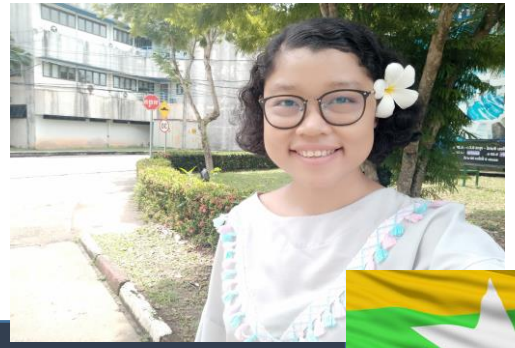
Analysis into Data Protection in E-commerce landscape from different ASEAN Scheme

Marlina

Abraham



Aye Hninn Khine

Dina Eka Putri

Pang (Peeyakorn)

OUTLINES

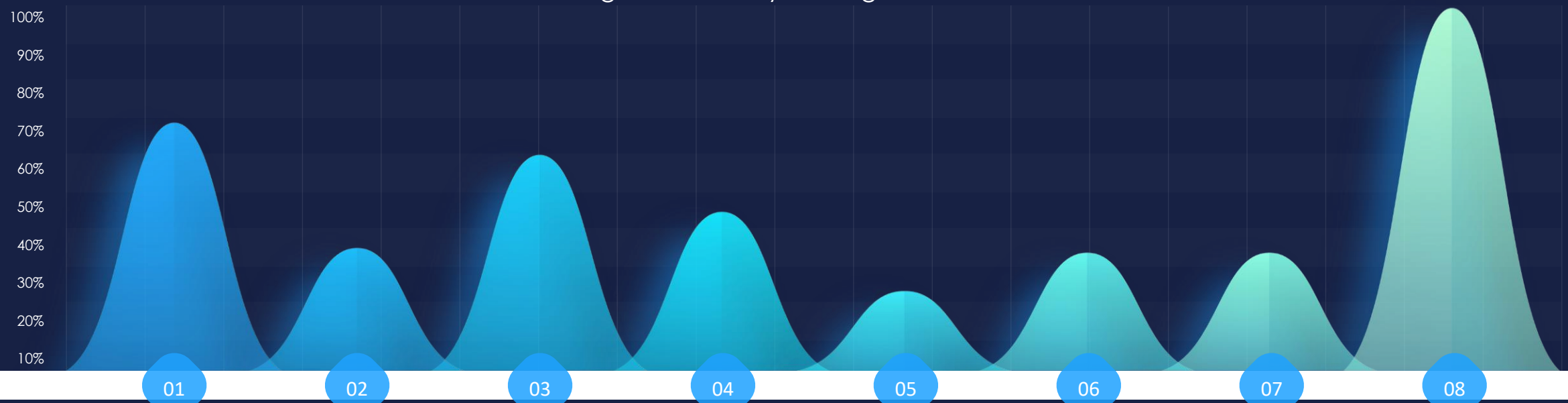
1. Digital Transformation and Digital Economy in ASEAN
2. The Importance of Data Protection in E-Commerce
3. Key Challenges of E-Commerce Landscape in ASEAN
4. Best Practice for Data Protection in E-Commerce
5. Strategies and Recommendations for Data Protection in E-Commerce

1 Digital Transformation and Digital Economy in ASEAN

- ASEAN Digital Transformation
- ASEAN Digital Economy
- Mini Survey on Consumer Behavior on Using E-Commerce and Digital Payment

ASEAN Digital Transformation: Faster Than Ever

COVID-19 has been serving as the catalyst of Digital Transformation in Southeast Asia



70%
of the region's population is now online

36%
consumers are new to digital services

63%
E-Commerce gained 63% growth from 2019 to 2020

47%
of online Grocery users are new, of which 76% plan to continue using the service going forward.

25%
e-Wallets transactions rose to 25% post-COVID-19 (from an average of 18% pre-COVID-19)

37%
Cash as payment method fell from 48% of transactions to 37% in 2020

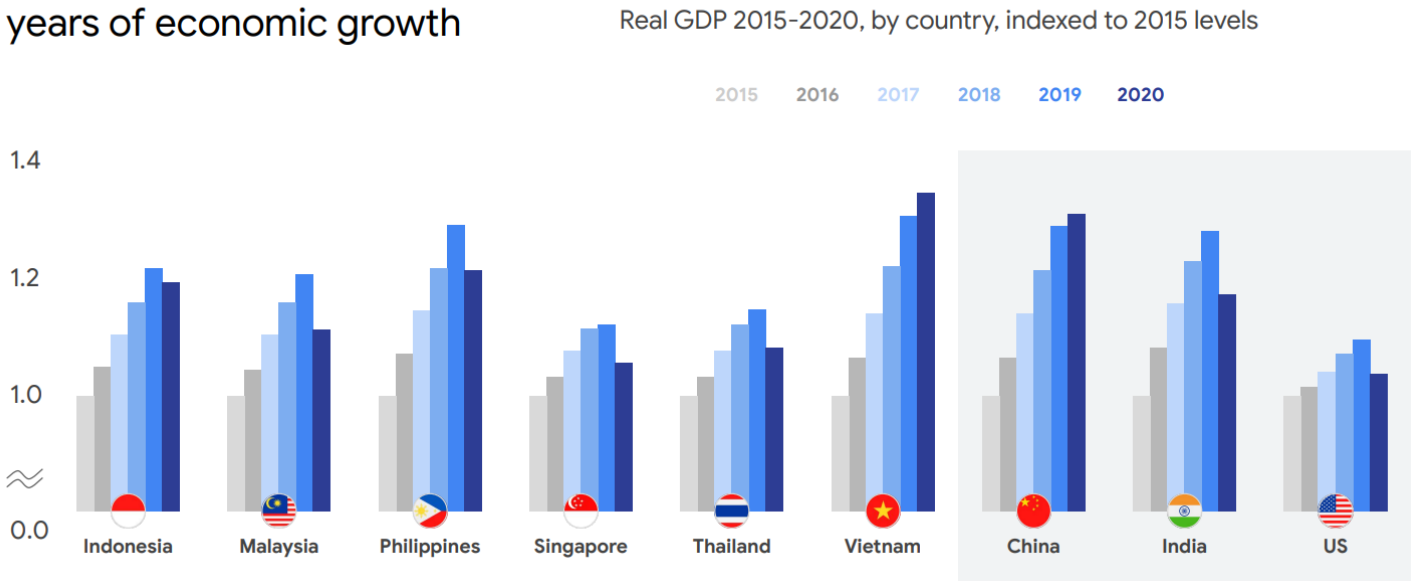
37%
New Users of Food Delivery users during lockdown

94%
new digital service consumers intend to continue with the service post-pandemic

Source: 5th edition of e-Conomy SEA by Google, Temasek, Bain

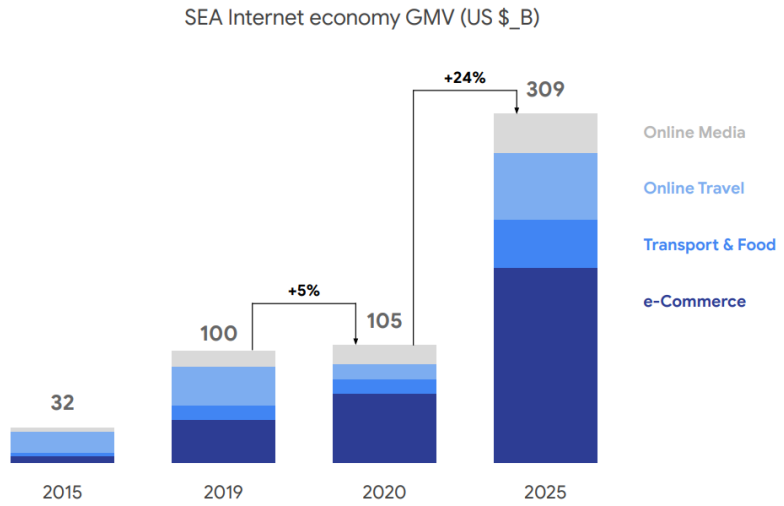
ASEAN Digital Economy: Resilient and Going Stronger

COVID-19 reversed
years of economic growth



The Internet economy **remains resilient at US $100B GMV**, even in the face of a global slowdown. As consumers and SMEs come online, **the 2025 number stands strong at over US $300B**, indicating growth despite a challenged environment.

