13 information, traffic data, CONTENT DATA, or any relevant data in his/its possession or
14 control within seventy-two (72) hours from receipt of the order in relation to a valid
15 complaint officially docketed and assigned for investigation **BEFORE THE LAW**
16 **ENFORCEMENT AGENCY** and the disclosure is necessary and relevant for the purpose
17 of investigation.

18 **FOR PURPOSES OF THIS ACT AND NOTWITHSTANDING THE**
19 **PROVISIONS OF REPUBLIC ACT NO. 1405, OTHERWISE KNOWN AS THE**
20 **“BANK SECRECY LAW”, AS AMENDED; REPUBLIC ACT NO. 6426,**
21 **OTHERWISE KNOWN AS THE “FOREIGN CURRENCY DEPOSIT ACT OF THE**
22 **PHILIPPINES”, AS AMENDED; REPUBLIC ACT NO. 8791, OTHERWISE**
23 **KNOWN AS “THE GENERAL BANKING LAW OF 2000” AND OTHER LAWS,**
24 **THE NBI AND PNP CYBERCRIME UNITS ARE HEREBY AUTHORIZED TO**

1 **REQUIRE THROUGH A SUBPOENA OR COURT ORDER VALIDLY ISSUED IN**
2 **ACCORDANCE WITH THIS SECTION, ANY BANKING INSTITUTION OR**
3 **NON-BANK FINANCIAL INSTITUTION AND THEIR SUBSIDIARIES AND**
4 **AFFILIATES, FINANCIAL INTERMEDIARIES, INTERNET PAYMENT**
5 **SYSTEM PROVIDERS (PSP), PAYMENT SERVICE PROVIDERS, AND OTHER**
6 **FINANCIAL FACILITATORS, THE DISCLOSURE OF BANK ACCOUNT**
7 **OWNER’S INFORMATION SUCH AS NAME, HOME/DELIVERY ADDRESS,**
8 **EMAIL ADDRESS, MOBILE OR OTHER CONTACT DETAILS WHEN IT HAS**
9 **BEEEN ESTABLISHED THAT THERE IS REASONABLE GROUND TO BELIEVE**
10 **THAT THE DEPOSIT OR INVESTMENT ARE RECIPIENTS OF OR USED IN**
11 **THE COMMISSION OF CYBERCRIMES OR CYBER-RELATED OFFENSES.”**

12 SEC. 11. Section 16 of the same Act shall be renumbered as Section 20 and is hereby
13 amended to read as follows:

14 **“Section 16 20. Custody of Computer Data.** — All computer data, including
15 content and traffic data, examined under a proper warrant shall, within forty-eight (48)
16 hours after the expiration of the period fixed therein, be deposited with the court in a sealed
17 package, and shall be accompanied by an affidavit of the law enforcement authority
18 executing it stating the dates and times covered by the examination, and the law
19 enforcement authority who may access the deposit, among other relevant data. ~~The law~~
20 ~~enforcement authority shall also certify that no duplicates or copies of the whole or any~~
21 ~~part thereof have been made.~~ **PROVIDED THAT, LAW ENFORCEMENT**
22 **AUTHORITIES ARE AUTHORIZED TO RETAIN AND USE A COPY OF THE**
23 **COMPUTER DATA AS EVIDENCE FOR PURPOSES OF FILING A COMPLAINT**
24 **BEFORE THE PROSECUTOR’S OFFICE OR DURING THE PENDENCY OF A**

1 **CASE BEFORE THE COURT AND FOR RECORD KEEPING WHICH SHALL BE**
2 **CONSIDERED CONFIDENTIAL IN NATURE.**

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

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

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

11 SEC. 13. Section 20 of the same Act shall be renumbered as Section 21 and is hereby
12 amended to read as follows:

13 **“Section 21. Noncompliance.** — Failure **OF A SERVICE PROVIDER** to comply
14 with the ~~provisions of Chapter IV hereof specifically the~~ orders from law enforcement
15 authorities shall be punished as ~~a violation of Presidential Decree No. 1829~~ with
16 imprisonment of prison correctional in its maximum period or a fine of ~~One hundred~~
17 ~~thousand pesos (PHP100,00-420.00)~~ **ONE MILLION PESOS (PHP1,000,000.00)** or
18 both, for each and every noncompliance with an order issued by law enforcement
19 authorities **WITHOUT PREJUDICE TO THE PROVISIONS OF PRESIDENTIAL**
20 **DECREE NO. 1829.”**

21 SEC. 14. Sections 22 to 26 shall be renumbered accordingly and a new Section 27 is hereby
22 inserted to read as follows:

1 **“SECTION 27. CREATION OF THE ANTI-SCAM HUB. – WITHIN SIX (6)**
2 **MONTHS AFTER THE EFFECTIVITY OF THIS ACT, THE ANTI-SCAM HUB,**
3 **HEREINAFTER REFERRED TO AS THE “ASH”, SHALL BE CREATED UNDER**
4 **THE CONTROL AND SUPERVISION OF THE CYBERCRIME INVESTIGATION**
5 **AND COORDINATING CENTER (CICC) EXECUTIVE COMMITTEE TO**
6 **CENTRALIZE INVESTIGATIONS OF SCAM-RELATED CRIMES, DISRUPT**
7 **SCAMMERS’ OPERATIONS, AND HELP MITIGATE VICTIMS’ LOSSES.**

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

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

16 SEC. 15. Section 27 of the same Act is renumbered as Section 28, as well as succeeding
17 Sections, and Section 27, now Section 8, is hereby amended to read as follows:

18 **“Section ~~27~~ 28. Appropriations.** The amount of Fifty million pesos
19 (PhP50,000,000.00) shall be appropriated annually for the implementation of this Act.

20 **MOREOVER, THE CAPABILITY AND CAPACITY ENHANCEMENT**
21 **FOR THE PNP ANTI-CYBERCRIME GROUP AND NBI CYBERCRIME**
22 **DIVISION SHAL BE INCLUDED IN THE ANNUAL GENERAL**
23 **APPROPRIATIONS ACT.**

1 **PROVIDED FURTHER THAT, THE AMOUNT NECESSARY TO CREATE**
2 **THE ANTI-SCAM HUB SHALL BE CHARGED AGAINST THE CURRENT**
3 **YEAR’S APPROPRIATIONS OF THE AGENCIES CONCERNED. IN ADDITION,**
4 **THE AMOUNT OF ONE HUNDRED MILLION PESOS (PHP100,000,000.00) AS**
5 **INITIAL FUNDING FOR THE ANTI-SCAM HUB TO BE CHARGED AGAINST**
6 **THE UNEXPENDED CONTINGENCY FUND OF THE OFFICE OF THE**
7 **PRESIDENT IS HEREBY APPROPRIATED. THEREAFTER, THE AMOUNT**
8 **NEEDED FOR THE IMPLEMENTATION OF THE HUB SHALL BE INCLUDED**
9 **IN THE ANNUAL GENERAL APPROPRIATIONS ACT.”**

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

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

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

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

22 *Approved,*