



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: COMMISSION ON ELECTIONS,
SMARTMATIC GROUP OF COMPANIES,
RVA, WS, AND OTHER JOHN DOES
AND JANE DOES

NPC SS 22-001
and NPC SS 22-008

INITIATED AS A *SUA SPONTE* NPC
INVESTIGATION ON POSSIBLE
DATA PRIVACY VIOLATIONS
COMMITTED IN RELATION TO THE
ALLEGED HACK AND BREACH OF
THE COMMISSION ON ELECTIONS
SYSTEM OR SERVERS

X-----X

DECISION

AGUIRRE, D.P.C.;

Before this Commission is a *sua sponte* initiated case by the Complaints and Investigation Division (CID) of the National Privacy Commission (NPC) against the Commission on Elections (COMELEC), Smartmatic Group of Companies (Smartmatic), RVA , Winston Steward (Steward), and other John Does and Jane Does for an alleged violation of Section 29 and Section 30 of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

The case arose from a news article of Manila Bulletin published on 10 January 2022 entitled “Comelec servers hacked; Downloaded data may include information that could affect 2022 elections.”¹ The news article reported that the Manila Bulletin Technews team allegedly discovered that hackers breached the server of COMELEC and “downloaded files that included, among others, usernames, and

¹ Manila Bulletin Technews, *Comelec servers hacked; Downloaded data may include information that could affect 2022 elections*, MANILA BULLETIN, 10 January 2022, available at <https://mb.com.ph/2022/01/10/comelec-servers-hacked-downloaded-data-may-include-information-that-could-affect-2022-elections/> (last accessed 28 September 2022).

PINS of vote-counting machines (VCM) [...] network diagrams, IP addresses, list of all privileged users, domain admin credentials, list of all passwords and domain policies, access to the ballot handling dashboard, and QR code captures the bureau of canvassers with login and password.”² The news article further stated that the downloaded data “included list of overseas absentee voters, location of all voting precincts with details of board of canvassers, all configuration list of database, and list of all user accounts of [COMELEC] personnel.”³

On the same day, COMELEC made an announcement on its official website entitled “*COMELEC Statement on Alleged Hacking Incident*” stating:

The COMELEC is presently validating the allegations of the article published by the Manila Bulletin, specifically whether COMELEC systems have, in fact been compromised. With no independent verification that a hack has indeed taken place, one thing immediately stands out: the article alleges that the hackers were able to “download files that included, among others, usernames and PINS of vote-counting machines (VCM).” The fact, however, is that such information still does not exist in COMELEC systems simply because the configuration files – which includes usernames and PINs – have not yet been completed. This calls into question the veracity of the hacking claim.

As for the rest of the allegations made, please note that the article offers scant substantiation for its assertions despite claiming that the authors had “verified that there was an ongoing hack.” Indeed, the article does not even offer proof of such verification.

Moving forward, the COMELEC assures the public of its full and scrupulous compliance with the Data Privacy Act, as well as its continuing cooperation with the National Privacy Commission. The COMELEC will likewise continue its efforts to validate the assertions made by the article. In this regard, we invite the authors to shed light on their allegations, particularly with regard to the “verification” they claim to have carried out. Considering that “news” like this could potentially damage the credibility of the elections, the COMELEC stands ready to pursue all available remedies against those who, either

² *Id.*

³ *Id.*

deliberately or otherwise, undermine the integrity of the electoral process.⁴

On 11 January 2022, the CID conducted an initial investigation and drafted its Initial Report.⁵ The CID reported that it checked the website of COMELEC for any vulnerabilities and did not find any major vulnerability while using online tools.⁶ It also discovered that the website of COMELEC uses Cloudflare to protect the website against Distributed Denial of Service (DDoS) attacks.⁷ The CID sent Notices to Explain to COMELEC, Manila Bulletin, and Mr. ASJ, an editor of Manila Bulletin, and invited them to appear for a clarificatory hearing on 25 January 2022.⁸

On 15 January 2022, ASJ complied with the Notice to Explain and submitted artifacts that he allegedly received from his source.⁹

On 20 January 2022, COMELEC requested the postponement of the Clarificatory Hearing scheduled on 25 January 2022.¹⁰

On 21 January 2022, the CID denied COMELEC's request and directed COMELEC to appear during the 25 January 2022 Clarificatory Hearing and to submit additional documents and information.¹¹

On 24 January 2022, the CID, in a Supplemental Technical Report, narrated that on 20 January 2022, it contacted "XSOX Group" (XSOX Group), the group claiming responsibility for the alleged hacking of the COMELEC and Smartmatic servers, via their TOX messenger address supplied by ASJ.¹² It requested for more samples of election

⁴ Commission on Elections, *COMELEC Statement on Alleged Hacking Incident*, COMMISSION ON ELECTIONS, 10 January 2022, available at <https://comelec.gov.ph/?r=References/Announcements/10Jan2022pr> (last accessed 30 September 2022).

⁵ Initial Report, Complaints and Investigation Division, 11 January 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁶ *Id.* at 2.

⁷ *Id.* at 3.

⁸ Notices to Explain, Complaints and Investigation Division, 11 January 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁹ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 2, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

¹⁰ *Id.* at 2.