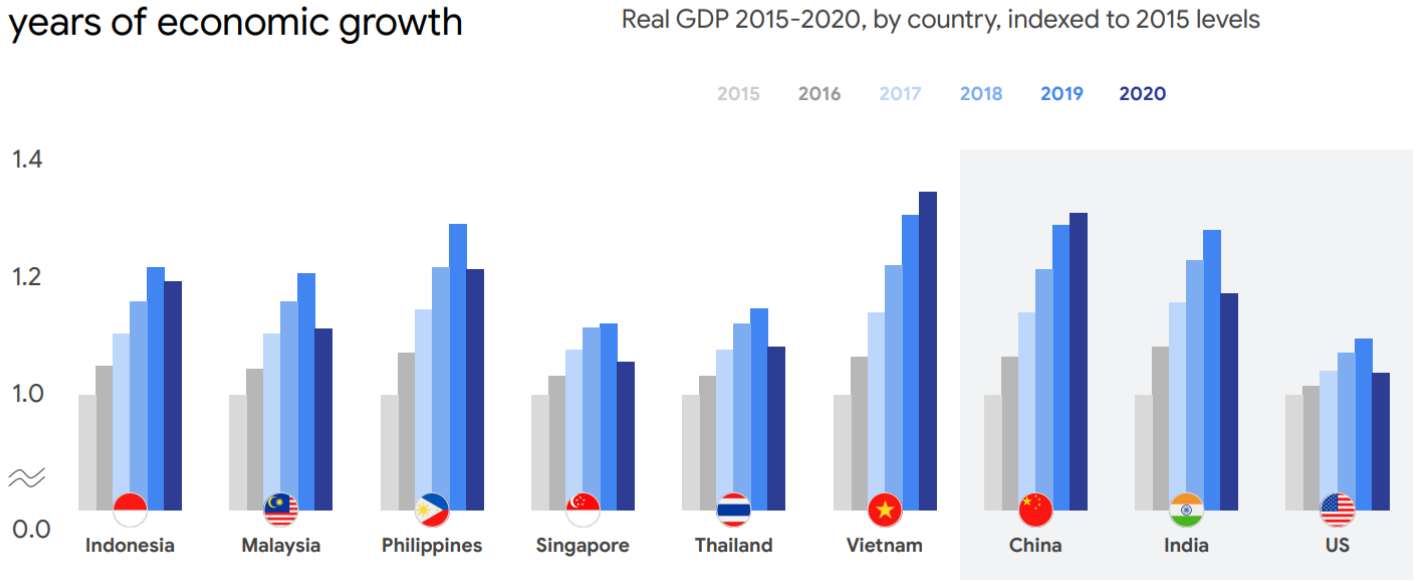
The SEA Internet economy will exceed **$100B GMV** this year despite headwinds



Source: 5th edition of e-Conomy SEA by Google, Temasek, Bain

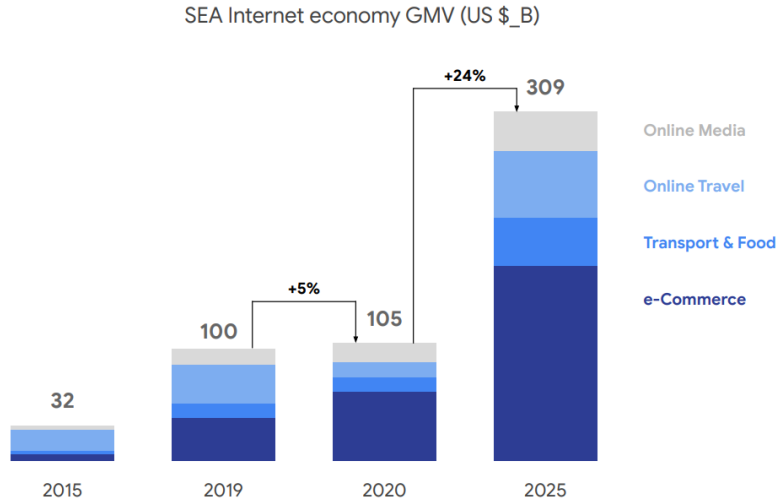
ASEAN Digital Economy: Resilient and Going Stronger

COVID-19 reversed
years of economic growth



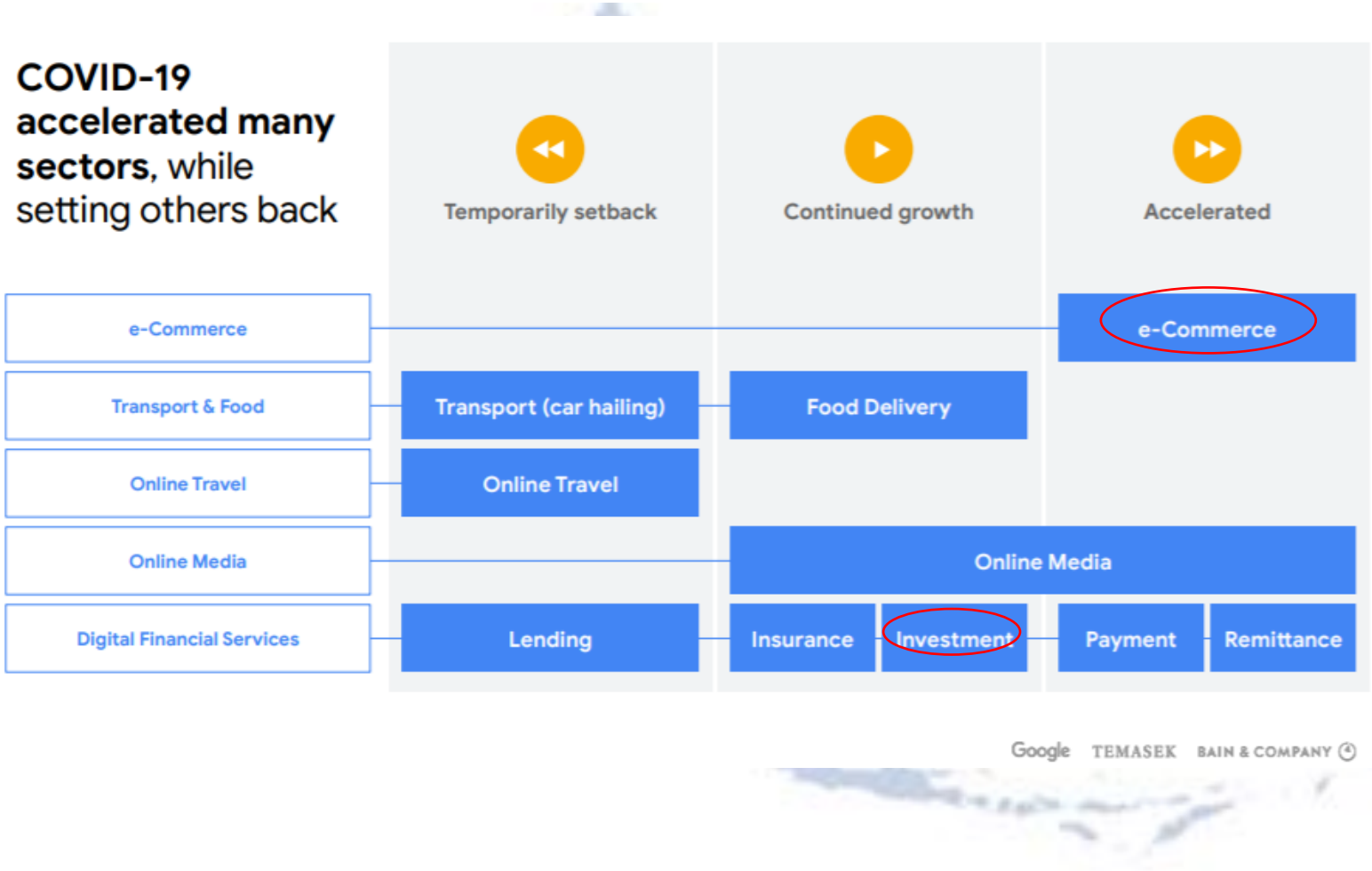
The Internet economy **remains resilient at US $100B GMV**, even in the face of a global slowdown. As consumers and SMEs come online, **the 2025 number stands strong at over US $300B**, indicating growth despite a challenged environment.

