



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

EIGHTEENTH CONGRESS
Second Regular Session

House Bill No. 7712



Introduced by Hon. Junie E. Cua
Lone District, Quirino

AN ACT
DEFINING ECONOMIC SABOTAGE IN COMPUTER-RELATED OFFENSES AND
AMENDING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE
“CYBERCRIME PREVENTION ACT OF 2012”

EXPLANATORY NOTE

The developments in information and communications technology has allowed cybercriminals to reach a vast multitude of Filipinos online resulting in high victimization rates for computer related fraud and forgery specifically through the social engineering scam known as “*phishing*”. In recent years, we have seen a rapid increase in cases of “*phishing*”, leading to losses amounting to hundreds of millions of pesos to the banking sector and the banking public in general.

As the country entered into periods of community quarantines to fight the pandemic brought about by COVID-19, most of the exchanges in goods and services and the corresponding payment transfers and other financial transactions, shifted to digital modes and online. The high demand for online financial transactions further exacerbated the increase of “*phishing*” cases. Without much information and awareness, many fell prey into the unlawful activities of cybercriminals adding to the mounting economic burden of bank clients and general Filipino public.

It is in this light that this bill is being introduced in order to curb the exploitation of information and communications technology as a means of perpetrating crimes in bulk and at massive scales. The current law does not provide hefty penalties to massive fraud via unauthorized transactions.

The steady rise of cybercrimes when left unattended and not prosecuted, will not only deprive Filipinos of their hard-earned money but will also undermine and render into disrepute the financial system. “*Phishing*” and other new forms of cyberfraud have an adverse impact on the banking industry and a deleterious effect on the confidence of clients to conduct online banking at such a time when they need it the most. Given the health crisis that the country is

facing, the hard life that our people are going through, and their critical dependency on online banking, what the fraudsters are doing is a form of economic sabotage.

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

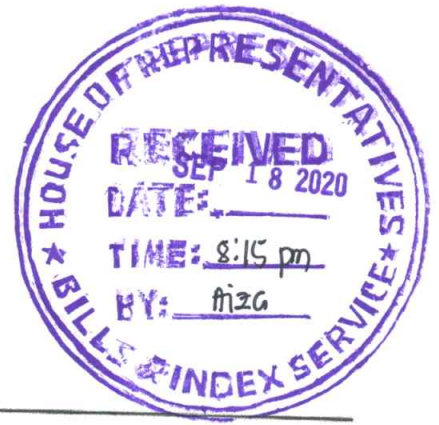
JUNIE E. CUA



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

EIGHTEENTH CONGRESS
Second Regular Session

House Bill No. 7712



Introduced by Hon. Junie E. Cua
Lone District, Quirino

AN ACT
DEFINING ECONOMIC SABOTAGE IN COMPUTER-RELATED OFFENSES AND
AMENDING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE
"CYBERCRIME PREVENTION ACT OF 2012"

EXPLANATORY NOTE

The developments in information and communications technology has allowed cyber criminals to reach a vast multitude of Filipinos online resulting in high victimization rates for computer related fraud and forgery specifically through the social engineering scam known as "*phishing*". In recent years, we have seen a rapid increase in cases of "*phishing*", leading to losses amounting to hundreds of millions of pesos to the banking sector and the banking public in general.

As the country entered into periods of community quarantines to fight the pandemic brought about by COVID-19, most of the exchanges in goods and services and the corresponding payment transfers and other financial transactions, shifted to digital modes and online. The high demand for online financial transactions further exacerbated the increase of "*phishing*" cases. Without much information and awareness, many fell prey into the unlawful activities of cybercriminals adding to the mounting economic burden of bank clients and general Filipino public.

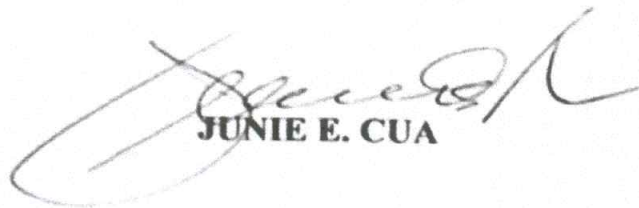
It is in this light that this bill is being introduced in order to curb the exploitation of information and communications technology as a means of perpetrating crimes in bulk and at massive scales. The current law does not provide hefty penalties to massive fraud via unauthorized transactions.

The steady rise of cybercrimes when left unattended and not prosecuted, will not only deprive Filipinos of their hard-earned money but will also undermine and render into disrepute the financial system. "*Phishing*" and other new forms of cyberfraud have an adverse impact on the banking industry and a deleterious effect on the confidence of clients to conduct online banking at such a time when they need it the most. Given the health crisis

Accred

that the country is facing, the hard life that our people are going through, and their critical dependency on online banking, what the fraudsters are doing is a form of economic sabotage.