¹¹ Order (To submit additional documents and provide further information), Complaints and Investigation Division, 21 January 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

¹² Supplemental Technical Report, Complaints and Investigation Division, 24 January 2022, at 1, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS

canvassers and a sample of the overseas absentee voters list to gather evidence and information regarding the alleged hacking and data leak in the COMELEC and Smartmatic servers.¹³ As a response to the request, the XSOX Group gave the CID an additional ten (10) files that contained details of election canvassers dated 2016.¹⁴

On 25 January 2022, during the Clarificatory Hearing, COMELEC Director James Jimenez narrated the circumstances surrounding the alleged hacking incident.¹⁵ His narration later formed part of a Memorandum that was eventually submitted to the CID on 28 January 2022.¹⁶ COMELEC contradicted the assertions of the published news article by contending that “COMELEC’s system for generating the usernames and P[ersonal] I[nformation] N[umber]s for the VCMs is not online. Therefore, it has not been breached and cannot be breached as claimed in the article.”¹⁷ COMELEC alleged that it has not started generating the PINs yet for the VCMs for the 2022 elections as the list of candidates has not been finalized as of the date of the published news article.¹⁸ COMELEC also asserted that it does not have a system with a “ballot handling dashboard” and “QR code captures” and it also stated that it does not constitute a “bureau of canvassers” as what the news article published.¹⁹

COMELEC also addressed the issue regarding the list of overseas absentee voters.²⁰ COMELEC alleged that the list is not included in any component of the automated election system and the list is available in the official COMELEC website “www.comelec.gov.ph” as a required publication in compliance with the law.²¹ As such, COMELEC stated that the list of overseas absentee voters does not need to be “hacked” in order for it to be accessed.²²

22-008, (NPC 2022); Supplemental Report, Complaints and Investigation Division, Annex B, 20 January 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

¹³ *Id.*

¹⁴ *Id.*

¹⁵ Clarificatory Hearing with the Commission on Elections, 25 January 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

²¹ Clarificatory Hearing with the Commission on Elections, 25 January 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

²² *Id.*

COMELEC further alleged that its server for the preparation of election data for the 2022 elections is installed offline and is only accessible via a Local Area Network (LAN) at the COMELEC Warehouse.²³ COMELEC asserted that access to its server is governed by strict security protocols and an individual who gains access to its server must be authorized and must be physically present at the COMELEC Warehouse to do so.²⁴

On the same date, the CID also conducted a clarificatory hearing with ASJ and SC of the Manila Bulletin where ASJ. narrated his version of the circumstances surrounding the incident.²⁵

On 27 January 2022, the CID sent an Order to Submit Compliance directing COMELEC to submit documents and information that were discussed during the Clarificatory Hearing.²⁶

On 28 January 2022, COMELEC submitted a Memorandum and an internal Position Paper dated 19 January 2022 on the alleged hacking incident.²⁷ The Memorandum containing the Position Paper reiterated COMELEC's position during the 25 January 2022 Clarificatory Hearing.²⁸

On 27 January 2022, the CID issued an Order to Appear for Clarificatory Hearing on 04 February 2022 and Submit Compliance to Smartmatic.²⁹

On 04 February 2022, during the Clarificatory Hearing with Smartmatic, Smartmatic narrated that COMELEC ordered Smartmatic to explain the alleged hacking incident when the Manila Bulletin news article was released.³⁰ Smartmatic submitted

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ Order (To Submit Compliance), 27 January 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

²⁷ Memorandum No. 220177, 26 January 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

²⁸ *Id.*

²⁹ Order (To Appear), 28 January 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

³⁰ Clarificatory Hearing with Smartmatic Group of Companies, 04 February 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

documents and information in compliance with the Order dated 28 January 2022.³¹

On 08 February 2022, the CID issued an Order to Ventureslink Management Solutions, Inc. (VMSI), a manpower agency contracted to perform site surveys during the 2016 elections, to attend a clarificatory hearing on 11 February 2022.³² During the 11 February 2022 Clarificatory Hearing, VMSI confirmed that it was engaged to conduct site survey of precincts in Regions IV-A, IV-B, VI, VII, and VIII for the 2016 elections.³³ Its representative informed the CID that he could not confirm that the artifact presented to him was the same form used during the conduct of the site survey.³⁴ He also stated that VMSI surrendered all documents and information to Smartmatic.³⁵

On 11 February 2022, Smartmatic's counsels manifested that it cannot participate in the ongoing investigation due to an alleged Letter dated 10 February 2022 sent by COMELEC Commissioner Marlon Casquejo (Commissioner Casquejo).³⁶ The Letter allegedly contained a directive to Smartmatic that prohibited it from disclosing further information since the matter was covered by a non-disclosure agreement and involved the preparations and conduct of elections that COMELEC asserted to be within its exclusive jurisdiction.³⁷

On 14 February 2022, the CID issued Orders directing COMELEC and Smartmatic to appear for a clarificatory hearing on 22 February 2022 and to submit compliance.³⁸ It also directed Smartmatic to appear for a clarificatory hearing on 24 February 2022.³⁹

³¹ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 5, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

³² Order (To Appear), 08 February 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

³³ Clarificatory Hearing with Ventureslink Management Solutions, Inc., 11 February 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

³⁸ Clarificatory Hearing with Smartmatic Group of Companies, 11 February 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

³⁹ *Id.*

³⁸ Order (To Appear), 14 February 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

³⁹ *Id.*

On 18 February 2022, COMELEC submitted a Memorandum on the voting system and data policy of overseas voters, and sample forms used in the registration of overseas voters.⁴⁰

On 22 February 2022, during the Clarificatory Hearing with COMELEC and Smartmatic, the CID requested a copy of the purported Letter dated 10 February 2022 but Commissioner Casquejo declined to furnish a copy of the Letter to the CID.⁴¹

In the same hearing, the CID presented an artifact that purports to be the list of overseas absentee voters for COMELEC to verify.⁴² COMELEC refuted the artifact presented because there are data fields, specifically “height” and “weight”, that are not collected in the forms.⁴³ COMELEC submitted its overseas voter registration form to make a comparison to the artifact presented to show that there is no collection of data pertaining to “height” and “weight”.⁴⁴

On 24 February 2022, Smartmatic did not appear in the scheduled Clarificatory Hearing. Instead, it filed a Manifestation and Motion dated 24 February 2022 and reiterated its position in the 22 February 2022 Clarificatory Hearing.⁴⁵

On the 04 March 2022 Clarificatory Hearing, Smartmatic reiterated its Manifestation with Motion dated 24 February 2022.⁴⁶ It also filed an Omnibus Manifestation stating that it dispenses its right to participate as a witness and will comment when evidence is presented in the appropriate forum.⁴⁷