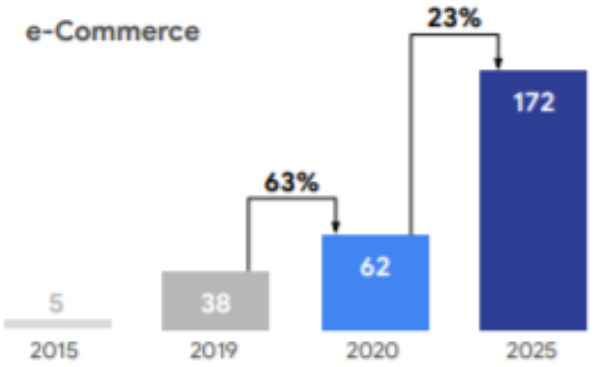
The SEA Internet economy will exceed **$100B GMV** this year despite headwinds

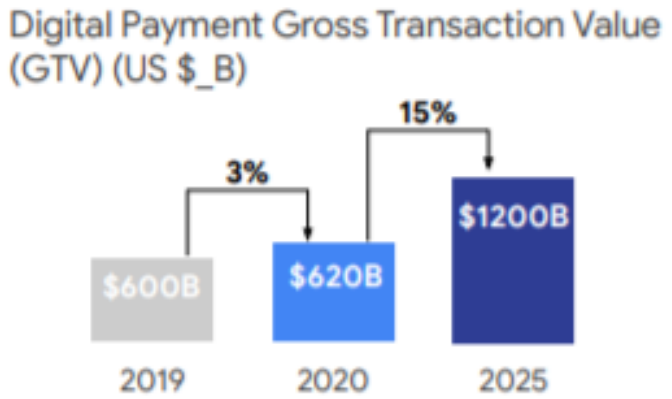


Source: 5th edition of e-Conomy SEA by Google, Temasek, Bain

ASEAN Digital Economy: Promising Future of E-Commerce and Digital Payment







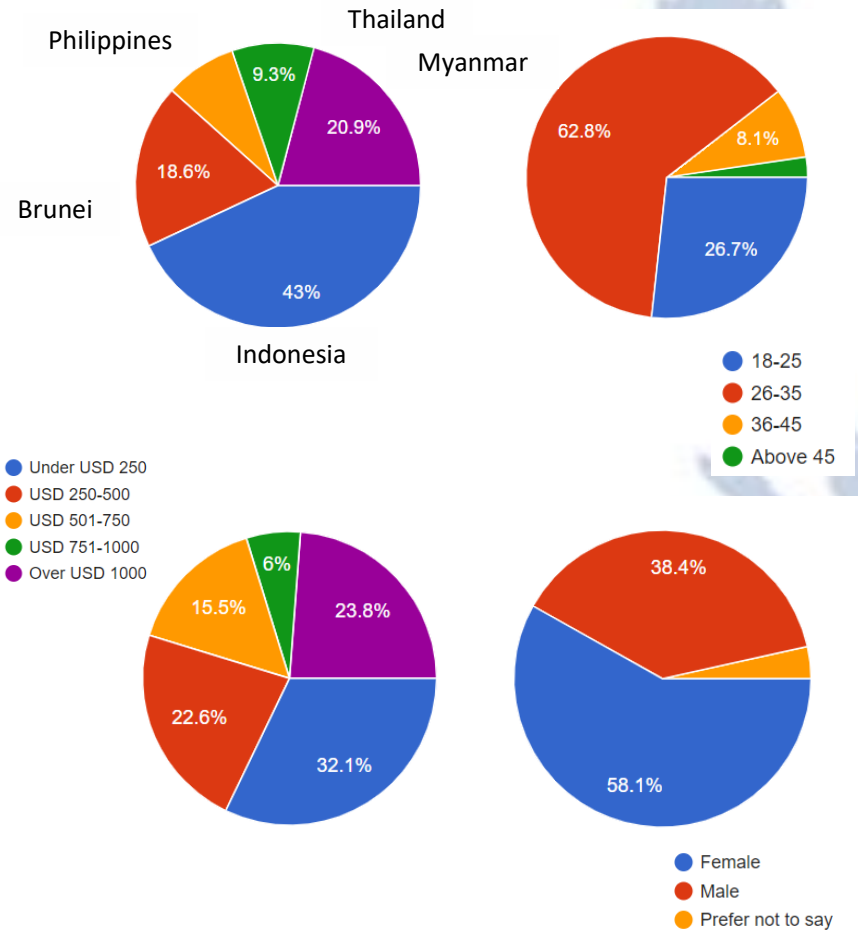
Source: 5th edition of e-Conomy SEA by Google, Temasek, Bain

Mini Survey on Consumer Behavior on Using E-Commerce and Digital Payment

Mini Survey conducted to recognize consumer behavior on using E-Commerce and Digital Payment confirmed the earlier studies on the same topics, as well as capture how very-well aware consumers are towards their data privacy and protection.

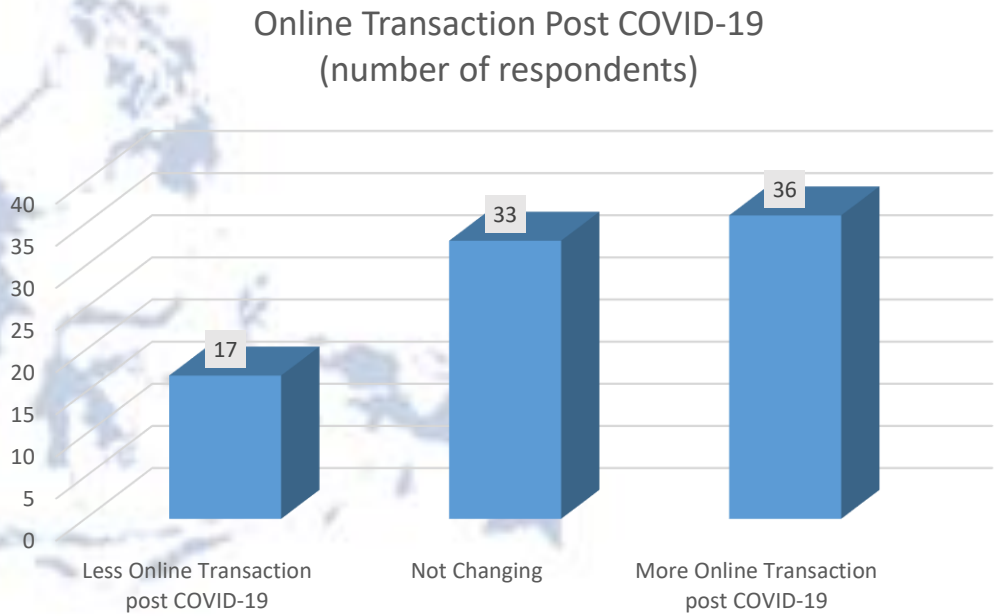
Respondents profiling:

No of Respondents: 86



Respondents Changing Habits on E-Commerce (Pre-Post COVID-19):

We investigated the changing behavior on E-Commerce/Online Transaction Usage pre and post COVID using nonparametric statistical different test i.e. Sign Test, Wilcoxon, and Marginal Homogeneity. All showed that **there is significant difference on average number of online transaction between pre and post COVID-19 with significance of 0.034 , 0.006, and 0.006, respectively (on confidence level 95%).**