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



JUNIE E. CUA



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

EIGHTEENTH CONGRESS
Second Regular Session

House Bill No. 7712

Introduced by Hon. Junie E. Cua
Lone District, Quirino

AN ACT
DEFINING ECONOMIC SABOTAGE IN COMPUTER-RELATED OFFENSES AND
AMENDING REPUBLIC ACT NO. 10175, OTHERWISE KNOWN AS THE
“CYBERCRIME PREVENTION ACT OF 2012”

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

SECTION 1. Section 2 of Republic Act No. 10175 is hereby amended to read as follows:

"Section 2. Declaration of Policy.— The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting electronic commerce, and data processing, in the nation's overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. **THE STATE LIKEWISE ACKNOWLEDGES THAT THE CAPACITY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY TO BE USED AS A MEANS OF PERPETRATING CRIME IN BULK AND AT A SCALE PREVIOUSLY UNHEARD OF, HAS BEEN EXPLOITED BY CRIMINALS AND CRIMINAL SYNDICATES IN PERPETRATING FRAUDULENT ACTIVITIES TO UNDERMINE THE TRUST OF THE PUBLIC IN THESE NEW TECHNOLOGIES AND THE EMERGING NEW ECONOMY IT SUPPORTS. DUE TO THIS DELETERIOUS EFFECT ON THE ECONOMY, THE STATE DECLARES THAT THE COMMISSION OF CERTAIN CRIMES UNDER THIS**

ACT USING INFORMATION AND COMMUNICATIONS TECHNOLOGY IS A FORM OF ECONOMIC SABOTAGE AND A HEINOUS CRIME AND SHALL BE PUNISHABLE TO THE MAXIMUM LEVEL ALLOWED BY LAW. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.”

SEC. 2. Section 3 of the same Act is hereby amended to read as follows:

“Section 3. Definition of Terms. — For purposes of this Act, the following terms are hereby defined as follows:

x x x

(C) BULK EMAIL/MASS MAILER REFERS TO A SERVICE OR SOFTWARE USED TO SEND ELECTRONIC MAIL IN MASS.

(D) Communication x x x;

(E) Computer x x x;

(F) Computer data x x x;

(G) Computer program x x x;

(H) Computer system x x x;

(I) Without right x x x;

(J) Cyber x x x;

(K) Critical infrastructure x x x;

(L) Cybersecurity x x x;

(M) Database x x x;

(N) Interception x x x;

(O) PHISHING REFERS TO A SOCIAL ENGINEERING SCHEME TO OBTAIN OR ANY ATTEMPT TO OBTAIN SENSITIVE INFORMATION SUCH AS USERNAMES, PASSWORDS, BANK ACCOUNT DETAILS, CREDIT CARD, DEBIT CARD, AND E-WALLET INFORMATION AMONG OTHER ELECTRONIC CREDENTIALS BY DISGUIISING AS A TRUSTWORTHY ENTITY IN AN ELECTRONIC COMMUNICATION FOR THE PURPOSE OF ILLEGALLY ACCESSING A VICTIM'S ONLINE ACCOUNT FOR FINANCIAL GAIN.

(P) Service provider x x x;

(Q) Subscriber's information x x x;

(R) Traffic data or non-content data x x x.”

SEC. 3. Section 4(b) of the same Act is hereby amended to read as follows:

“Section 4. *Cybercrime Offenses.* — The following acts constitute the offense of cybercrime punishable under this Act:

XXX

(b) Computer-related Offenses:

(1) Computer-related Forgery. — x x x

(2) Computer-related Fraud. — x x x

(3) Computer-related Identity Theft. — x x x

(4) ECONOMIC SABOTAGE - ANY OFFENSE PERPETRATED UNDER THIS SUBSECTION USING A BULK E-MAIL, MASS MAILER OR ANY SERVICE, SOFTWARE, OR OTHER METHOD OF DELIVERY CALCULATED TO UTILIZE THE MASSIVE REACH OF THE INTERNET TO REACH THE MAXIMUM NUMBER OF VICTIMS, PURSUANT TO A “PHISHING” OR OTHER SIMILAR FRAUDULENT SCHEME, SHALL BE PUNISHED AS AN ACT OF ECONOMIC SABOTAGE.”

SEC. 4. Section 8 of the same Act is hereby amended to read as follows:

“Section 8. *Penalties.* — Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a maximum amount commensurate to the damage incurred or both.

Any person found guilty of the punishable act under Section 4(a)(5) shall be punished with imprisonment of *prision mayor* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to maximum amount commensurate to the damage incurred or both, shall be imposed.

ANY PERSON FOUND GUILTY OF AN OFFENSE THAT CONSTITUTES ECONOMIC SABOTAGE UNDER SECTION 4(B)(4) SHALL BE PUNISHED WITH LIFE IMPRISONMENT AND A FINE OF NOT LESS THAN ONE MILLION PESOS (₱1,000,000.00) BUT NOT MORE THAN FIVE MILLION PESOS (₱5,000,000.00).

X x x.”

SEC. 5. Separability Clause. If any separable provision of this Act is declared unconstitutional, the remaining provisions shall continue to be in force.

SEC. 6. Repealing Clause. All laws, decrees, executive orders, rules and regulations or parts thereof which are inconsistent with this Act are hereby repealed, amended or modified accordingly.

SEC. 7. Effectivity. This Act shall take effect fifteen (15) days after its publication in the *Official Gazette* or in a newspaper of general circulation.