⁴⁰ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 7, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁴¹ Clarificatory Hearing with the Commission on Elections and Smartmatic Group of Companies, Inc., 22 February 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁴² Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 7, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ Manifestation with Motion, 24 February 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁴⁶ Clarificatory Hearing with Smartmatic Group of Companies, 04 March 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁴⁷ Omnibus Manifestation, 04 March 2022, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

On 09 March 2022, the CID issued a Notice for On-site Inspection scheduled on 18 March 2022,⁴⁸ and an Order directing COMELEC to submit a copy of the Letter dated 10 February 2022.⁴⁹ The CID did not receive any response from COMELEC.⁵⁰ As a result, it served a copy of the Notice for On-Site Inspection and Order on 16 March 2022.⁵¹

On 17 March 2022, the CID's representatives appeared before the Senate Committee on Electoral Reform and People's Participation to provide information on the alleged breach of COMELEC servers.⁵²

On 18 March 2022, the CID attempted to conduct an on-site inspection of COMELEC's Warehouse.⁵³ COMELEC, however, refused the CID's admission to its premises. It also informed the CID of a letter dated 17 March 2022, which provides that the COMELEC was not amendable to an on-site inspection for various reasons.⁵⁴

The CID sent a Letter dated 18 March 2022 to the National Bureau of Investigation (NBI) requesting for information that its Cybercrime Division had gathered regarding the breach in COMELEC and Smartmatic servers.⁵⁵

Subsequently, the NBI supplied the CID with the *Sinumpaang Salaysay* of RVA dated 02 February 2022.⁵⁶ The lawyer who assisted RVA in his *Sinumpaang Salaysay* informed him that he was being investigated for the crime of Illegal Access under the Cybercrime Prevention Act of 2012.⁵⁷

In his *Sinumpaang Salaysay*, RVA stated that he worked at Smartmatic from August 2021 to January 2022 as a Quality Assurance Tester and,

⁴⁸ Notice, 09 March 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁴⁹ Order (To Submit Compliance), 09 March 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁵⁰ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 7, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁵¹ *Id.*

⁵² *Id.*

⁵³ *Id.*

⁵⁴ Letter, 17 March 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁵⁵ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 8, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁵⁶ *Id.* Annex S.

⁵⁷ *Id.* Annex S at 1.

due to his role, he had access to the virtual private network (VPN) of Smartmatic.⁵⁸ When asked about the details leading up to the alleged Illegal Access he had committed, RVA narrated that he received a private message from a certain WS on Facebook Messenger promising to pay him Fifty Thousand Pesos (Php 50,000.00) to Three Hundred Thousand Pesos (Php 300,000.00) in exchange for giving access to his computer while connected to Smartmatic's servers.⁵⁹

RVA narrated that when he went to the COMELEC Office for work, he gave access to his computer using AnyDesk App through the internet while connected to Smartmatic servers on the last week of December 2021.⁶⁰ RVA further explained that the AnyDesk App is a closed source remote desktop application that gains remote access or control of file transfers and VPN functionality in another computer device without even having physical control over the computer and that may be accessed at a different location.⁶¹

RVA also stated that while he accomplished his end of the deal, Steward did not carry out his promise of paying him the sum of money.⁶² Instead, he was given online computer lectures such as Cobalt Strike and Lateral Movement.⁶³

On 05 April 2022, the CID submitted its Consolidated Fact-Finding Report⁶⁴ that serves as the Complaint for *sua sponte* initiated cases with the CID as the Nominal Complainant.⁶⁵ It asserted that RVA, Steward, and several John Does and Jane Does (RVA, *et al.*) are liable for Section 29 (Unauthorized Access or Intentional Breach) of the DPA. The CID stated that it was through RVA's actions that Steward and other unknown individuals "were able to breach and consequently access the overseas [absentee] voters list and site survey

⁵⁸ *Id.* Annex S at 2.

⁵⁹ *Id.* Annex S at 2-3.

⁶⁰ *Id.* Annex S at 3.

⁶¹ Consolidated Fact-Finding Report, Complaints and Investigation Division, Annex S at 3, 05 April 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁶² *Id.*

⁶³ *Id.*

⁶⁴ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, Winston Steward, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁶⁵ See National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule X, §§ 5-6 (28 January 2021).

forms.”⁶⁶ Thus, the CID contended that without RVA’s indispensable participation, the breach would not have happened, and the access of Steward and other unknown individuals to the personal data stored in Smartmatic’s servers could have been averted.⁶⁷

The CID also opined that COMELEC and Smartmatic be recommended for prosecution to the Department of Justice (DOJ) for a violation of Section 30 (Concealment of Security Breaches Involving Sensitive Personal Information) of the DPA.⁶⁸ The CID alleged that the data fields in the site survey form and overseas absentee voter list involve personal data that can be used for identity fraud.⁶⁹ The CID claimed that COMELEC and Smartmatic concealed the personal data breach as both entities, after several hearings, have adamantly denied and insisted that no breach has ever occurred on their servers.⁷⁰

On 11 April 2022, the Commission issued an Order directing COMELEC, Smartmatic, RVA, and Steward to submit their Comment within fifteen (15) days from receipt of the Order. It provides:

WHEREFORE, premises considered, Respondents Commission on Elections, Smartmatic Group of Companies, RVA, and Winston Steward are ORDERED, within fifteen (15) days from receipt of this Order, to file their respective COMMENTS on the allegations in the attached Consolidated Fact-Finding Report, pursuant to Section 6 of Rule X of NPC Circular No. 2021-01.

Further, the Complaints and Investigation Division (CID) of the National Privacy Commission, may, in its discretion, submit its REPLY within ten (10) days from receipt of Respondents’ respective comments.

Respondents may, in their discretion, submit their respective REJOINDERS to the CID’s Reply within ten (10) days from receipt of the Reply.

SO ORDERED.⁷¹

⁶⁶ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 21, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ *Id.* at 16.

⁷⁰ *Id.* at 17.