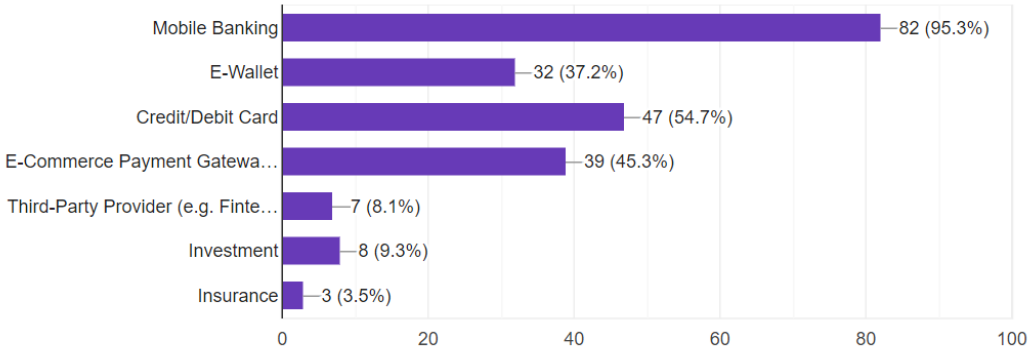


Source: Group Project 4 Mini Survey

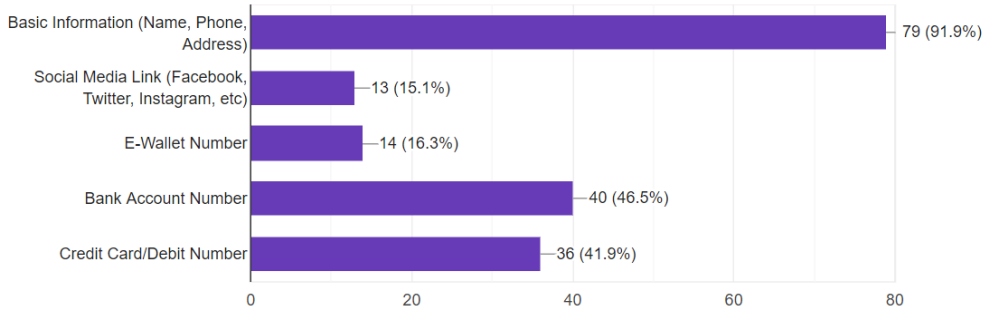
Mini Survey on Consumer Behavior on Using E-Commerce and Digital Payment

Respondents E-Commerce and Digital Payment Preference:

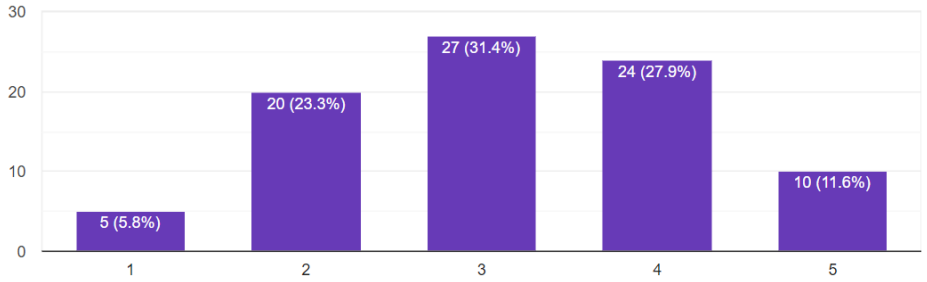
financial service respondents currently use



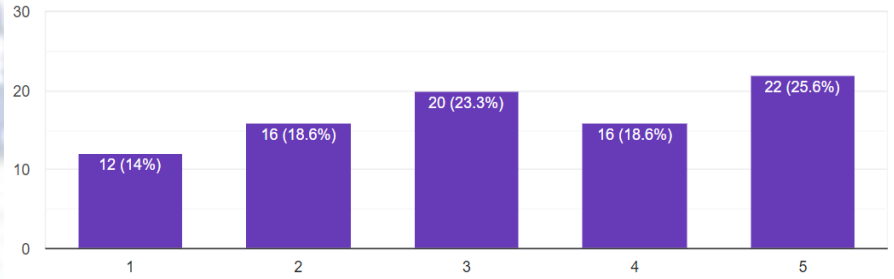
information are required in your e-commerce account or while doing online transaction



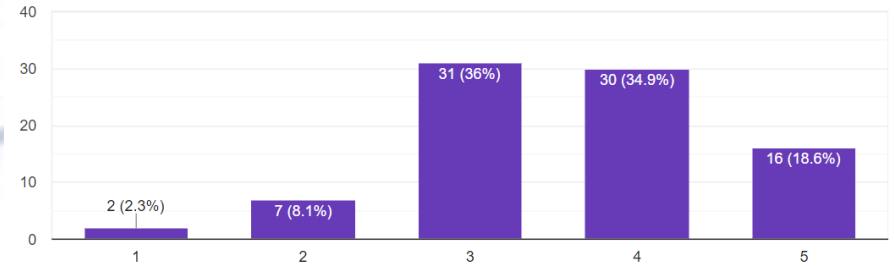
Trust level in E-Commerce



Data Awareness in E-Commerce



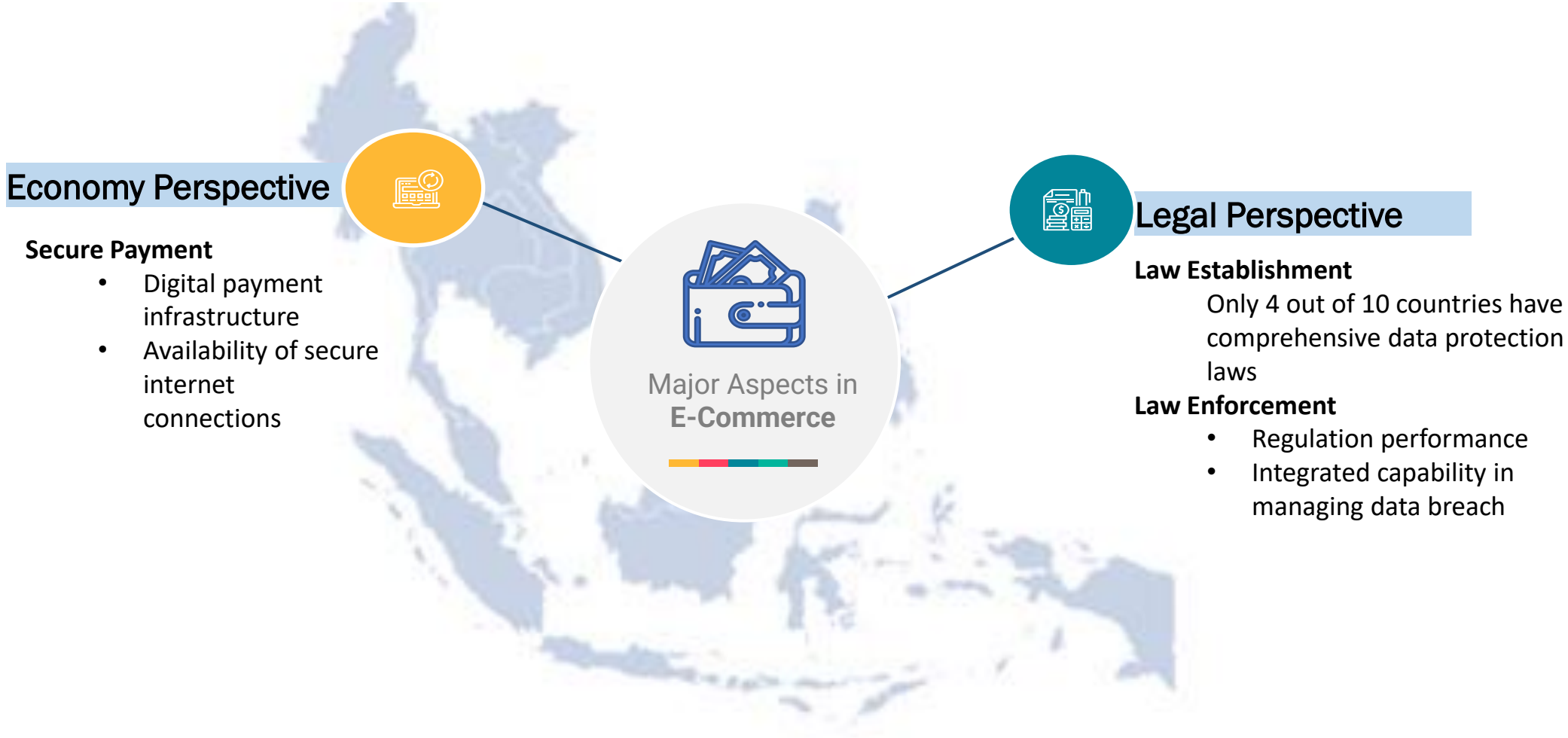
Data Protection Knowledge to Stay Secure in E-Commerce



