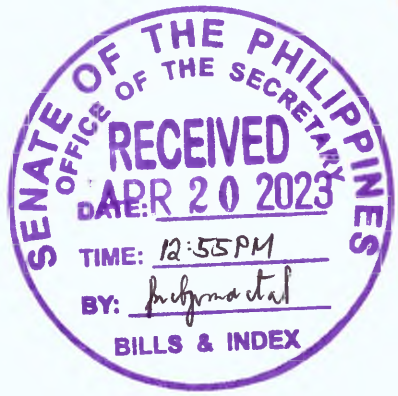
NINETEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)



S E N A T E

P.S. Res. No. 573

Introduced by SENATOR RAMON BONG REVILLA, JR.

RESOLUTION

DIRECTING THE APPROPRIATE SENATE COMMITTEE TO CONDUCT AN INQUIRY, IN AID OF LEGISLATION, INTO THE REPORTED BREACH OF THE DATABASE OF THE PHILIPPINE NATIONAL POLICE (PNP) AND OTHER GOVERNMENT AGENCIES WHICH STORE PERSONAL DATA OF BOTH EMPLOYEES AND THE GENERAL PUBLIC, WITH THE END IN VIEW OF AUDITING THE EXTENT AND IMPACT OF THE BREACH, AND ENACTING POLICIES TO STRENGTHEN CYBERSECURITY

WHEREAS, Republic Act No. 10173, or the "*Data Privacy Act of 2012*", emphasizes that "[t]he State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected";

WHEREAS, VPNMentor, leading cybersecurity research company, reported that a staggering 1,279,437 records belonging to law enforcement agencies, including sensitive police employee information, have been compromised in an unprecedented data breach. The report was authored by cybersecurity researcher, Jeremiah Fowler;

WHEREAS, the reported voluminous data hack has exposed 817.54 gigabytes of both applicant and employee records under multiple state agencies, including the Philippine National Police (PNP), National Bureau of Investigation (NBI), Bureau of Internal Revenue (BIR), and Special Action Force (SAF);

WHEREAS, the possibly compromised records include highly sensitive data such as fingerprint scans, birth certificates, tax identification numbers (TIN), tax filing

records, academic transcripts, and even passport copies. The report even revealed that the said data were available for public access for at least six weeks;

WHEREAS, the same report highlighted that "these documents were stored in an unsecured, non-password-protected database, which is easily accessible to individuals with an internet connection and highly vulnerable to cyberattacks or ransomware";

WHEREAS, Kroll, an independent risk advisory firm shared that enterprises in the Philippines are among the most vulnerable in the Asia-Pacific region to cyberattacks that cause business interruption and even data loss. The country came in second with the most cyberattacks in the region;

WHEREAS, in a similar report from virtual private network service provider, Surfshark, the Philippines ranked 23rd out of 250 countries that were most affected by data breaches, with a total of 523,684 leaked accounts in the third quarter of 2022;

WHEREAS, International Data Corp.'s (IDC) Asia-Pacific Security Sourcing Survey 2022, highlighted that companies in Southeast Asia recognize the need to invest in cybersecurity in the advent of heightened usage of digital platforms in their operations;

WHEREAS, similar data breaches have been recorded in the past with government agencies being vulnerable to said attacks. Back in November 2021, the Department of Foreign Affairs (DFA) reported a similar data leak in their online passport tracking system. The Commission on Elections (COMELEC) has also revealed in 2022 that around "60 gigabytes" worth of "sensitive voter information" and other data have been hacked. Before this, a group of hackers also downloaded the personal data records of some 54 million registered voters;

WHEREAS, the private sector is not spared from these attacks. They are equally vulnerable to cybersecurity threats. In fact, in November 2022, it was reported that nearly eighty percent (80%) of companies in the Philippines have experienced data breach over a period of 12 months, with two in every five firms losing at least $500,000 to digital fraudsters;

WHEREAS, without reliable and trustworthy cybersecurity measures in place, these reported data breaches remain to have the dangerous potential of exposing individuals to identity theft, phishing attacks, and a range of other malicious activities,

which will ultimately victimize the public. Even worse, government agencies as well as private entities may very well be endangered by the susceptibilities of our cybersecurity if left inadequate;

WHEREAS, the alarm raised by these data breaches in government records may lead to potential national security issues;

WHEREAS, if unabated, the exposed data may lead to nefarious transactions such as criminals taking advantage of the leaked data to blackmail and threaten law enforcers;

WHEREAS, data privacy and protection is a matter of national interest and it is imperative for Congress to enact responsive policies to deter possible data breaches;

NOW THEREFORE, BE IT RESOLVED, as it is hereby resolved, to direct the appropriate Senate Committee to conduct an inquiry, in aid of legislation, into the reported breach of the database of the Philippine National Police (PNP) and other government agencies which store personal data of both employees and the general public, with the end in view of auditing the extent and impact of the breach, and enacting policies to strengthen cybersecurity.

Adopted,

RAMON BONG REVILLA, JR.