⁷¹ Order to Comment, 11 April 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008, (NPC 2022).

On 20 May 2022, the NPC received Smartmatic's Manifestation.⁷² Smartmatic stated that the CID's Consolidated Fact-Finding Report was not attached to the Order dated 11 April 2022.⁷³

On 23 May 2022, COMELEC and Smartmatic was served a copy of the Order, the CID's Consolidated Fact-Finding Report, and its corresponding annexes.⁷⁴

On 03 June 2022, Smartmatic filed a Manifestation with Motion for Additional Time to File a Comment.⁷⁵ Smartmatic stated that it needed an extension to "properly verify the allegations in the Consolidated Fact-Finding Report and the voluminous attachments and/or annexes referred therein[.]"⁷⁶ Smartmatic also alleged that it "is still engaged with the post-election matters in the conduct of the 2022 National and Local Elections."⁷⁷ Thus, Smartmatic prayed that an additional period of fifteen (15) calendar days from 07 June 2022, or until 22 June 2022 to submit its Comment on the Consolidated Fact-Finding Report.⁷⁸

On 07 June 2022, COMELEC filed a Motion for Extension of Time to Submit a Comment.⁷⁹ COMELEC alleged that although the National and Local Elections had come to an end, it is still "engaged in the assessment and winding up of various election-related activities, [as well as] being called to immediately exercise its administrative and quasi-judicial functions over election matters and cases filed before it[.]"⁸⁰ COMELEC further alleged that "[it] is already on another cycle of its election preparations [... for the ...] Synchronized Barangay and Sangguniang Kabataan Elections."⁸¹ Aside from internal reasons given by the COMELEC, it claimed that it "is still awaiting the reply from the Office of the Solicitor General (OSG), whose legal assistance

⁷² Smartmatic Group of Companies Manifestation, 20 May 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁷³ *Id.*

⁷⁴ Order, 10 June 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁷⁵ Smartmatic Group of Companies Manifestation, 03 June 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁷⁶ *Id.* at 2.

⁷⁷ *Id.*

⁷⁸ *Id.* at 2-3.

⁷⁹ Commission on Election Motion for Extension, 07 June 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁸⁰ *Id.* at 2.

⁸¹ *Id.*

was sought by it.”⁸² Thus, COMELEC prayed that it be given an additional period of fifteen (15) days from 07 June 2022, or until 22 June 2022 to file its Comment on the Consolidated Fact-Finding Report.⁸³

On 10 June 2022, the Commission issued an Order granting Smartmatic’s request for additional time to file its Comment.⁸⁴ The Commission also firmly reminded Smartmatic to strictly comply with the additional period it requested for and that no further extension shall be allowed.⁸⁵

On 20 June 2022, the Commission issued an Order granting COMELEC’s request for additional time to file its Comment.⁸⁶

On 22 June 2022, Smartmatic submitted its Comment on the Consolidated Fact-Finding Report.⁸⁷ Smartmatic argued that the CID’s investigation and report did not state sufficient basis for its conclusion that there was a personal data breach in COMELEC’s or Smartmatic’s servers.⁸⁸ Smartmatic alleged that the CID’s investigation and report were based on sources provided by a certain XSOX Group that should be considered as an anonymous tip or complaint.⁸⁹ Smartmatic claimed that “there was no verification or substantiation as the CID essentially accepted the validity of the documents from an anonymous criminal group wholesale.”⁹⁰ As such, Smartmatic contended that the proceedings before the CID in validating the alleged artifacts were improper and not credible as the CID could not verify the artifacts by independent means and the CID merely resorted to inviting resource persons to “shed light” on the matter.⁹¹

On 24 June 2022, the Commission received another Motion for Extension of Time to Submit its Comment dated 17 June 2022 from

⁸² *Id.*

⁸³ *Id.*

⁸⁴ Order, 10 June 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁸⁵ *Id.*

⁸⁶ *Id.*

⁸⁷ Smartmatic Group of Companies Comment, 22 June 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁸⁸ *Id.* at 6.

⁸⁹ *Id.* at 6-8.

⁹⁰ *Id.* at 8.

⁹¹ *Id.* at 9-10

the OSG requesting for additional period of fifteen (15) days from 22 June 2022, or until 07 July 2022. The OSG explained that “considering the intricacies of the issues involved in this case and the need to coordinate with the COMELEC Law Department regarding the preparation of the Comment, additional time is needed by the OSG.”⁹² The OSG also stated that the case was assigned to the undersigned Solicitor only on 15 June 2022, a week before the deadline given to COMELEC to file its Comment.⁹³

On 08 July 2022, a day after the lapse of the initial extension of time it requested, the Commission received another Motion for Additional Extension of Time to File Comment from the OSG dated 04 July 2022.⁹⁴ The OSG claimed that “while [it] has already coordinated with the COMELEC Law Department regarding the filing of the required Comment, the OSG is still awaiting their reply to its Letter dated 17 June 2022 requesting for pertinent documents and additional significant information on the matter.”⁹⁵ Thus, the OSG prayed that the COMELEC be given an additional period of fifteen (15) days from 07 July 2022, or until 22 July 2022 to file its Comment.⁹⁶

On 14 July 2022, the Commission issued an Order granting the OSG’s Motion for Additional Extension of Time to File Comment dated 04 July 2022.⁹⁷ The Commission ordered the OSG to submit COMELEC’s Comment on the Consolidated Fact-Finding Report within a non-extendible period of fifteen (15) days from 07 July 2022, or until 22 July 2022.⁹⁸

On 22 July 2022, the COMELEC, through the OSG, submitted its Comment.⁹⁹ COMELEC contended that “the CID significantly failed to determine with reasonable certainty that the breach involving

⁹² Motion for Extension of Time to Submit Comment, Office of the Solicitor General, 17 June 2022, at 2, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁹³ *Id.*

⁹⁴ Motion for Additional Extension of Time, Office of the Solicitor General, 04 July 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁹⁵ *Id.* at 2-3.

⁹⁶ *Id.* at 3.