2 The Importance of Data Protection

“Fear about privacy and the lack of trust continue to be the biggest obstacles to the growth of online commerce”

E-Commerce & Data Protection: The Major Factors



Economy Perspective

Secure Payment

- Digital payment infrastructure
- Availability of secure internet connections

Legal Perspective

Law Establishment

Only 4 out of 10 countries have comprehensive data protection laws

Law Enforcement

- Regulation performance
- Integrated capability in managing data breach

E-Commerce & Data Protection: The Major Factors

Cybersecurity: Preparedness and Commitments

Country/Group	NCSI		GCI		
	Score	Ranking (/100)	Score	Ranking (/175)	Level of commitment
Brunei	38.96	54	0.62	64	medium
Cambodia	n.a.	n.a.	0.16	131	low
Indonesia	19.48	83	0.78	41	high
Lao PDR	16.88	86	0.19	120	low
Malaysia	72.73	11	0.89	8	high
Myanmar	n.a.	n.a.	0.17	128	low
Philippines	31.17	63	0.64	58	medium
Singapore	57.14	32	0.89	6	high
Thailand	n.a.	n.a.	0.79	35	high
Viet Nam	n.a.	n.a.	0.69	50	high
China	38.96	53	0.83	27	high
India	50.65	39	0.72	47	high

GCI = Global Cybesecurity Index, n.a. = not available, NCSI = National Cyvser Security Index.
Source: The author. Based on ITU (2019b).

3 Data Protection Key Challenges

Some Case Studies in Data Protection

14 million alleged Amazon and eBay account details sold online (2021)

13 million records from Lazada Thailand were being offered for sale on an underground trading forum (2020)

Case Study 1: Data leak & Business Guidance from legal Framework

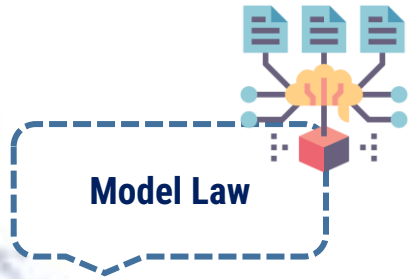
1. No definition of **Data Leak and Data Breach** provided by the Thai PDPA law
2. **Data Leak and Data Breach** mean violation of the Consent Principle

To sum, someone accesses the data or passes it on <u>without proper authorisation</u>

<u>Consent</u> of Data subjects → Processing Personal Data

- Collecting
- Using
- Disclosing
- Editing
- Transferring

Ref: Thailand's Personal Data Protection Act 2019 (PDPA) and European Union's (EU) General Data Protection Regulation 2016/679 (GDPR); Information Commissioner's Office



No Specific Guidance under Thai PDPA; therefore, relying on International Compliance

Recital 85 of the UK GDPR

"A personal data breach may, if not addressed in an appropriate and timely manner, <u>result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.</u>"

What do Business have to do in case of a data leak/breach?

1. Has to notify the supervisory authority without <u>undue delay</u>
2. If the company/organization is a data processor it <u>must notify every data breach to the data controller.</u>
3. <u>Inform the individuals (Clients),</u> while a high risk is occurred
4. Impose the technical and measures <u>to stop and prevent the future data leak</u>

Ref: European Commission, EU GDPR, Information Commissioner's Office

Case Study 2: Bundled Consent (including E-Commerce website in Thailand)

Thongraweewong, Privacy Laws specialist and the Dean of Saint John's University, Thailand.
In his personal interview with the author, he pointed out that bundled consent has been the problem with businesses operating in Thailand and that the agreements concerned may have various clauses, and the consent is bundled up with one or the other clause in the agreement.

Ref: Peeyakorn's Master Thesis; https://diligentcommerce.com/5-gdpr-changes-to-consider-for-your-ecommerce-website/

Guidance for Business under the Thai PDPA and EU GDPR

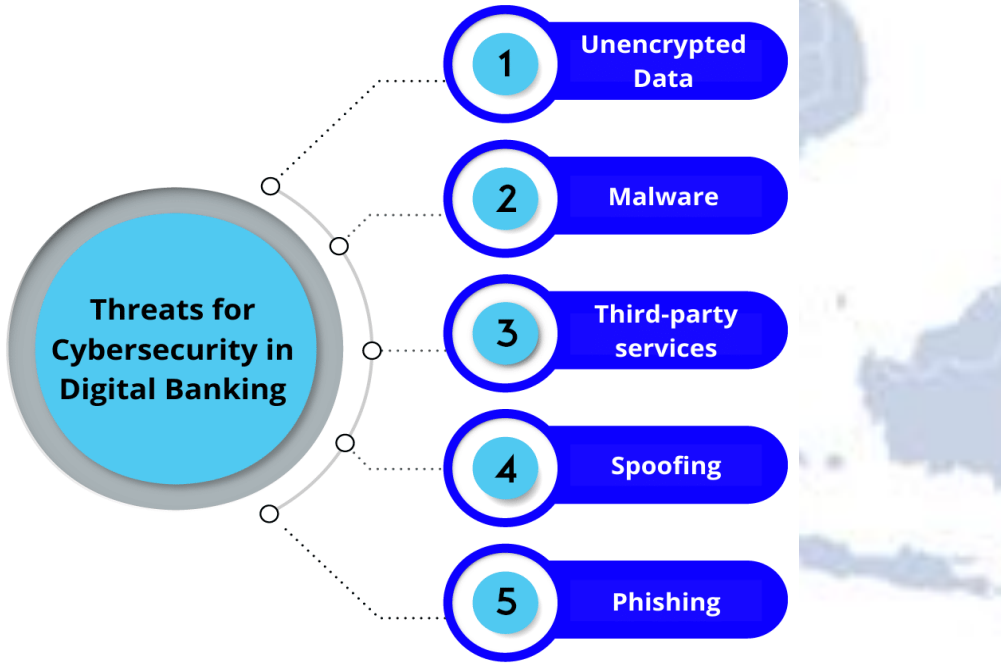
- Unbundled, data needs to be asked for separately for each purpose
- Collecting just "necessary for the performance of Contract" such as a date of birth is not necessary for E-commerce
- Review and update *the privacy policy* on website

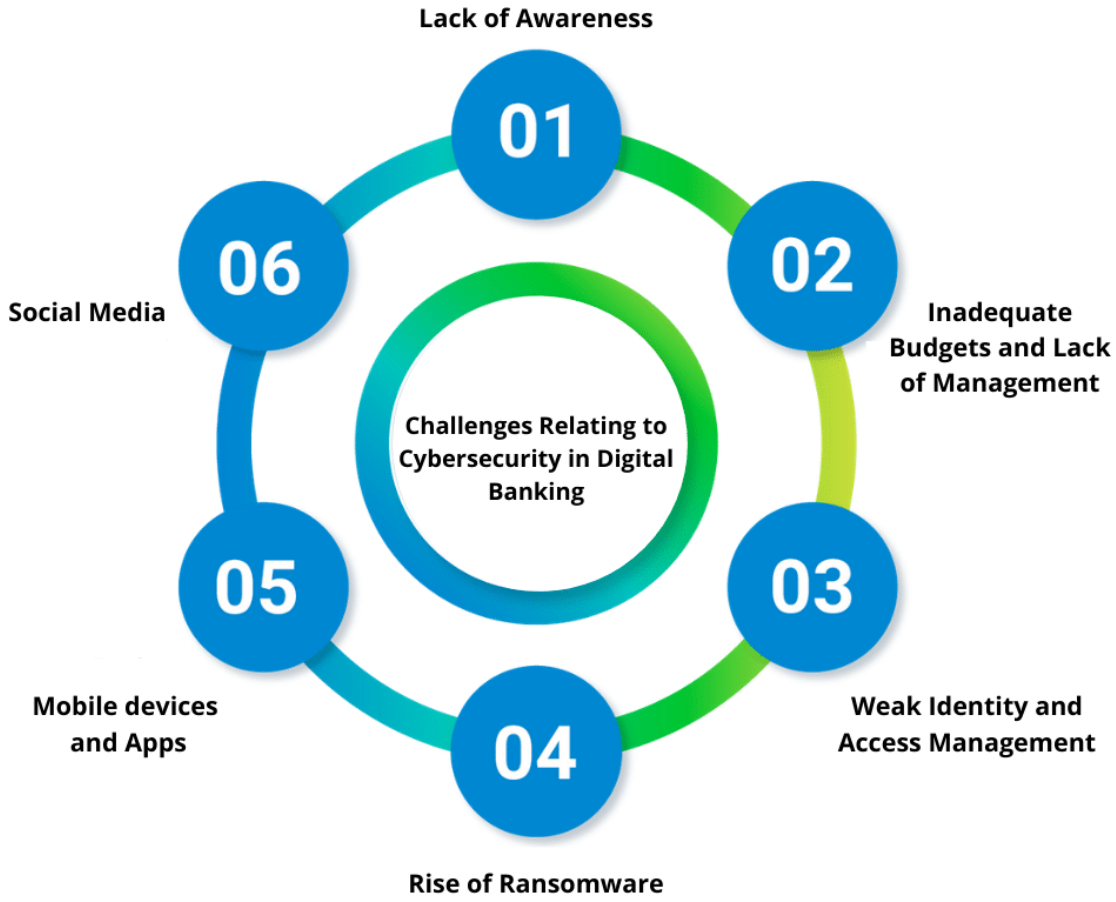
4 Best Practice for Data Protection in E-Commerce

Threats to Cyber Security in Digital Banking

Types of Online Payments in E-Commerce

- Credit/Debit Card Payment
- Bank Transfers
- E-wallet
- Cryptocurrencies
- Mobile Payments





Emerging Technologies in E-Commerce

Blockchain

- Blockchain-powered digital identity programs
- Securing financial transactions.

Internet of Things

- Tracking inventory in real-time
- Temperature-monitoring sensors can maintain optimum temperatures for perishable products.

Artificial Intelligence and Machine Learning

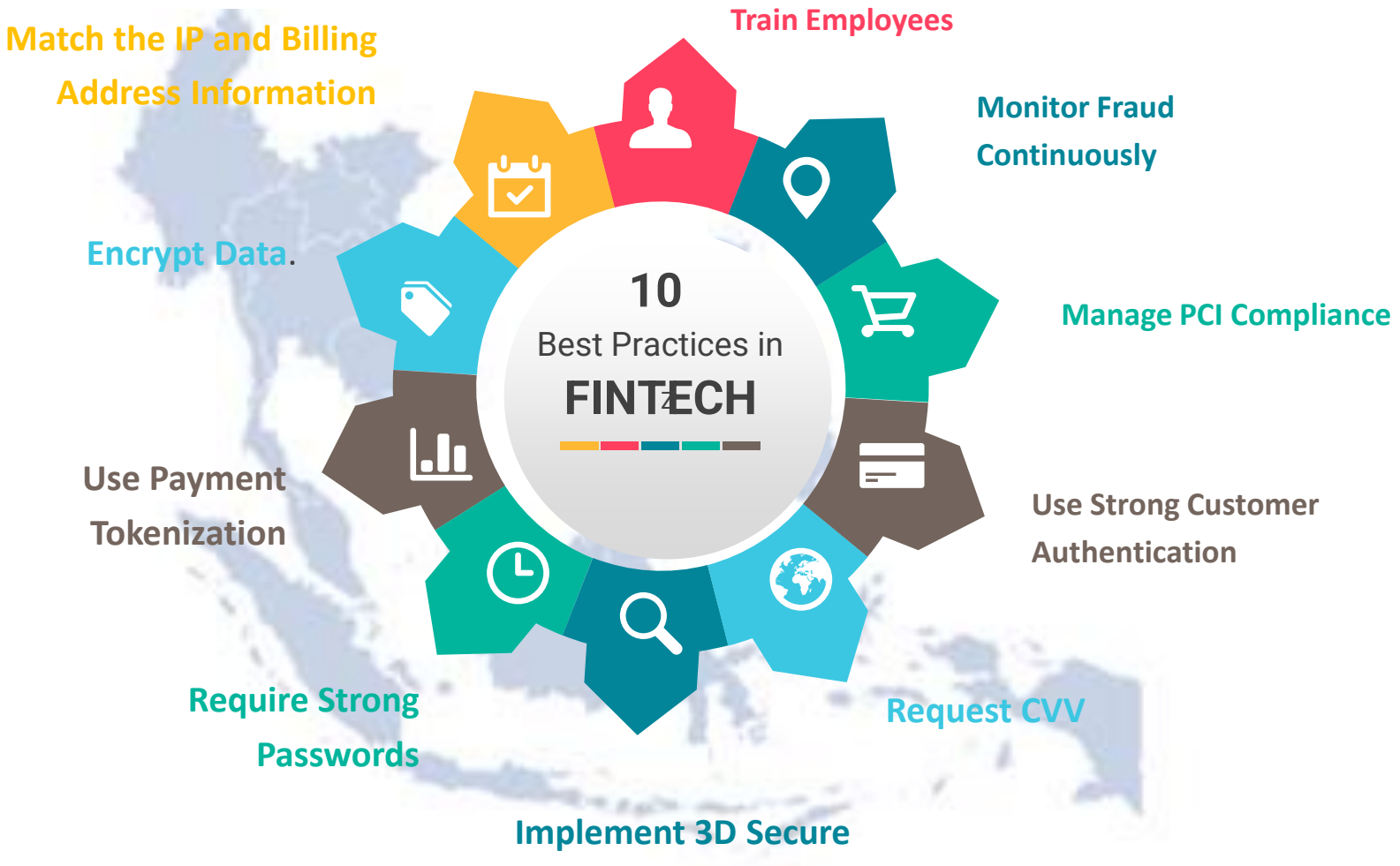
- Predicting Sales
- Market Segmentation
- Product Classification
- Product Recommendation and Search
- Image Recognition (Customer-Customer Platforms)

5G Technology

- Consumer willingness to engage in e-commerce, longer times on e-commerce websites and more purchases online
- consumer enjoyment when engaging in e-commerce-related activities
- vendor effectiveness in activities such as online advertising .

Big Data and Cloud Computing.

Best Practices in Financial Technology for Consumer Security



Best Practices in Financial Technology for Consumer Security

Monitor Fraud Continuously

Merchants need a payment gateway that detects and manages fraud. Built-in fraud monitoring identifies where there may be a real risk of a fraudulent purchase. Businesses can set rules, based on their situation and tolerance for risk, that limit or reject transactions that are deemed too high-risk, or require manual approval before a transaction is completed.

Use Case: Kasikorn Bank uses AI technology to monitor fraud tractions

Request CVV

The Card Verification Value (CVV) can be used to validate card-not-present transactions either on the phone or online. If the credit card numbers have been stolen, asking for information that is only available on the card can help merchants validate the payment.

Use Case: Master Card/VISA Card

Manage PCI Compliance

SSL and TLS – (Transport Layer Security) TLS and (Secure Sockets Layer) are protocols that authenticate and encrypt data when moving on the Internet. Securing transactions with SSL protocols ensure that sensitive information is encrypted and only accessible by the intended recipient.

Require Strong Passwords

Cybercriminals try to access user accounts with frequently used combinations of names, birthdays and dictionary words. Protecting customer accounts with a strong password can add a line of defense. In the event that the customer cannot remember their strong password, there does need to be a “forgot your password” process in place to allow them to access their account.

Use Payment Tokenization

Credit card tokenization de-identifies sensitive payment information by converting it to a string of randomly generated numbers, called a “token.” As a token, the information can be sent through the internet or payment networks to complete payment without being exposed.