⁹⁷ Order, 14 July 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

⁹⁸ *Id.* at 3.

⁹⁹ Commission on Elections Comment, Office of the Solicitor General, 22 July 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

[Smartmatic's] servers/system has a positive connection with personal data contained in [] COMELEC's certified list of overseas voters and/or the posted computerized voters list."¹⁰⁰ As such, COMELEC claimed that the CID committed "serious error"¹⁰¹ in recommending COMELEC to be liable for violating Section 30 of the DPA for allegedly concealing the personal data breach in Smartmatic's servers.¹⁰² Thus, COMELEC prayed that CID's recommendation be set aside for lack of factual and legal basis.

Issues

- I. Whether RVA, Winston Steward, and other John Does and Jane Does (RVA, WS, and other unknown individuals) are liable under Section 29 (Unauthorized Access or Intentional Breach) of the DPA.

- II. Whether COMELEC and Smartmatic are liable for Section 30 (Concealment of Security Breaches Involving Sensitive Personal Information) of the DPA.

Discussion

I. RVA, WS, and other unknown individuals are liable under Section 29 (Unauthorized Access or Intentional Breach) of the DPA.

In the CID's Consolidated Fact-Finding Report, which serves as the Complaint in this *sua sponte* initiated case,¹⁰³ the CID pointed to RVA's statements contained in his *Sinumpaang Salaysay* and alleged that RVA "knowingly and willingly allowed a certain Winston Steward access to [Smartmatic's] network[.]"¹⁰⁴ Thus, the CID recommended finding RVA, WS, and other unknown individuals liable in violation of Section 29 of the DPA. The pertinent provision provides:

¹⁰⁰ *Id.* at 4.

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ See NPC 2021 Rules of Procedure, rule X, § 5-6.

¹⁰⁴ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 21, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

Section 29. *Unauthorized Access or Intentional Breach.* The penalty of the penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five Hundred Thousand Pesos (Php500,000.00) but not more than Two Million Pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.¹⁰⁵

Unauthorized Access or Intentional Breach is committed when the following requisites concur:

1. The data system stores personal or sensitive personal information;
2. The accused breaks into the system; and
3. The accused knowingly and unlawfully broke into the system in a manner which violates data confidentiality and security of the same.¹⁰⁶

In this case, all requisites are present. As such, the Commission finds RVA, WS, and other unknown individuals liable for Unauthorized Access or Intentional Breach.

The first requisite is present in this case. It is not disputed that Smartmatic's data system stores personal or sensitive personal information. The data system of Smartmatic stores personal data of voters by reason of the election results transmissions solutions, management, and services (ERTSMS Contract) in connection with the 2016, 2019, and 2022 elections that it entered into with COMELEC.¹⁰⁷ As such, Smartmatic possessed the personal data of voters and rendered its services in relation to the conduct of elections as COMELEC's Personal Information Processor (PIP).¹⁰⁸ Thus, the first requisite of a data system storing personal or sensitive personal information is present.

¹⁰⁵ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 29 (2012).

¹⁰⁶ ACN v. DT, NPC 18-109, 01 June 2021, *available at* <https://www.privacy.gov.ph/wp-content/uploads/2022/01/Decision-NPC-18-109-ACN-v.-DT.pdf> (20 October 2022).

¹⁰⁷ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 5, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

¹⁰⁸ *Id.* at 21.

As for the second requisite or “the accused breaks into the system”, RVA admitted in his *Sinumpaang Salaysay* that he gave unauthorized access to Steward and other unknown individuals through the use of the AnyDesk App.¹⁰⁹ RVA narrated that on December 2021, he gave access to his computer using the AnyDesk App through the internet while connected to Smartmatic servers.¹¹⁰ RVA while connected to Smartmatic’s servers was at the COMELEC Office when he gave unauthorized access through the AnyDesk App to Steward and other unknown individuals.¹¹¹ As the CID pointed out, “[i]t was through...RVA’s actions this WS and other unknown individuals were able to breach and consequently access the voters list and site survey forms.”¹¹² It was through RVA’s indispensable participation that led to WS and unknown individuals’ breaking into the system, thus, the second requisite is present in this case.

The third requisite is satisfied in this case. RVA, WS, and other unknown individuals knowingly and unlawfully broke into or breached Smartmatic’s servers that violated data confidentiality and security data systems. There is no question that these individuals knowingly and unlawfully consummated the act of breaking into Smartmatic’s system. Further, the bribe offered to RVA by WS and other unknown individuals shows the intention to do the illegal act of Unauthorized Access and Intentional Breach penalized under Section 29 of the DPA. For RVA, money was the motivation to commit the crime as he supposedly needed it to feed his two-month-old child.¹¹³ Regardless of his motivations, Argana must face the consequences of his illegal action of knowingly and unlawfully breaking into Smartmatic’s servers that resulted in violating data confidentiality and the security of data systems. Thus, the third element is satisfied.

Given the foregoing, the Commission finds RVA, WS, and other unknown individuals liable for violating Section 29 of the DPA. These individuals committed Unauthorized Access or Intentional Breach when they broke into Smartmatic’s servers that store personal

¹⁰⁹ *Id.* Annex S at 3.

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² *Id.* at 21.

¹¹³ Consolidated Fact-Finding Report, Complaints and Investigation Division, Annex S at 5, 05 April 2022, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

or sensitive personal information. These individuals are recommended for prosecution to the DOJ.

II. COMELEC and Smartmatic are not liable under Section 30 (Concealment of Security Breaches Involving Sensitive Personal Information) of the DPA.

As previously discussed, the Consolidated Fact-Finding Report serves as the Complaint in *sua sponte* investigations, with the CID as the Nominal Complainant.¹¹⁴ In this case, the CID alleged that there are two sets of personal data breaches that occurred in Smartmatic and COMELEC's servers.¹¹⁵ The first relates to site survey forms, and the second relates to the overseas absentee voters list.