Best Practices in Financial Technology for Consumer Security

Match the IP and Billing Address Information

Checking details provided during the transaction can help flag a potentially fraudulent transaction and protect the business before fraud occurs. Address Verification Service (AVS) compares the IP address of the buyer to the billing address of the credit card used to provide assurance that the customer is the cardholder.

Encrypt Data

SSL and TLS – (Transport Layer Security) TLS and (Secure Sockets Layer) are protocols that authenticate and encrypt data when moving on the Internet. Securing transactions with SSL protocols ensure that sensitive information is encrypted and only accessible by the intended recipient.

Use Strong Customer Authentication

SCA is used to reduce fraud and increase online payments security and asks for two or more elements from the use in the authentication process. Something you know (a password or PIN), something you have (a badge or smartphone) or something you are (fingerprints or voice recognition).

Use Case: SCB Easy App (Biometric Verification)

Train Employees

Provide individuals with the knowledge and skills that enable them to recognize and respond appropriately. When the team understands the secure payment process they are better prepared to identify fraudulent activity as it is happening and can prevent information security incidents. Employing these best practices for secure online payment processing is an important component for international ecommerce success.

Implement 3D Secure

3D Secure is a method of authentication set up to protect you from the unauthorized use of cards for online payments. Created by Visa ('Visa Secure') and MasterCard ('MasterCard SecureCode'), it adds an extra level of security to the card acquiring process. 3D Secure 2.0 (3DS 2.0 or 3DS2) is the latest 3D Secure authentication protocol.

Use Case: DBS Bank E-Commerce Payment

5 Strategies and Recommendations for Data Protection in E-Commerce

- ASEAN Data Management Framework
- Model Contract Clauses
- Codes of Conduct
- Group-wide Privacy Binding Corporate Rules
- Private Enforcement Suits and Multilateral Legal Assistance Treaties

Strategies and Recommendations for Data Protection in E-Commerce

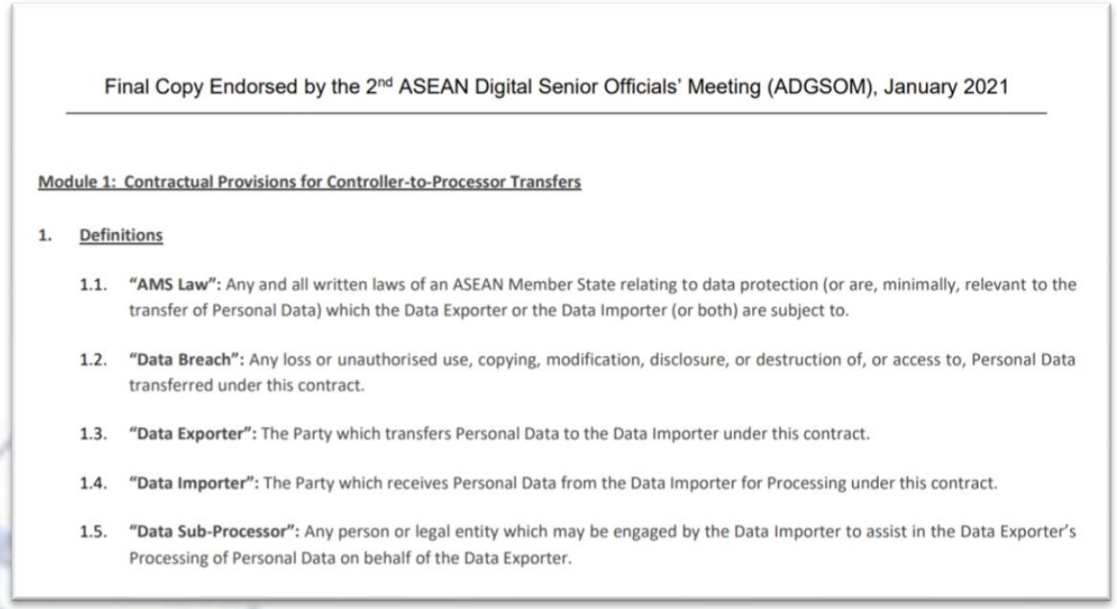
ASEAN Data Management Framework

6 foundational components of the DMF

These 6 foundational components aim to enable the organisation to leverage on a corporate governance structure to define, manage and monitor its data management processes.

1	2	3	4	5	6
Governance and oversight	**Policies and procedural documents**	**Data inventory**	**Impact / Risk assessment**	**Controls**	**Monitoring and continuous improvement**
Provide direction for employees across the organisation in implementing and executing the DMF and oversee the function to confirm it is operating as designed.	Develop data management policies and procedures based on the DMF throughout the data lifecycle, to ensure a clear mandate within the organisation.	Identify and gather the data used and collected as well as storage type, so as to enable understanding of data taxonomy and data purpose.	Assess the impact using different impact categories if confidentiality (C), integrity (I) or availability (A) parameters are compromised.	Design and implement protection controls within the systems according to the categories assigned and data lifecycle.	Monitor, measure, analyse and evaluate the DMF components implemented to keep it up-to-date and optimised.

Model Contract Clauses



Final Copy Endorsed by the 2nd ASEAN Digital Senior Officials' Meeting (ADGSOM), January 2021

Module 1: Contractual Provisions for Controller-to-Processor Transfers

1. Definitions

1.1. **"AMS Law":** Any and all written laws of an ASEAN Member State relating to data protection (or are, minimally, relevant to the transfer of Personal Data) which the Data Exporter or the Data Importer (or both) are subject to.

1.2. **"Data Breach":** Any loss or unauthorised use, copying, modification, disclosure, or destruction of, or access to, Personal Data transferred under this contract.

1.3. **"Data Exporter":** The Party which transfers Personal Data to the Data Importer under this contract.

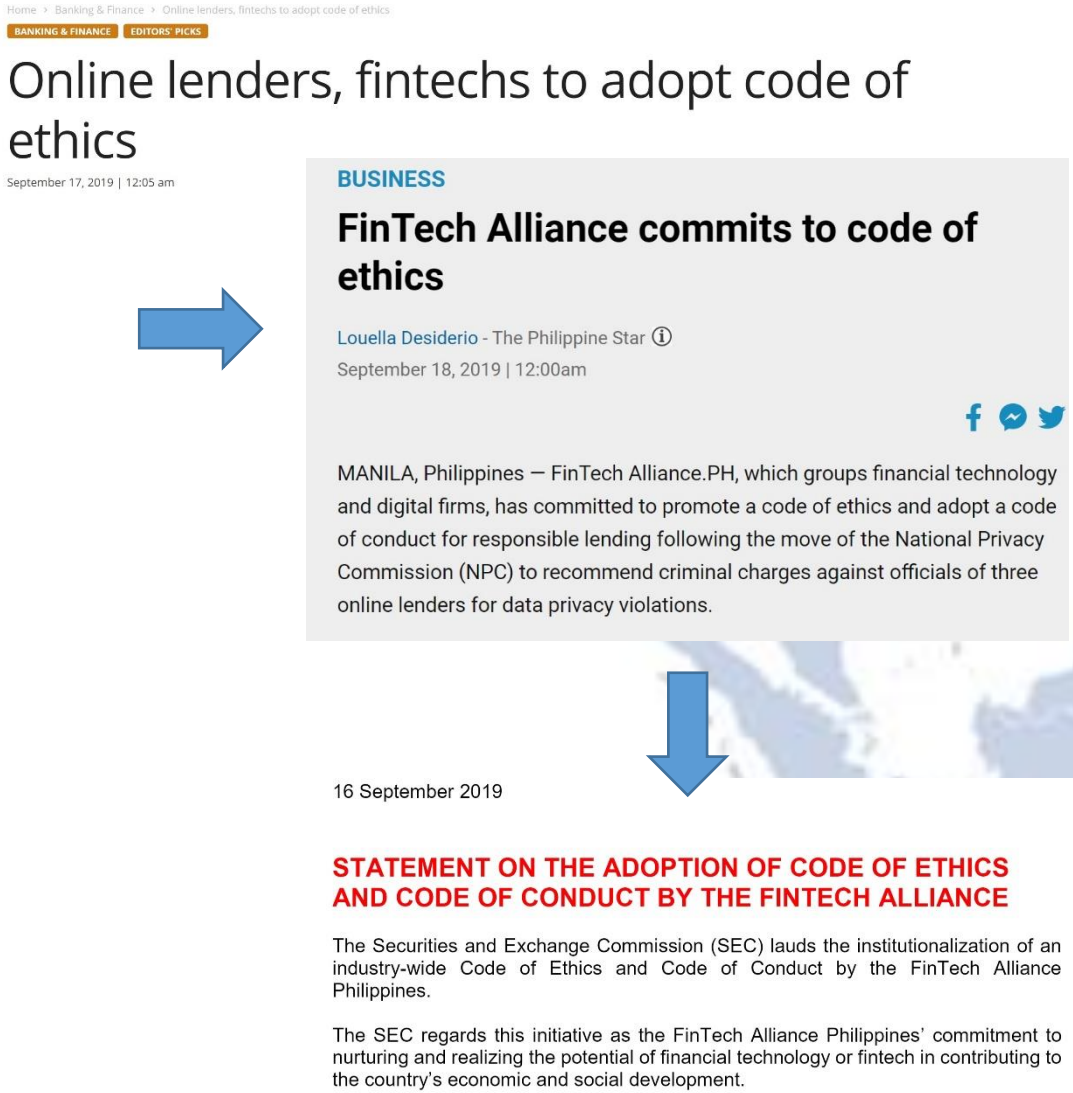
1.4. **"Data Importer":** The Party which receives Personal Data from the Data Importer for Processing under this contract.