A. COMELEC and Smartmatic did not violate Section 30 of the DPA in relation to the site survey forms.

In the CID's FFR, the CID alleged that COMELEC and Smartmatic are liable for Concealment of Security Breaches Involving Sensitive Personal Information under Section 30 of the DPA. It provides:

Section 30. Concealment of Security Breaches Involving Sensitive Personal Information. The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach.¹¹⁶

The requisites of Concealment of Security Breaches Involving Sensitive Personal Information are:

1. A personal data breach occurred;
2. The breach is one that requires notification to the Commission; and

¹¹⁴ See NPC 2021 Rules of Procedure, rule X, § 5-6.

¹¹⁵ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 10-11, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

¹¹⁶ Data Privacy Act of 2012, § 30.

3. The person knowingly conceals the fact of such breach from the Commission.¹¹⁷

Although Section 30 of the DPA penalizes the concealment or failure to notify the Commission of a security breach, the concealed security breach must be one that requires mandatory breach notification under Section 20 (f) of the DPA. This is because Section 30 refers to “the obligation to notify the Commission pursuant to Section 20(f).” Section 20 (f) of the DPA states:

Section. 20. *Security of Personal Information.*

...

(f) The personal information controller shall promptly notify the Commission and affected data subjects **when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.** The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.¹¹⁸

In relation to Section 20 (f) of the DPA, Section 11 of NPC Circular 16-03 (Personal Data Breach Management) discusses the parameters of mandatory breach notification:

Section 11. *When notification is required.* Notification shall be required upon knowledge of, or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

¹¹⁷ See Data Privacy Act of 2012, § 30.

¹¹⁸ Data Privacy Act of 2012, § 20 (f). Emphasis supplied.

- A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.

...

- B. There is reason to believe that the information may have been acquired by an unauthorized person; and
- C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.¹¹⁹

As such, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.¹²⁰

The Commission acknowledges that there had been a breach in Smartmatic's servers through the acts of RVA, Steward, and other unknown individuals. The Commission, however, finds that there is no obligation on the part of COMELEC, the Personal Information Controller (PIC), and Smartmatic, the Personal Information Processor (PIP) to report the breach to the Commission because the first and third requisite for mandatory breach notification are not present.

As to the first requisite, the breach does not involve sensitive personal information or information that may be used to enable identify fraud. In this case, the CID presented artifacts relating to site survey forms allegedly taken from Smartmatic or COMELEC's servers.¹²¹ The CID stated that it "discovered that the name and signature of both the person who performed the site survey and the

¹¹⁹ National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §11 (15 December 2016).

¹²⁰ NPC Circ. No. 16-03, §11.

¹²¹ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 11, *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

contact person or a representative of the latter appeared [in these forms].”¹²² The CID claims that it was able to verify and authenticate these forms when it “matched the name of RVA to the personnel list provided for by VMSI,”¹²³ the manpower agency that employed RVA to perform site surveys.¹²⁴ Aside from the name and signature alleged by CID, the site survey forms also shows the positions or designations of the data subjects.

The name, signature, and designation of the data subject cannot be considered as sensitive personal information, which refers to:

Section 3. *Definition of Terms.*

...

(l) Sensitive personal information refers to personal information:

(1) About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(2) About an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.¹²⁵

A data subject’s name, signature, and designation clearly do not fall within the definition of sensitive personal information.

The name, signature, and designation when taken by themselves, cannot also be considered as information that may be used to enable

¹²² *Id.*

¹²³ *Id.*

¹²⁴ *Id.* at 5.

¹²⁵ Data Privacy Act of 2012, § 3 (l).

identity fraud. A determination of whether the compromised information may enable identity fraud requires a consideration of circumstances other than the nature of the personal information involved, including the manner in which the personal information was obtained, whether that information was specifically targeted, and the specific nature of the breach. In this case, a data subject's name and signature without other pieces of information that substantiate a data subject's identity cannot be considered as sufficient to perpetuate identity fraud. To add to this, the data subjects whose personal information were exposed in the site survey forms were either government employees or were performing services pursuant to a contract with the government. Following Section 4 (a) and (b) of the DPA, the names and designations of these data subjects are excluded from the scope of the DPA, thus:

Section. 4. *Scope.*

...

This Act does not apply to the following:

- (a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual

...

- (b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services[.]¹²⁶; .

Given all this, the first requisite for mandatory breach notification is lacking.

The third requisite that the unauthorized acquisition is likely to give rise to a real risk of serious harm is also not present. The CID presented artifacts of the site survey forms that contain data fields

¹²⁶ Data Privacy Act of 2012, § 4.

regarding the 2016 elections.¹²⁷ Given that the alleged breach happened in 2022, the personal information taken from the breach may be inaccurate and outdated. Taken together with the fact that the personal information involved is neither sensitive personal information nor information that enables identity fraud, the unauthorized acquisition of personal information in the site survey forms is unlikely to give rise to a real risk of serious harm to the affected data subjects.

Considering that the first and third requisites for mandatory breach notification are absent in this case, the Commission finds that the breach pertaining to personal information leaked through the site survey forms does not require mandatory breach notification to the Commission. Since the PIC and the PIP do not have an obligation to notify the Commission of the breach under Section 20 (f) of the DPA, the Commission finds Smartmatic and COMELEC not liable for Concealment of Security Breaches Involving Sensitive Personal Information.

B. COMELEC and Smartmatic did not violate Section 30 of the DPA in relation to the overseas absentee voters list.

On the issue of the overseas absentee voters list, the CID presented several artifacts supplied by the XSOX Group relating to the overseas absentee list that allegedly contained personal data of approximately one hundred thirty-eight thousand nine hundred (138,900) individuals.¹²⁸ As these artifacts received by the CID are uncorroborated, the CID contended that it took steps to verify the artifacts stating:

To verify and determine whether the artifact may be an actual voters list, the CID randomly selected individuals and attempted to cross-reference them to the overseas voters' list on the COMELEC website, however, no such list was available therein. As an alternative, the CID cross-referenced the names on the artifact to certified voters' list provided for in the Department of Foreign Affairs (DFA) website for various Philippine Embassies in different countries, however, no

¹²⁷ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 18, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022)*.

¹²⁸ *Id.* at 10.

matches were made. Also, the sheer size and volume of records and the limited overseas list available for cross-referencing made it an impractical pursuit.

Notwithstanding, the CID also randomly selected from the artifact, ten (10) individuals and searched over the Internet for any digital footprint or identifier. This resulted in a match with ten (10) Facebook profiles. From the ten (10) selected, nine (9) individuals matched details with respect to their name and city or province of their residence as stated in their respective profiles. Moreover, these individuals maintain relatively active profiles.

As such, the CID can reasonably conclude that the artifact contains actual data pertaining to existing individuals.

We recall that during the clarificatory hearing conducted on 25 January 2022 and again on 22 February 2022, the CID confronted representatives of COMELEC with the voter's list reduced into an excel file and readily denied its ownership. COMELEC observed that it contained data fields with respect to height and weight and noted that COMELEC did not collect such information for registration purpose. To support COMELEC's assertions, it submitted sample registration forms used during the 2016 elections up to the present.¹²⁹

An examination of the records show that the CID failed to sufficiently prove that the artifacts it received from the XSOX Group were gathered from an alleged breach of Smartmatic or COMELEC's servers. In this case, the CID, as the Nominal Complainant, has the burden of proof and must prove its allegations with substantial evidence.

In administrative proceedings, it is the complainant who carries the burden of proving their allegations with substantial evidence or such "relevant evidence that a reasonable mind might accept as adequate to support a conclusion."¹³⁰ Section 1, Rule 131 of the 2019 Amendments to the Revised Rules on Evidence provides:

Section 1. Burden of proof and burden of evidence. Burden of proof is the duty of a party to present evidence on the facts in issue

¹²⁹ *Id.* at 10-11.

¹³⁰ *Ombudsman v. MLF*, G.R. No. 211450, 23 July 2018.

necessary to establish his or her claim or defense by the amount of evidence required by law. Burden of proof never shifts.

Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a *prima facie* case. Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case.¹³¹

It is the party who alleges a fact that has the burden of proving it. The Supreme Court held that “it is basic in the rule of evidence that bare allegations, unsubstantiated by evidence, are not equivalent to proof. In short, mere allegations are not evidence.”¹³² Thus, the CID will not be able to discharge its burden of proof with substantial evidence by mere allegations.

The CID cannot simply conclude that the unverified artifacts came from a breach because it tested ten (10) out of the one hundred thirty-eight thousand nine hundred (138,900) individuals. From the ten (10) individuals selected, nine (9) of them had Facebook profiles that matched the purported overseas absentee voters list that was taken from the alleged breach of Smartmatic’s server. Testing ten (10) out of one hundred thirty-eight thousand nine hundred (138,900) individuals is insufficient because verifying ten (10) individuals is too small of a sample size and will not produce a meaningful result. Further, the only thing that the CID’s test confirmed is that some of the people on the artifacts are real people. The test results, however, do not show that the list came from a breach of COMELEC’s or Smartmatic’s systems or servers.

Further, the artifact of overseas absentee voters list presented by the CID contained data fields that COMELEC does not collect, specifically height and weight. To support COMELEC’s assertions, COMELEC submitted sample registration forms that were used during the 2016 elections up to the present.¹³³ After reviewing the submitted sample registration forms of COMELEC, the data fields of

¹³¹ 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. No. 19-08-15-SC, Rule 131, §1 (1 May 2020). Emphasis supplied.

¹³² *Government Service Insurance System v. Prudential Guarantee and Assurance, Inc.*, Development Bank of the Philippines and Land Bank of the Philippines, G.R. No. 165585, 20 November 2013.

¹³³ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 11 and Annex F, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022);

“height” and “weight” were not collected by COMELEC. Thus, in comparing CID’s artifacts to COMELEC’s sample registration forms that have been used in the past several elections, the irregularities between the two opposing evidence cast doubt on the veracity and authenticity of CID’s evidence.

Smartmatic argued that the CID’s evidence were not properly authenticated and verified:

17. The subsequent parallel investigation covered by Reference No. SS 22-008 (“SS 22-008”) (which is essentially identical to SS 22-[0]01 except in its title) was also prompted by the posts of the same XSOX.Group in social media:

‘On 11 February 2022, while conducting active monitoring of the internet for privacy violations, data breaches, and data dumps affecting personal information, **the Commission monitored posts made by XSOX Group.**

An extensive examination of the **numerous posts made by XSOX [Group] revealed artifacts that point to a probable breach of Smartmatic servers/system, which appear to involve personal information.**’

18. Curiously, however, even after the Investigation was already concluded, the CID still acknowledges that its sources have not been properly verified, thus:

‘xxx at the very beginning of this controversy, a group identified only as XSOX Group has expressly taken responsibility and authorship over the attack on [Smartmatic’s] servers/system. **The members of this group are still unknown, and there is insufficient evidence or lead/information, at this point, to readily identify the members of this organization. Similarly, the identity of ASJ’s Source cannot be determined with certainty.**’

19. In *Anonymous Complaint v. Presiding Judge Dagala*, the Supreme Court ruled that anonymous complaints should always be treated with great caution. Consequently, the Supreme Court will act on an **anonymous complaint** provided its allegations can be **reliably verified and properly substantiated by competent evidence, like public records of**

indubitable integrity. In this case, however, there was no verification or substantiation as the CID essentially accepted the validity of the documents from an anonymous criminal group wholesale.¹³⁴

Smartmatic asserted that CID's artifacts can be likened to an "anonymous complaint" that needs to properly authenticated and corroborated by competent evidence.¹³⁵ The CID, however, erroneously concluded that the artifacts have sufficiently been verified and authenticated by cross-checking merely ten (10) selected individuals as its sample size. The CID's procedure of verifying and substantiating the anonymous tips provided by the XSOX Group did not overcome its dubious origin.