1.5. **"Data Sub-Processor":** Any person or legal entity which may be engaged by the Data Importer to assist in the Data Exporter's Processing of Personal Data on behalf of the Data Exporter.

Source: Association of Southeast Asian Nations

Strategies and Recommendations for Data Protection in E-Commerce

Codes of Conduct



Home › Banking & Finance › Online lenders, fintechs to adopt code of ethics

BANKING & FINANCE EDITORS' PICKS

Online lenders, fintechs to adopt code of ethics

September 17, 2019 | 12:05 am

BUSINESS

FinTech Alliance commits to code of ethics

Louella Desiderio - The Philippine Star

September 18, 2019 | 12:00am

MANILA, Philippines — FinTech Alliance.PH, which groups financial technology and digital firms, has committed to promote a code of ethics and adopt a code of conduct for responsible lending following the move of the National Privacy Commission (NPC) to recommend criminal charges against officials of three online lenders for data privacy violations.

16 September 2019

STATEMENT ON THE ADOPTION OF CODE OF ETHICS AND CODE OF CONDUCT BY THE FINTECH ALLIANCE

The Securities and Exchange Commission (SEC) lauds the institutionalization of an industry-wide Code of Ethics and Code of Conduct by the FinTech Alliance Philippines.

The SEC regards this initiative as the FinTech Alliance Philippines' commitment to nurturing and realizing the potential of financial technology or fintech in contributing to the country's economic and social development.

Group-wide Privacy Binding Corporate Rules

Binding Corporate Rules (ASEAN-Adapted)

- Some examples of approved Binding Corporate Rules documentation.
- **eBay** with the Luxemburg DPA as the lead.
- **First Data** with the UK ICO as the lead DPA.
- **HP** with the CNIL as the lead DPA.
- **Intel** with the UK ICO as the lead DPA.
- **JPMorgan Chase** with the UK ICO as the lead DPA

Source: International Association of Privacy Professionals (IAPP)

Strategies and Recommendations for Data Protection in E-Commerce

Private Enforcement Suits and Multilateral Legal Assistance Treaties

Private Enforcement Suits, Will ASEAN follow?

2014

The Right to Be Forgotten (Google v. Spain)

Background | Legal Documents | Additional Resources | EPIC's Related Work | News

Summary

In Google v. Spain, the European Court of Justice ruled that the European citizens have a right to request that commercial search firms, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant. The Court did not say newspapers should remove articles. The Court found that the fundamental right to privacy is greater than the economic interest of the commercial firm and, in some circumstances, the public interest interest in access to Information. The European Court affirmed the judgment of the Spanish Data Protection Agency which upheld press freedoms and rejected a request to have the article concerning personal bankruptcy removed from the web site of the press organization.

2021

Delhi High Court recognises 'Right to be Forgotten' in a suit

ANI | Updated: Aug 26, 2021 00:24 IST

New Delhi [India], August 26 (ANI): In a suit filed by an unnamed actress, the Delhi High Court has upheld and reiterated that 'Right to be Forgotten' and 'Right to be Left Alone' are an essential and inherent part of the Fundamental Right to Privacy.

The bench of Justice Asha Menon in an order passed on Tuesday, also allowed Plaintiff's application seeking protection of the identity and retaining the confidentiality of the proceedings.

"In the circumstances and in view of the fact that the plaintiff is entitled to be left alone and to be forgotten, she is entitled to protection from invasion of her privacy by strangers and anonymous callers on account of such publication/streaming/ transmission of the suit videos by the defendants," noted the court. The Plaintiff actress

Continuing Trend Of Private Enforcement In Other Jurisdictions within their respective territories

Extraterritoriality of Privacy Enforcement

GDPR: This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

Philippine DPA: SEC. 6. *Extraterritorial Application.* – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:

(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;

(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:

Strategies and Recommendations for Data Protection in E-Commerce

Extraterritoriality of Privacy Enforcement

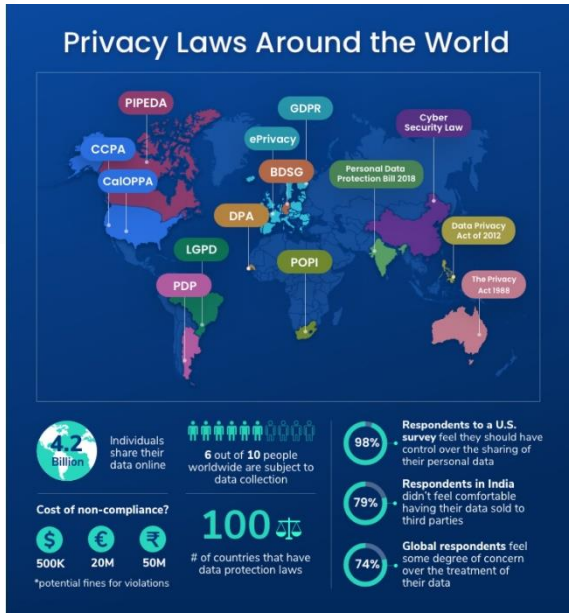
Thailand:
The PDPA has extra-territorial applicability over entities outside Thailand that collect, use, and/or disclose personal data of data subjects who are in Thailand in two situations:

- where the activities of collection, use, and disclosure are related to the offering of goods or services to the data subjects who are in Thailand, irrespective of whether the payment is made by the data subject; or

- where the activities of collection, use, and disclosure are related to the monitoring of the data subject's behaviour, where the behaviour takes place in Thailand

Singapore:
The PDPA applies to all organizations that collect, use and disclose data in Singapore, and the PDPA has extraterritorial effect as it applies to all organizations collecting, using or disclosing personal data from individuals in Singapore (whether or not the company has a physical presence in Singapore).

Extraterritoriality of Privacy Enforcement



There is a need to facilitate data subject's ability to enforce their rights internationally, as unlike laws, data does not respect borders.

Source: Termly

Conclusion

1. ASEAN region is a thriving landscape for e-commerce, with more growth opportunities driven by the pandemic

2. Legal and economic factors play key roles in creating reliable and secure e-commerce landscape;

3. As reflected in the case study (Thailand), consent principle is a critical principle under the Data Protection Framework. Bundled consent creates challenges as consent is acquired while tied to other clause(s) in an agreement;

4. State-of-the-art technologies such as AI/Blockchain can facilitate the implementation of secure digital payment systems for e-commerce;

5. Comprehensive data management framework as well as enforcement of regulations are recommended to strengthen country's data protection capabilities, thus creating a secure environment for e-commerce to thrive