The COMELEC asserted that the CID found that there was no breach in COMELEC's servers or system.¹³⁶ The COMELEC pointed to the CID's Consolidated Fact-Finding Report as basis:

2. Whether there was a hack or breach of COMELEC servers/system

While the news article published by Manila Bulletin alluded to a hack or breach of COMELEC servers, the CID is not convinced that COMELEC servers or its system were breach nor is it convinced that the artifacts that it has gathered from multiple sources are any indication that said COMELEC servers or system was compromised.

The pieces of evidence gathered in the course of CID's investigation in this case also suggest that COMELEC servers or its system were not breached.¹³⁷

COMELEC further argued that Smartmatic's system and COMELEC'S system are separate and are completely different from one another.¹³⁸ It averred that an alleged breach in Smartmatic's servers or system does not necessarily relate to the personal

¹³⁴ Smartmatic Group of Companies Comment, 22 June 2022, at 7-8, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

¹³⁵ *Id.* at 7-8.

¹³⁶ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 12, *in* In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

¹³⁷ *Id.* Emphasis supplied.

¹³⁸ *Id.* at 4.

information stored in COMELEC's database pertaining to the overseas absentee voters list:

3. [...] In this case, **the CID significantly failed to determine with reasonable certainty that the breach involving the [Smartmatic] servers/system has a positive connection with personal data contained in respondent's COMELEC's certified list of overseas voters and/or posted computerized voter's list.** Such being the case, the CID committed serious error in holding respondent COMELEC liable for violation of Section 30 of R.A. No. 10173 for allegedly concealing the security breach of [Smartmatic] servers/system involving personal data contained in an overseas absentee voter's list that is speculated to have originated from respondent COMELEC but which speculation was not duly substantiated.¹³⁹

The burden of proof is on the CID to provide a direct link that connects the alleged breach in Smartmatic's servers or system to COMELEC's servers or system. The CID, however, failed to make a positive connection and simply concluded that the system was not breached by the alleged hacking by the XSOX Group.¹⁴⁰

Assuming that the overseas absentee voters list did come from Smartmatic's servers or system, COMELEC may be held liable for a breach of Smartmatic's servers or system following the principle of accountability. The DPA provides for the Principle of Accountability and concomitant obligations of a PIC:

Section. 21. *Principle of Accountability.* Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the requirements of this Act and shall use

¹³⁹ Commission on Elections Comment, Office of the Solicitor General, 22 July 2022, at 4, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022). Emphasis supplied.

¹⁴⁰ Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 20-21, *in* *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.¹⁴¹

In this case, COMELEC is considered as the PIC as it is the Constitutional Commission with exclusive jurisdiction relative to the conduct of elections. It is in a position to exercise control and discretion in matters relating to the conduct of elections. COMELEC entered into the ERTSMS Contract with Smartmatic, its PIP, in order for Smartmatic to render its services. Thus, COMELEC, as the PIC, is accountable for any personal data breach that may have occurred in Smartmatic's servers or system.

Although COMELEC may be held accountable for a breach that occurred in Smartmatic's servers or system, the Commission finds that there is no breach in relation to the overseas absentee voters list. The CID failed to prove with substantial evidence its allegations that the overseas absentee voters list resulted from a breach of Smartmatic's servers or system. Thus, its assertions that Smartmatic and COMELEC should be held liable for Concealment of a Breach of Sensitive Personal Information in relation to the overseas absentee voters list must fail.

To summarize, the Commission does not find COMELEC and Smartmatic liable for Concealment of Security Breaches Involving Sensitive Personal Information under Section 30 of the DPA. On matters relating to the site survey forms, there is no obligation to notify the Commission of the breach because the first and third requisites for mandatory breach notification are lacking.

On the issue regarding the overseas absentee voters list, the CID failed to discharge its burden of proof and was unable to prove its allegations with substantial evidence. The Commission cannot find COMELEC and Smartmatic liable on the basis of mere allegations of the CID in its FFR.

The Commission notes that there is no evidence on record that shows that there was a lack of reasonable and appropriate security measures that could have resulted in the breach. Smartmatic's servers or

¹⁴¹ Data Privacy Act of 2012, § 21.

system being breached was caused by employee malfeasance. While there is no security measure that is 100% effective, this becomes all the more true when there is employee malfeasance involved. Nevertheless, it remains the obligation of PICs to take proactive steps to ensure that its security measures minimize, if not altogether eliminate, these risks. The inevitability of breaches should not give rise to indolence but instead spur action. After all, the protection of our fundamental human right to privacy is at stake.

WHEREFORE, premises considered, this Commission hereby:

1. **FINDS** RVA, Winston Steward, and other John Does or Jane Does violated Section 29 of the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).
2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice and **RECOMMENDS** the prosecution of RVA, Winston Steward, and other John Does or Jane Does for Unauthorized Access or Intentional Breach under Section 29 of the DPA;
3. **DISMISSES** the case against Commission on Elections and the Smartmatic Group of Companies for lack of merit.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against Respondents Commission on Elections, Smartmatic Group of Companies, RVA, Winston Steward, and other John Does or Jane Does before any other forum or tribunal, if any.

SO ORDERED.

City of Pasay, Philippines.
22 September 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

BSJ
Data Protection Officer
COMMISSION ON ELECTIONS

COMMISSION ON ELECTIONS
LAW DEPARTMENT
8/F Palacio del Gobernador,
General Luna Street,
Intramuros, Manila
law@comelec.gov.ph
comelec.law@gmail.com

RVA

OFFICE OF THE SOLICITOR GENERAL
Counsel for Commission on Elections
134 Amorsolo St., Legaspi Village,
Makati City
docket@osg.gov.ph

ANGARA ABELLO CONCEPCION REGALA & CRUZ
*Counsel for Smartmatic Philippines, Inc., Smartmatic TIM Corporation,
SMMT, INC., and SMMT-TIM 2016, INC.*

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission