แนวทางการจัดการกับปัญหาการส่งข้อความสั้นหรือโทรศัพท์ที่ไม่พึงประสงค์ (spam) และหลอกลวง (scam) ต่อผู้บริโภคในต่างประเทศ

โดย นางสาวโสภิดา วีรกุลเทวัญ

เกริ่นนำ

การสร้างความรำคาญและการหลอกลวงผู้บริโภคผ่านการส่งข้อความสั้นหรือ ที่เรียกว่า SMS ตลอดจน การโทรศัพท์และการใช้แพลตฟอร์มออนไลน์อื่น ๆ เป็นปรากฏการณ์ระดับโลกที่หน่วยงานภาครัฐของนานาประเทศ ตระหนักและออกมาตรการเพื่อจัดการแก้ไขและหาทางป้องกัน ปัญหาดังกล่าวแบ่งออกได้เป็นสองลักษณะกว้าง ๆ ได้แก่ ลักษณะแรกเป็นการส่งข้อความหรือโทรศัพท์ที่สร้างความรำคาญหรือไม่พึงประสงค์ต่อผู้บริโภค (spam) ลักษณะที่สองเป็นการส่งข้อความหรือโทรศัพท์ที่มุ่งหลอกลวงผู้บริโภค (scam) ลักษณะหลังส่งผลกระทบต่อผู้บริโภคนับตั้งแต่การสูญเสียข้อมูลส่วนบุคคลและเชื่อมโยงเงินทองจำนวนมาก

ข้อมูลจากประเทศเพื่อนบ้านในอาเซียนอย่างสิงคโปร์เมื่อปีพ.ศ.2563[1] พบกรณีที่ประชาชนโดนหลอกลวงจำนวน 15,700 ราย คิดเป็นเงินถึง 201 ล้านเหรียญสิงคโปร์ ซึ่งมีทั้งอีคอมเมิร์ซ เงินกู้ ธนาคารและการล่อลวงทางโซเชียลมีเดีย ข้ามฟากจากฝั่งเอเชียไปทางทวีปยุโรป ในสหราชอาณาจักรมีความรุนแรงไม่น้อยไปกว่ากัน ฤดูร้อนปีพ.ศ.2564 มีรายงานว่าผู้คนที่นั่นเกือบ 45 ล้านคนเผชิญกับข้อความสั้นที่เข้าข่ายหลอกลวงผ่านระบบมือถือหรือการโทรศัพท์เข้ามือถือและโทรศัพท์บ้าน[2] หลาย

ประเทศพบว่ามีการหลอกลวงในรูปแบบที่หลากหลายซับซ้อนมากยิ่งขึ้น โดยเฉพาะอย่างยิ่งในช่วงสถานการณ์การแพร่ระบาดโควิด-19 ในเรื่องนี้ประเทศไทยมีรายงานข่าวและการแชร์เรื่องราวของผู้ประสบภัยไม่แตกต่างกัน แต่ยังไม่พบว่ามีหน่วยงานใดรวบรวมข้อมูลและรายงานความสูญเสียอย่างเป็นทางการ เราจะมาดูกันว่าหน่วยงานภาครัฐในต่างประเทศมีวิธีการจัดการและรับมือต่อปัญหานี้เพื่อคุ้มครองผู้บริโภคในประเทศของพวกเขาอย่างไร

ออสเตรเลีย

ออสเตรเลียมีหน่วยงานกำกับดูแลกิจการด้านการสื่อสารเรียกว่า Australian Communications and Media Authority –ACMA องค์กรแห่งนี้นิยามข้อมูลที่ส่งมายังผู้บริโภคออกเป็นสองส่วน ได้แก่ ข้อมูลทางการตลาดที่ไม่พึงประสงค์ของผู้รับ (spam) กับข้อมูลที่ขายสินค้าหรือบริการผ่านระบบโทรศัพท์หรือส่งข้อความ (telemarket) โดย ACMA มีกฎกติกาที่เรียกว่า the Spam Act 2003 [3]กล่าวคือ ผู้ส่งข้อมูลใด ๆ ที่เป็นการโฆษณาประชาสัมพันธ์การตลาดต้องได้รับการยินยอมจากผู้รับเท่านั้น และต้องส่งรายละเอียดที่อยู่ที่ติดต่อได้ของผู้ส่ง (contact details) มาพร้อมข้อความ เพื่อแจ้งให้ผู้รับมีช่องทางในการหยุดการส่งหากไม่ต้องการได้รับข้อความดังกล่าว หากผู้ส่งข้อความไม่ปฏิบัติตามกติกาดังกล่าว ผู้บริโภคสามารถร้องเรียนมายัง ACMA ได้ ทั้งนี้ Spam rule ใช้บังคับในกรณีที่เป็นข้อความที่เกี่ยวข้องกับการขายสินค้าและบริการ ไม่นับรวมข้อความทางการเมืองและอื่น ๆ ACMA วางแนวทางรับมือเรื่องสแปมสองรูปแบบ ได้แก่ 1.สแปมที่ส่งมาทางโทรศัพท์บ้าน มือถือ และโทรสาร 2.สแปมที่ส่งผ่าน SMS หรือ อีเมล

รูปแบบที่หนึ่ง ACMA มีระบบฐานข้อมูลที่เรียกว่า Do Not Call Register ระบบนี้ถูกสร้างขึ้นเพื่อให้บุคคลและองค์กรสามารถลงทะเบียน ตรวจสอบ และยกเลิกหมายเลขโทรศัพท์บ้าน หมายเลขมือถือและหมายเลขโทรสาร หากไม่ประสงค์ที่จะได้รับข้อมูลเกี่ยวกับสินค้าและบริการใด ๆ เมื่อผู้ใช้โทรศัพท์ได้ลงทะเบียนกับระบบ ผู้ที่ทำหน้าที่ส่งข้อมูลทางการตลาดจะมีเวลา 30 วันในการรับรู้และยกเลิกการส่งข้อความหรือโทรไปยังหมายเลขที่จดทะเบียนดังกล่าว ACMA จึงเป็นหน่วยงานที่ดูแลเรื่องระบบการลงทะเบียน Do Not Call และกำกับดูแลให้เป็นไปตามกฎหมายที่เกี่ยวข้องหลายฉบับ ได้แก่ Do Not Call Register Act 2006, Do Not Call Register Regulations 2017, Telecommunication (Telemarketing and Research Calls) Industry Standard 2017, Fax Marketing Industry Standard 2011

รูปแบบที่สอง กรณีที่ผู้บริโภคได้รับข้อความสั้นหรืออีเมลที่ไม่พึงประสงค์ ซึ่งละเมิดกติกาในการส่งข้อความตามกฎว่าด้วยเรื่องสแปม ผู้บริโภคมีสองทางเลือก คือ 1.ร้องเรียน (complaint) มายัง ACMA ผ่านช่องทางของเว็บไซต์หน่วยงาน หาก ACMA รีวิวเรื่องร้องเรียนแล้วอาจจะติดต่อไปยังผู้ส่งข้อความเพื่อให้แสดงความรับผิดชอบตามกฎหมายในเรื่องสแปม 2.หากผู้บริโภคไม่ประสงค์จะร้องเรียนแต่ต้องการรายงาน (report) เท่านั้น สามารถส่งต่อข้อความสแปมดังกล่าวมายังหมายเลข 0429999888 หรืออีเมล report@submit.spam.acma.gov.au อีเมลนี้เป็นอีเมลเพื่อการรับแจ้งรายงานสแปมโดยมีการตอบรับอีเมลแบบอัตโนมัติ

ภายหลังจากที่ได้รับเรื่องร้องเรียนหรือรายงานจากผู้บริโภค ภารกิจของ ACMA คือการรวบรวมข้อมูลเพื่อวิเคราะห์ปัญหาและประเด็นที่กำลังเกิดขึ้นกับผู้บริโภคและจะแจ้งเตือนไปยังผู้ให้บริการรวมทั้งสืบสวนในกรณีที่เป็นปัญหารุนแรงตลอดจนดำเนินการตามกฎหมาย ทั้งนี้ ACMA จะจัดทำรายงานผลการดำเนินงานในการจัดการกับสแปมและการขายสินค้าและบริการทางไกลโดยมีการเผยแพร่ทุกไตรมาส เช่น ผลการดำเนินการ

ในเรื่องการบล็อคเบอร์โทรหลอกลวงจำนวน 214 ล้านสายในช่วง 7 เดือนภายหลังจากที่ประกาศใช้กฎใหม่, การส่งคำเตือนยังผู้ให้บริการจำนวน 5 แห่งที่ละเมิดกฎ การแจ้งเตือนแก่ผู้บริโภค (consumer alerts) ในประเด็นหลอกลวงแบบใหม่ ๆ เช่น การหลอกลวงเกี่ยวกับวัคซีนโควิด-19 การสั่งลงโทษปรับผู้ให้บริการซึ่งอยู่ภายใต้การกำกับของ ACMA กว่า 2.5 ล้านเหรียญออสเตรเลีย รวมทั้งวิเคราะห์ข้อมูลเรื่องร้องเรียนที่ได้รับและส่งรายงานไปแจ้งแก่ผู้ให้บริการตื่นตัวในการแก้ปัญหา เป็นต้น

สำหรับกรณีที่เป็นการสื่อสารรูปแบบต่าง ๆ ที่เข้าข่ายหลอกลวง (scam) นั้น จะมีหน่วยงานเฉพาะที่ทำหน้าที่ดูแลคือ the Australian Competition and Consumer Commission (ACCC) ซึ่งจัดตั้งแผนกเฉพาะชื่อว่า Scamwatch (https://www.scamwatch.gov.au/) เป็นหน่วยงานของรัฐที่ทำหน้าที่ให้ข้อมูลแก่ประชาชนในเรื่องการหลอกลวงทุกรูปแบบและแนะนำวิธีหลีกเลี่ยงเพื่อป้องกันตนเองจากการตกเป็นเหยื่อ ACCC ทำงานร่วมกับหน่วยงานที่ดูแลเรื่องการคุ้มครองผู้บริโภคและหน่วยงานภาครัฐอื่น ๆ เพื่อสร้างตระหนักแก่ผู้บริโภคเกี่ยวกับรูปแบบวิธีการหลอกลวง แต่ไม่ได้มีหน้าที่ในการให้ความช่วยเหลือทางกฎหมายเป็นรายกรณี ภารกิจของ Scamwatch คือการเผยแพร่เอกสาร ข้อเท็จจริง รายงานประจำปีเกี่ยวกับรูปแบบการหลอกลวงเพื่อให้ประชาชนรู้เท่าทันสถานการณ์ เช่น ในปี 2563 มีผู้รายงานการหลอกลวงมายังเว็บไซต์นี้มากกว่า 400,000 ราย ประเมินความสูญเสียมากกว่า 850 ล้านเหรียญออสเตรเลีย ซึ่งประเภทการหลอกลวงสูงสุดสองเรื่องแรกได้แก่ การหลอกลวงเพื่อลงทุน (investment) และการหลอกรักออนไลน์ (romance) ด้วยแนวคิดของภาครัฐที่มองว่าการป้องกันการหลอกลวงที่ดีที่สุดคือการให้การศึกษาแก่ประชาชนผ่านการเผยแพร่ความรู้ความเข้าใจให้ผู้บริโภคกลุ่มต่าง ๆ มีความตระหนักและเท่าทัน ทำให้องค์กรแห่งนี้มีการผลิตเอกสารและเผยแพร่เพื่อให้การศึกษาแก่ประชาชน ยกตัวอย่างงานเผยแพร่ชิ้นล่าสุดเมื่อเดือนมกราคม 2565 ได้แก่ the Little Black Book of

Scams เนื้อหาประกอบด้วย รูปแบบการหลอกลวงที่พบมากที่สุด วิธีการต่าง ๆ และเครื่องมือที่ผู้หลอกลวงนำมาใช้ สิ่งที่เป็นสัญญาณเตือนให้รู้ว่ากำลังจะเกิดภัยและแนวทางตลอดจนวิธีการป้องกันตนเอง รวมทั้งช่องทางการขอความช่วยเหลือเมื่อตกเป็นเหยื่อ ทั้งนี้ประชาชนสามารถโหลดไฟล์อิเล็กทรอนิกส์จากเว็บไซต์หรือขอให้จัดส่งเป็นแบบฉบับพิมพ์ไปยังที่พักของตนภายในประเทศออสเตรเลียได้ฟรีหรือโทรแจ้งหมายเลข 1300 30250 หรืออีเมล publishing.unit@accc.gov.au โดยเอกสารดังกล่าวจัดทำเป็นภาษาต่าง ๆ จำนวน 11 ภาษาเพื่อรองรับผู้บริโภคทุกกลุ่ม

วิธีการที่น่าสนใจของ Scamwatch คือ การเผยแพร่ข้อมูลที่เท่าทันต่อสถานการณ์การหลอกลวงตลอดจนครอบคลุมไปยังคนทุกกลุ่มด้วยการคำนึงถึงความแตกต่างทางภาษาและกลุ่มผู้สูงอายุ เช่น ในช่วงการแพร่ระบาดโควิด-19 มีรูปแบบการหลอกลวงอย่างไรบ้างก็จะจัดทำเป็น fact sheet เพื่อให้ประชาชนเท่าทันต่อสิ่งที่กำลังเกิดขึ้น การจัดทำรายงานนำเสนอในรูปแบบอินโฟกราฟิกเพื่อให้ประชาชนรับทราบอย่างชัดเจนว่ากำลังเกิดการหลอกลวงรูปแบบใด และเกิดขึ้นกับคนกลุ่มช่วงอายุ เพศ รวมทั้งมีการเผยแพร่คู่มือในกรณีการหลอกลวงที่เกิดขึ้นกับกลุ่มผู้สูงอายุ

Scamwatch ไม่ได้เป็นหน่วยงานที่ให้ความช่วยเหลือผู้บริโภคเป็นรายกรณี ภารกิจหลักคือการสร้างความตระหนักและป้องกันตนเองจากการถูกหลอกลวง หน่วยงานนี้จึงกระตุ้นให้ประชาชนร้องเรียนหรือรายงานปัญหาที่เผชิญทุกรูปแบบของการหลอกลวง โดยผู้บริโภคสามารถส่งรายละเอียดไปยัง https://www.scamwatch.gov.au/report-a-scam เรื่องร้องเรียนและรายงานในฐานข้อมูลจำนวนมาก ทำให้หน่วยงานสามารถจำแนกแยกแยะ วิเคราะห์สถานการณ์อย่างทันท่วงที เช่น รายงานของ Scamwatch แบ่งการหลอกลวงออกเป็น 8 ประเภท แต่ละประเภทระบุชัดเจนว่าประชาชนสามารถไปร้องเรียนหรือขอความช่วยเหลือได้จากหน่วยงานใด ยกตัวอย่าง การจัดแบ่งประเภทการหลอกลวง ได้แก่ 1)

ธนาคาร ให้ประชาชนติดต่อไปยังสถาบันการเงินโดยตรง 2) การแอบอ้างในเรื่องดูแลด้านสุขภาพหรือการดูแลเด็กและการแอบอ้างหน่วยงานของรัฐบาล จะมีหน่วยงานที่ประชาชนสามารถติดต่อไปยังหมายเลขโทรศัพท์ 1800 941 126 3) กรณีอาชญากรรมทางไซเบอร์ ติดต่อไปยัง Reportcyber 4) กรณีการปลอมแปลงและโจรกรรม สามารถติดต่อตำรวจท้องถิ่น 5) กรณีการคุกคามออนไลน์หรือเนื้อหาที่ผิดกฎหมายในเรื่องเพศจะมีหน่วยงานที่เรียกว่า Office of the eSafety Commissioner 6) กรณีสแปม สามารถติดต่อไปยัง ACCC 7) การหลอกลวงที่เกี่ยวข้องกับเรื่องการจ่ายภาษีสามารถติดต่อไปยัง Australian Taxation Office 8) กรณีที่เกี่ยวข้องกับการลงทุนหรือการเงิน ติดต่อไปยังหน่วยงาน Australian Securities and Investments Commission เป็นต้น

สิงคโปร์

สิงคโปร์มีหน่วยงาน Infocomm Media Development Authority-IMDA ทำหน้าที่กำกับดูแลผู้ให้บริการด้านโทรคมนาคม สำหรับการส่งข้อความเพื่อเสนอขายสินค้าหรือบริการซึ่งผู้รับไม่ได้ขอให้ส่ง (Unsolicited communication)[4] หรือที่เรียกว่า สแปม นั้นในประเทศสิงคโปร์มีกฎหมายสองฉบับในการกำกับดูแลเรื่องนี้ ได้แก่ กฎหมายการควบคุมสแปม (the Spam Control 2007) และ กฎหมายคุ้มครองข้อมูลส่วนบุคคล (the Personal Data Protection Act 2012-PDPA) ซึ่งมีบทบัญญัติหนึ่งว่าด้วย การห้ามโทร หรือ Do Not Call –DNC

กฎหมายการควบคุมสแปม จะกำหนดแนวทางสำหรับผู้ส่งข้อความเพื่อเสนอขายสินค้าหรือบริการว่าต้องได้รับความยินยอมจากผู้บริโภคล่วงหน้า (opt-in) ต้องมีการระบุชื่อที่อยู่ของบริษัทในข้อความนั้น ต้องมีการระบุตัวอักษร ADV ที่ต้นข้อความทางการตลาดเพื่อให้ผู้บริโภคได้รับทราบอย่างชัดเจน และต้องมีช่องทางเพื่อบอกเลิกรับข้อความ (opt-out) สำหรับผู้บริโภค เช่น มีลิงค์สำหรับคลิกเพื่อยกเลิกการรับข้อความ แจ้งหมายเลข

โทรศัพท์หรือการส่งข้อความเพื่อขอยกเลิกการบอกรับ เป็นต้น ดังนั้นเมื่อประชาชนประสบปัญหาจากการได้รับข้อความสแปมรูปแบบต่าง ๆ คำแนะนำของ IMDA คือให้ติดต่อโดยตรงกับบริษัทที่ส่งข้อความทางการตลาดเหล่านั้นเพื่อให้ลบที่อยู่ของตนออกจากฐานข้อมูลของบริษัท เนื่องจากการส่งอีเมลล์หรือข้อความที่ส่งผ่านทางโทรศัพท์มือถือซึ่งเป็นการโฆษณาผลิตภัณฑ์และบริการที่ส่งมายังผู้รับในวงกว้างโดยไม่ผ่านการอนุญาตหรือยินยอมจากผู้รับนั้น ผู้ส่งมีความผิดเป็นค่าปรับเป็นรายข้อความ ๆ ละ 25 เหรียญสิงคโปร์ โทษปรับสูงสุดถึงหนึ่งล้านเหรียญ

สำหรับการขายสินค้าและบริการทางโทรศัพท์ (telemarketing) เป็นกิจกรรมที่อยู่ภายใต้การกำกับดูแลของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (the Personal Data Protection Commission-PDPC) โดยผู้บริโภคจะได้รับการคุ้มครองภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (the Personal Data Protection Act 2012-PDPA) ซึ่งมีบทบัญญัติหนึ่งว่าด้วย การห้ามโทร หรือ Do Not Call –DNC บทบัญญัตินี้กำหนดห้ามองค์กรต่าง ๆ ส่งข้อความทางการตลาดไม่ว่าในรูปแบบของเสียง ข้อความหรือส่งแฟกซ์ไปยังหมายเลขโทรศัพท์ในสิงคโปร์ไม่ว่าจะเป็นเบอร์มือถือ โทรศัพท์บ้าน ที่พักอาศัยหรือธุรกิจที่ลงทะเบียนไว้กับ DNC ดังนั้น DNC Registry[5] จึงเป็นฐานข้อมูลของประเทศซึ่งผู้ใช้บริการโทรศัพท์สามารถลงทะเบียนแจ้งความจำนงค์ว่าไม่ต้องการรับสายหรือข้อความได้สามลักษณะ ได้แก่ No voice, No text, No fax การลงทะเบียนในฐานข้อมูลนี้ทำได้สามวิธีคือ ลงทะเบียนผ่านทางเว็บไซต์ การลงทะเบียนทางเอสเอ็มเอสโดยส่งข้อความไปยังหมายเลข 78771 และทางโทรศัพท์ ขณะเดียวกันองค์กรหรือหน่วยงานที่ต้องการทำการตลาดผ่านการส่งข้อความสั้นหรือโทรศัพท์ก็จำเป็นต้องเข้าไปตรวจสอบจากฐานข้อมูล ทั้งนี้องค์กรหรือหน่วยงานที่จะเข้าไปตรวจสอบจะต้องจดทะเบียนกับ Corppass ซึ่งเป็นระบบของรัฐที่กำกับการเข้าถึงบริการทางอิเล็กทรอนิกส์ต่าง ๆ

สำหรับกรณีการหลอกลวงผู้บริโภค ในสิงคโปร์มีการจัดตั้งหน่วยงานชื่อ Scam Alert อยู่ภายใต้ the National Crime Prevention Council เป็นองค์กรไม่แสวงหากำไรซึ่งเกิดขึ้นจากความร่วมมือของภาคเอกชนและประสานงานร่วมกับตำรวจเพื่อสร้างความตระหนักในเรื่องภัยอาชญากรรมรูปแบบต่าง ๆ แนวคิดขององค์กรนี้เห็นว่าวิธีรับมือกับการหลอกลวงที่ดีที่สุดคือการเรียนรู้ว่ามีสัญญาณที่กำลังพาเราเข้าสู่กระบวนการหลอกลวงเพื่อจะได้ป้องกันตนเองได้ทันเวลา หากโดนหลอกลวงและต้องการความช่วยเหลือสามารถติดต่อไปที่หมายเลข 1800-7722-6688 ผู้บริโภคสามารถเข้ามาติดตามรูปแบบใหม่ล่าสุดเกี่ยวกับการหลอกลวงได้ที่เว็บไซต์ www.scamalert.sg โดยเว็บไซต์นี้จะจัดแบ่งประเภทการหลอกลวงที่เกิดขึ้น-แนะนำวิธีการป้องกันและมีตัวอย่างเรื่องราวที่ทำให้ผู้อ่านเกิดความเท่าทัน ได้แก่ การหลอกลวงในเรื่องการซื้อขายออนไลน์ (online purchase scam) หลอกรักออนไลน์ (Internet love online) การแอบอ้างหรือปลอมแปลงที่มา (impersonation scam) การหลอกลวงเกี่ยวกับการลงทุน (investment scam) การหลอกลวงที่มีการแลกเปลี่ยนในเรื่องเพศ (credit –for-sex scam) การทำสื่อในการเตือนภัยของ Scam Alert มีการนำเสนอเนื้อหาหลายรูปเพื่อการเผยแพร่ เช่น การทำโปสเตอร์ในประเด็นใหม่ ๆ ที่มีการหลอกลวง เช่น การหลอกลวงโดยอ้างเรื่องการจ้างงาน เรื่องการให้กู้เงิน การทำคลิปวิดีโอสั้น ทั้งที่เป็นภาษาจีนกลางและภาษาอังกฤษ และสนับสนุนให้ประชาชนที่โดนหลอกลวงแบ่งปันเรื่องราวที่ตนเองประสบ นอกจากนี้ the National Crime Prevention Council ยังจัดทำแอปพลิเคชั่นชื่อ Scamshield เพื่อช่วยกรองการโทรเข้าและการรับข้อความสั้นที่ไม่พึงประสงค์ ทั้งนี้แอพดังกล่าวยังคงใช้ได้เฉพาะมือถือในระบบ iOS เท่านั้น[6]

ในช่วงปลายปี พ.ศ.2564 มีปัญหาการหลอกลวงเงินด้วยการส่งข้อความสั้นแจ้งว่าหมายเลขบัญชีธนาคารของผู้ใช้มีปัญหาและขอให้กดลิงค์เว็บไซต์ปลอมของธนาคารและใส่รหัสเพื่อเข้าไปตรวจสอบในบัญชี

ออนไลน์ หรือที่รู้จักกันว่า Smishing เป็นปัญหาแพร่ระบาดในสิงคโปร์ มีรายงานว่า ลูกค้าธนาคาร OCBC ตกเป็นเหยื่อมากถึง 790 ราย สูญเงินไปราว 13.7 ล้านเหรียญสิงคโปร์ รัฐมนตรีด้านการสื่อสารและสารสนเทศของสิงคโปร์วางมาตรการในการรับมือหลากหลายวิธี[7] ดังต่อไปนี้

1) การบล็อคเว็บไซต์ (website blocking) โดยตำรวจและ IMDA ทำงานอย่างใกล้ชิดกับผู้ให้บริการอินเทอร์เน็ตเพื่อบล็อคเว็บไซต์ต้องสงสัย 500 เว็บไซต์ในปีพ.ศ.2563 และอีก 12,000 เว็บไซต์ ในปีถัดมา

2) การบล็อกการโทรเข้าจากต่างประเทศที่เป็นสายที่ต้องสงสัยเข้าข่ายหลอกลวง ซึ่งมีการใช้ปัญญาประดิษฐ์ในการคัดกรองและให้บริษัทโทรคมนาคมเตือนผู้บริโภค (consumer alert) เมื่อมีสายเข้าจากต่างประเทศด้วยการเพิ่มเครื่องหมาย + หน้าหมายเลขเพื่อป้องกันการรับสายที่ปลอมแปลงว่าเป็นการโทรจากเบอร์ท้องถิ่น

3) การจัดทำโครงการนำร่องเพื่อให้ลงทะเบียนระบุตัวตนของผู้ส่งข้อความสั้น (the pilot SMS sender ID protection registry) โดย IMDA ร่วมกับธนาคารกลางของสิงคโปร์ (the Monetary Authority of Singapore) ให้ธนาคารต่าง ๆ เข้าร่วมโครงการดังกล่าว

4) การศึกษาความเหมาะสมในการกำหนดให้ผู้ให้บริการ SMS และบริษัทโทรคมนาคมตรวจสอบผู้ส่งข้อความสั้นในระบบการลงทะเบียน ทำให้ข้อความสั้นที่มาจากผู้ส่งที่ปลอมแปลงตัวตนไม่สามารถส่งมายังผู้บริโภคได้เนื่องจากรายละเอียดของผู้ส่งไม่ตรงกับข้อมูลที่บันทึกไว้ โดยทุกองค์กรที่ต้องการส่ง SMS มายังผู้ใช้บริการโทรศัพท์ในสิงคโปร์จะต้องมีหมายเลขประจำตัวขององค์กรที่รัฐบาลออกให้ (a valid Unique Entity Number-UEN) เพื่อช่วยตำรวจในการสืบสวนคดีหากเกิดการหลอกลวงขึ้น ทั้งนี้รัฐบาลสิงคโปร์ยังอยู่ระหว่างการศึกษาก่อนการตัดสินใจบังคับใช้

สหราชอาณาจักร

สหราชอาณาจักรมีหน่วยงานกำกับดูแลด้านสื่อและโทรคมนาคมเรียกว่า Ofcom องค์กรแห่งนี้ได้จัดแบ่งการส่งข้อความสั้นหรือโทรศัพท์ในระบบมือถือและโทรศัพท์บ้านออกเป็นสองลักษณะ ได้แก่ 1) การส่งข้อความสั้นหรือโทรที่ไม่พึงประสงค์ (spam) และ 2) การส่งข้อความหรือโทรเพื่อหลอกลวง (scam) แต่ละลักษณะมีวิธีการจัดการกับปัญหาแตกต่างกันดังนี้

ลักษณะแรก การส่งข้อความสั้นหรือโทรที่ไม่พึงประสงค์ หรือที่เรียกว่า spam texts นั้น จะมีหน่วยงานที่กำกับดูแลเรื่องนี้ได้แก่ the Information Commissioner's Office (ICO) ทำหน้าที่กำกับกติกาต่าง ๆ เกี่ยวกับ spam texts แก่หน่วยงานที่ส่งข้อความ ดังนั้นหากผู้บริโภคได้แจ้งไปยังผู้ส่งข้อความว่าไม่พึงประสงค์จะรับข้อความใด ๆ แล้วยังคงได้รับอีก สามารถร้องเรียนมายัง ICO สามวิธี ได้แก่ ทางโทรศัพท์ 0303 123 1113 หรือร้องเรียนผ่าน เว็บไซต์ ICO หรือส่งไปรษณีย์มายังหน่วยงานแห่งนี้ สำหรับผู้บริโภคที่ไม่ประสงค์จะรับโทรศัพท์ใด ๆ ที่เป็นการแจ้งขายสินค้าและบริการสามารถลงทะเบียน หรือบริการ Do Not Call สามารถแจ้งมายังหน่วยงานชื่อ Telephone Preference Service ด้วยการลงทะเบียนผ่านทางเว็บไซต์ https://www.tpsonline.org.uk/ ทั้งนี้การโทรศัพท์ไปยังหมายเลขบ้านหรือมือถือที่ลงทะเบียนไว้ว่าไม่ประสงค์รับข้อความทางการตลาดใด ๆ ถือเป็นการกระทำที่ผิดกฎหมายของสหราชอาณาจักรหรือกล่าวอีกแบบหนึ่งก็คือบริษัทการตลาดใด ๆ จะโทรศัพท์หาลูกค้าไม่ว่าจะเป็นการติดต่อไปยังมือถือหรือโทรศัพท์บ้านจะต้องได้รับการยินยอมจากเจ้าของหมายเลขดังกล่าวแล้วเท่านั้น กฎหมายที่กำกับดูแลในเรื่องนี้คือ the Privacy and Electronic Communications (EC Directive) Regulation 2003 [8]

ลักษณะที่สอง การส่งข้อความสั้นหรือโทรศัพท์ที่เข้าข่ายหลอกลวง (scam) Ofcom เปิดให้มีหมายเลขโทรศัพท์ 7726 เพื่อให้ผู้บริโภคสามารถรายงานเมื่อพบว่ามีความผิดปกติที่เข้าข่ายการหลอกลวง เหตุที่เลือกหมายเลข 7726 เนื่องจากสะกดมาจากคำว่า SPAM บนแป้นพิมพ์ของโทรศัพท์เพื่อให้ง่ายแก่การจดจำ วิธีการรายงาน Ofcom ได้นำเสนอเป็นคลิปวิดีโอสั้นสำหรับมือถือทั้งระบบ iOS และ Android โดยแบ่งออกเป็นการรายงานในรูปแบบข้อความสั้นและรายงานโทรศัพท์ ความน่าสนใจในการทำงานของ Ofcom คือการรวบรวมข้อมูลที่ได้รับจากการร้องเรียนและนำมาใช้สื่อสารกับสาธารณะเพื่อให้ประชาชนเท่าทันการหลอกลวงที่มีรูปแบบเปลี่ยนแปลงตลอดเวลา เช่น การหลอกลวงในช่วงสถานการณ์แพร่ระบาดโควิด-19 มีการส่งข้อความสั้นหรือโทรศัพท์โดยอ้างว่ามาจากหน่วยงานรัฐบาล หรือองค์การอนามัยโลก เป็นต้น ข้อความสั้นหรือสายโทรศัพท์เหล่านี้อาจเสนอในเรื่องการทดสอบไวรัสโควิดแก่ผู้บริโภค การดูแลหรือการให้ความช่วยเหลือทางการแพทย์ หากผู้รับสายหรือข้อความสั้นเผลอไผลไปสนทนาด้วย อาจตกอยู่ในความเสี่ยงที่จะให้ข้อมูลส่วนบุคคล การเงิน หรือโดนหลอกโอนเงิน เป็นต้น Ofcom จะนำเรื่องราว รูปธรรมที่เข้าข่ายการหลอกลวงมานำเสนอแก่สาธารณะ และเปิดให้ผู้บริโภคสามารถรับข้อมูลเกี่ยวกับสถานการณ์ที่พึงรับรู้ไว้เพื่อป้องกันตนเองทางอีเมล

สำหรับการหลอกลวงที่เป็นการฉ้อโกงหรืออาชญากรรมไซเบอร์ ผู้บริโภคจะได้รับการแนะนำให้ติดต่อไปยัง Action Fraud https://www.actionfraud.police.uk/ ซึ่งเป็นศูนย์ที่รับรายงานการฉ้อโกงและอาชญากรรมไซเบอร์เป็นการเฉพาะ เนื่องด้วยการติดตามสถานการณ์ส่งผลกระทบแก่ผู้บริโภคอย่างใกล้ชิด ทำให้ Ofcom เสนอรูปแบบการหลอกลวงใหม่ ๆ เช่น การโทรศัพท์ที่ไม่มีเสียงพูดจากต้นทาง (silent calls) กล่าวคือ เมื่อปลายทางรับโทรศัพท์แล้วแต่กลับไม่มีปฏิกริยาใด ๆ จากต้นทางที่เป็นฝ่ายโทรมา การปลอมแปลงหมายเลขผู้โทร (caller ID

spoofing) หรือการใช้เทคโนโลยี Voice over IP (VoIP) ส่งผลให้การโทรศัพท์มายังผู้รับอาจเกิดขึ้นได้จากทั่วโลก ในเรื่องนี้ Ofcom แนะนำวิธีป้องกันตนเองด้วยการวางสายโดยไม่ให้ข้อมูลใด ๆ อย่างไรก็ตามหากเกิดความพลาดพลั้งขึ้นให้รายงานเรื่องดังกล่าวกับหน่วยงานตำรวจ หรือติดต่อไปยัง Action Fraud หมายเลข 0300 123 2040 หรือเว็บไซต์ www.actionfraud.police.uk

โดยสรุป Ofcom นอกเหนือจากการให้ข้อมูลรูปแบบการหลอกลวงที่มีความเปลี่ยนแปลงตลอดเวลาแก่ผู้บริโภคเพื่อให้เท่าทันต่อพลวัตดังกล่าวแล้ว ยังนำเสนอช่องทางการรายงานดังนี้ 1.ส่งอีเมล report@phishing.gov.uk 2. กรณีที่ได้รับข้อความสั้นให้ส่งต่อไปยังหมายเลข 7726 โดยไม่ต้องเสียเงิน 3.กรณีที่ตกเป็นเหยื่อจากการหลอกลวง ให้รายงานไปยัง Action Fraud ด้วยการโทรไปที่ 0300 123 2040 หรือไปที่ www.actionfraud.police.uk

สหรัฐอเมริกา

ในสหรัฐฯ เรื่องนี้หนักหน่วงไม่แพ้กัน ดูได้จากการร้องเรียนของผู้บริโภคที่ส่งมายังหน่วยงานกำกับดูแลด้านการสื่อสารของประเทศนี้ที่เรียกว่า FCC หรือ Federal Communications Commission พบว่ามีสแปมบริการโทรและตอบรับอัตโนมัติ หรือ Robocall ส่งถึงผู้บริโภคเกือบ 4,000 ล้านสายต่อเดือนในปี 2563 แม้แต่ Jessica Rosenworcel ประธานหญิงแห่ง FCC ก็หนีไม่พ้นจากสายอัตโนมัติทำนองนี้เช่นกัน[9] FCC มีหน้าที่คุ้มครองผู้บริโภคและธุรกิจจากข้อความทางอิเล็กทรอนิคส์เชิงพาณิชย์ที่ไม่พึงประสงค์ ซึ่งส่งมาทางโทรศัพท์มือถือ (unwanted mobile service commercial messages) อำนาจหน้าที่ดังกล่าวอยู่ภายใต้กฎหมาย CAN-SPAM Act 2003

ในสหรัฐฯรับมือกับเรื่องนี้ด้วยการประสานความร่วมมือระหว่างสองหน่วยงาน ได้แก่ FCC และหน่วยงานด้านคุ้มครองผู้บริโภค FTC -

Federal Trade Commission Protecting America's Consumers ในปี 2563 สองหน่วยงานนี้ได้ออกจดหมายร่วมระหว่างองค์กรไปยังผู้ให้บริการ Voice over Internet Protocol (VoIP) ในแคมเปญจ์ต่อต้านการขายสินค้าและบริการทางโทรศัพท์ที่ผิดกฎหมาย (illegal telemarketing) โดยเฉพาะการใช้ช่องทาง VoIP เพื่อหลอกลวงประชาชนในช่วงการแพร่ระบาดโควิด-19 นอกจากนี้ FCC ยังสั่งลงโทษปรับผู้ประกอบการที่ขายบริการด้านประกันสุขภาพโดยใช้การโทรแบบอัตโนมัติถึง 1,000 ล้านสายอัตโนมัติ บริษัทแห่งนี้ถูกปรับเป็นเงิน 225 ล้านเหรียญสหรัฐซึ่งสูงสุดในประวัติศาสตร์ของ FCC[10] และในปีพ.ศ.2564 FCC ออกจดหมายเตือนไปยังบริษัทโทรคมนาคมหลายแห่งเพื่อเตือนให้ยุติการให้บริการแก่ลูกค้าที่ใช้การโทรอัตโนมัติผิดกฎหมายไปยังผู้บริโภคภายใน 48 ชั่วโมง และรายงานกลับมายัง FCC ภายใน 14 วัน ถ้ายังทำเพิกเฉย ทาง FCC อาจถูกถอนออกจากการลงทะเบียนผู้ให้บริการเสียง[11]

นอกเหนือจากมาตรการในการเตือนและสั่งปรับผู้ให้บริการที่ทำผิดกฎหมายแล้ว FCC ให้ความสำคัญกับการวิเคราะห์ข้อมูลจากเรื่องร้องเรียนเพื่อให้ความรู้แก่ผู้บริโภคเพื่อให้เข้าใจรูปแบบการหลอกลวงใหม่ ๆ รวมทั้งแนวทางการรับมือเมื่อเกิดเหตุ ยกตัวอย่างเช่น การรวบรวมอภิธานศัพท์ที่เกี่ยวข้องกับการหลอกลวงสารพัดแบบ (scam glossary) เพื่อให้ข้อมูลแก่ประชาชนสามเรื่องสำคัญ ได้แก่ 1) สแกมแต่ละแบบเกิดขึ้นอย่างไร 2) ผู้บริโภคควรจะรับรู้เท่าทันในแง่มุมใด และ 3) ควรทำอย่างไรเมื่อเกิดเหตุกับตน ข้อมูลที่นำเสนอเหล่านี้เป็นการสังเคราะห์มาจากเรื่องร้องเรียนที่รายงานมายัง FCC ยกตัวอย่างปัญหาใหญ่ในสหรัฐฯ คือ การปลอมแปลงเพื่อหลอกลวงให้ผู้บริโภคเข้าใจผิดหรือปกปิดที่มาของต้นสาย (spoofing) สแกมเมอร์จะหลอกลวงว่าหมายเลขที่ติดต่อเข้ามาเป็นเบอร์ในท้องถิ่น หรือปลอมแปลงหมายเลขว่ามาจากบริษัทหรือหน่วยงานรัฐที่ผู้รับรู้จักหรือเห็นว่าน่าเชื่อถือ ถ้าหากผู้รับตอบรับสายต้นทางก็จะสร้างบทสนทนาในการหลอกล่อเรื่องเงินทองหรือข้อมูลส่วน

บุคคลที่มีผลต่อการฉ้อโกง จากข้อมูลล่าสุด scam glossary รวบรวมรูปแบบของสแกมมากกว่า 60 รูปแบบ และมีการจัดเผยแพร่เป็นภาษาต่างประเทศรวม 6 ภาษา ได้แก่ อังกฤษ สเปน จีน เกาหลี ตากาล็อค และเวียดนาม

FCC รับร้องเรียนปัญหาที่ผู้บริโภคได้รับผลกระทบจากการรับสายหรือข้อความไม่พึงประสงค์แต่เป็นการรวบรวมเพื่อมาทำการวิเคราะห์และออกมาตรการหรือนโยบายรวมถึงบังคับใช้กับผู้ประกอบการ ไม่ได้เป็นการแก้ไขปัญหากับผู้บริโภคเป็นรายกรณี FCC จัดทำแนวทางสำหรับผู้บริโภคเพื่อหยุดสายโทรและข้อความไม่พึงประสงค์ (unwanted robocalls and text) ซึ่งรวมถึงสายที่ปลอมแปลงต้นทางและผิดกฎหมาย (illegal and spoofed robocalls) ทุกรูปแบบ โดยมีข้อแนะนำและเตือนภัยต่าง ๆ เช่น ไม่รับโทรศัพท์จากหมายเลขที่ไม่รู้จักหรือหากเผลอไปรับสายให้รีบวางสายทันทีอย่าได้ไปสนทนาด้วย ผู้บริโภคควรรู้ว่าถึงแม้หมายเลขที่แสดงหน้าจอว่าเป็นหมายเลขในท้องถิ่นแต่ว่าสายที่เรียกเข้าอาจไม่ได้เป็นผู้โทรจากท้องถิ่นก็เป็นได้ อย่าให้ข้อมูลส่วนบุคคลใด ๆ เป็นต้น ทาง FCC แนะนำให้พูดคุยกับบริษัทเพื่อเรียนรู้ในเรื่องแอปพลิเคชั่นหรือเครื่องมือในการบล็อคเบอร์โทรที่ไม่พึงประสงค์ รวมทั้งแนะนำให้ไปลงทะเบียนในฐานข้อมูล Do Not Call List ซึ่งบรรดาผู้ขายสินค้าและบริการออนไลน์จะต้องปฏิบัติตามกติกาไม่โทรหาผู้บริโภคที่ลงทะเบียนไว้ ทั้งนี้ผู้บริโภคที่ประสงค์จะงดรับข้อความสั้นหรือโทรศัพท์ที่เกี่ยวข้องกับการตลาดหรือการซื้อขาย สินค้าและบริการ (telemarketing) สามารถลงทะเบียนได้ที่ www.donotcall.gov/register.html หรือ Do Not Call Registry ซึ่งเป็นศูนย์รับลงทะเบียนภายใต้การกำกับดูแลของหน่วยงานที่คุ้มครองผู้บริโภค Federal Trade Commission Protecting America's Consumers ภายหลังจากที่ผู้บริโภคลงทะเบียนเพื่องดรับโทรศัพท์ใด ๆ แล้วภายใน 31 วันหากยังได้รับสายเรียกเข้าอีกสามารถรายงานมายัง FTC ได้ สำหรับข้อความที่ไม่พึงประสงค์ (unwanted text)

ผู้ให้บริการโทรศัพท์มือถือจะเปิดให้มีการส่งต่อข้อความไปยังหมายเลข 7726 [12](หรือคำว่า SPAM)

ในเรื่องการหลอกลวง ถือเป็นอีกหนึ่งหน้าที่หลักของ FTC ที่ต้องสร้างความตื่นตัวให้แก่ผู้บริโภคเพื่อให้เท่าทันการหลอกลวงในทุกรูปแบบ รวมทั้งกระตุ้นให้ผู้บริโภคช่วยกันรายงานมายัง FTC และเช่นเดียวกับ FCC คือ ทั้งสองหน่วยงานไม่ได้แก้ปัญหาแก่ผู้บริโภคเป็นรายกรณีแต่จะใช้รายงานที่ผู้บริโภคแจ้งมาเพื่อเป้าหมายสามเรื่องได้แก่ 1. สืบสวนต่อและนำไปสู่การดำเนินการต่อไปในเรื่องการปลอมแปลง การหลอกลวง และการปฏิบัติที่เลวร้ายของบรรดาธุรกิจต่าง ๆ 2. วิเคราะห์แนวโน้มของการหลอกลวง 3. ให้ความรู้กับผู้บริโภค คำแนะนำของ FTC มีการแยกแยะประเภทการหลอกลวง วิธีการแก้ปัญหาเฉพาะหน้า หน่วยงานที่ต้องติดต่อโดยเร็ว เช่น กรณีโอนเงินไปแล้วควรแก้ปัญหาอย่างไร, กรณีที่ถูกขโมยข้อมูลส่วนบุคคล, กรณีที่สแกมเมอร์เข้าถึงคอมพิวเตอร์หรือมือถือ เป็นต้น สำหรับช่องทางในการรายงานข้อความสแปม FTC แนะนำไว้สามช่องทาง ได้แก่ 1.รายงานผ่านแอปพลิเคชั่นของมือถือที่ใช้ 2. คัดลอกและส่งต่อข้อความไปยังหมายเลข 7726 (SPAM) 3.รายงานมายังเว็บไซต์ของ FTC https://reportfraud.ftc.gov/#/

ความน่าสนใจในการทำงานของ FTC ที่กระตุ้นให้ผู้บริโภครายงานการหลอกลวงรูปแบบต่าง ๆ อยู่ตรงที่ FTC ไม่เพียงแบ่งปันรายงานดังกล่าวให้กับหน่วยงานที่มีหน้าที่บังคับทางกฎหมายโดยคำนึงถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลเท่านั้น แต่ FTC ยังใช้ข้อมูลเพื่อนำมาวิเคราะห์และนำเสนอเรื่องราวในรูปแบบของ Data Spotlight: FTC Reporting back to you ยกตัวอย่างเช่น การวิเคราะห์เรื่องหลอกรักออนไลน์ (romance scam) ที่ติดอันดับสูงสุดในการรายงานของผู้บริโภคในปีพ.ศ.2564 การนำเสนอในรายงานได้แสดงตัวเลขเม็ดเงินที่ผู้บริโภคสูญเสียให้กับกิจกรรมหลอกลวงดังกล่าวในระหว่างช่วงปีพ.ศ.2560-2564

จากจำนวนเงิน 87 ล้านเหรียญสหรัฐในปีพ.ศ. 2560 เพิ่มเป็น 517 ล้านในปีพ.ศ.2564 กลุ่มคนที่ตกเป็นเหยื่อล่าสุดพบมากในช่วงอายุ 18-29 ปี และกิจกรรมนี้ยังถูกนำมาผูกโยงกับช่องทางการเงินผ่านการค้าเงินตราต่างประเทศและผ่านสกุลเงินดิจิทัลด้วย ในรายงานจะมีคำแนะนำว่าหากกำลังใช้บริการรักออนไลน์มีประเด็นอะไรบ้างที่ผู้บริโภคพึงระวัง[13]รูปแบบของการรายงานกลับหรือ Reporting back มายังผู้บริโภคจึงทำหน้าที่ช่วยประมวลสถานการณ์ที่ทันต่อเหตุการณ์และทำให้ประชาชนทุกกลุ่มได้รับประโยชน์จากการรายงานรายกรณีที่ผู้บริโภคแจ้งไปยังหน่วยงานด้วย

สรุป

การจัดการกับปัญหาการส่งข้อความสั้นหรือโทรศัพท์ที่ไม่พึงประสงค์ (spam) และหลอกลวง (scam) ต่อผู้บริโภคในสี่ประเทศ ได้แก่ ออสเตรเลีย สิงคโปร์ สหราชอาณาจักรและสหรัฐฯ พบแนวทางร่วมในการดำเนินการของทั้งสี่ประเทศที่น่าสนใจดังต่อไปนี้

1. การใช้ SPAM Rule หรือกฎหมายในการคุ้มครองผู้บริโภคในการรับข้อมูลข่าวสารที่เกี่ยวข้องกับธุรกิจและบริการในเชิงพาณิชย์ที่ไม่พึงประสงค์ สาระสำคัญคือ ผู้ส่งข้อความต้องได้รับความยินยอมจากผู้บริโภคในการตอบรับว่าประสงค์จะรับข้อความเท่านั้นจึงจะสามารถจัดส่งข้อความมายังโทรศัพท์มือถือ โทรศัพท์บ้านหรือโทรสารได้ (opt in) สามารถยกเลิกการบอกรับข้อความดังกล่าวได้โดยง่าย (opt out)

2. การใช้ระบบ Do not Call Registry เพื่อให้ผู้บริโภคสามารถแจ้งลงทะเบียนว่าหมายเลขของตนไม่พึงประสงค์จะรับการโทรเข้าใด ๆ เพื่อเสนอขายสินค้าและบริการ ระบบดังกล่าวในแต่ละประเทศ มีหน่วยงานกำกับดูแลแตกต่างกัน เช่น กรณีประเทศออสเตรเลีย หน่วยงานที่ดูแลเรื่องนี้คือ ACMA ขณะที่ในสิงคโปร์อยู่ภายใต้การดูแลของ PDPC หรือ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ส่วนในสหราชอาณาจักร ได้แก่ TPS

หรือ Telephone Preference Service สำหรับในสหรัฐฯ อยู่ในความดูแลของ FTC หรือคณะกรรมการการค้าเพื่อการคุ้มครองผู้บริโภค

3. หน่วยงานที่ทำหน้าที่ SCAM alert แต่ละประเทศมีชื่อเรียกต่างกัน แต่มีภารกิจที่ตรงกันคือ การสร้างความตระหนักและให้ข้อมูลแก่ผู้บริโภค เพื่อให้เท่าทันรูปแบบการหลอกลวงที่มีกลวิธีใหม่ ๆ เกิดขึ้นกับกลุ่มเป้าหมายต่าง ๆ กันตลอดเวลา ในกรณีของออสเตรเลีย มีหน่วยที่เรียกว่า Scam Watch ซึ่งอยู่ภายใต้การกำกับดูแลของ ACCC หรือคณะกรรมการด้านการแข่งขันและผู้บริโภค ในสิงคโปร์จะมีหน่วยงานด้านเรียกว่า SCAM Alert ภายใต้การกำกับดูแลขององค์กรป้องกันอาชญากรรมแห่งชาติ หรือ the National Crime Prevention Council ขณะที่ในสหราชอาณาจักร เป็นศูนย์รับรายงานการฉ้อโกงและอาชญากรรม ชื่อ Action Fraud สำหรับสหรัฐฯ มีส่วนที่เรียกว่า SCAM Alert ภายใต้การกำกับของ FTC เช่นกัน

4. ระบบการร้องเรียน การรายงานและการวิเคราะห์ข้อมูลเพื่อนำไปสู่การเตือนภัยการหลอกลวงผู้บริโภค ทุกประเทศเห็นตรงกันว่า การให้ความรู้แก่ผู้บริโภคเพื่อให้เท่าทันต่อการหลอกลวงทุกรูปแบบเป็นหัวใจของการป้องกันการสูญเสีย บทบาทขององค์กรกำกับดูแลที่เปิดให้ผู้บริโภครับเรื่องร้องเรียน หรือรายงานทั้งกรณี SPAM และ SCAM ไม่ได้แก้ไขปัญหาของผู้ร้องเป็นรายกรณี แต่จะนำข้อมูลที่ได้จากการร้องเรียนหรือรายงานมาวิเคราะห์และเผยแพร่เพื่อสื่อสารในรูปแบบที่หลากหลายทั้งภาษาและการนำเสนอเพื่อให้เข้าถึงกลุ่มคนที่มีความหลากหลายในสังคม ทำให้ผู้บริโภคมีแหล่งรวบรวมข้อมูลที่เชื่อถือได้ ทันต่อสถานการณ์ ตลอดจนวิธีการติดต่อไปยังหน่วยงานที่เกี่ยวข้อง

5. การบังคับใช้กฎหมายที่อยู่ภายใต้การกำกับดูแลและออกมาตราการใหม่เพื่อรับมือกับปัญหา องค์กรกำกับดูแลบังคับใช้กฎหมายด้วยการสั่งปรับผู้ให้บริการที่ไม่ปฏิบัติตามกฎหมายการควบคุมสแปม เช่น ใน

กรณีออสเตรเลีย[14] ACMA สั่งปรับ Sportsbet บริษัทพนันออนไลน์เป็นเงิน 2.5 ล้านเหรียญออสเตรเลียฐานที่ส่งข้อความมายังผู้บริโภคทั้งที่ได้แจ้งยกเลิกข้อความแล้วมากกว่า 1.5 แสนข้อความและอีเมลกว่า 37,000 รายตัวอย่างดังกล่าวสะท้อนให้เห็นว่า การร้องเรียนหรือรายงานของผู้บริโภคไปยังองค์กรกำกับดูแลได้รับการตอบสนองต่อการกระทำที่ละเมิดสิทธิผู้บริโภคตามกฎหมาย หรือความพยายามในการพัฒนาระบบ SMS Sender ID Registry (SSIR) เพื่อคุ้มครองผู้บริโภคจากผู้ส่งข้อความที่หลอกลวงในประเทศสิงคโปร์ภายหลังจากที่เกิดการส่งข้อความหลอกลวงลูกค้าธนาคารและทำให้ต้องสูญเงินเป็นจำนวนมาก[15] เป็นต้น

6. การประสานความร่วมมือทั้งในแง่ของข้อมูลและกลไกการทำงานระหว่างองค์กรต่าง ๆ ที่เกี่ยวข้อง อาจกล่าวได้ว่าการหลอกลวงหรือ Scam เป็นปัญหาระดับโลก ตัวอย่างของการแก้ปัญหาทั้งสี่ประเทศในกรณีศึกษาทำให้เราเห็นว่า การป้องกันและแก้ไขปัญหาต้องมีการประสานและแบ่งปันเรื่องร้องเรียนและรายงานที่ผู้บริโภคแจ้งเข้ามายังหน่วยงานที่เปิดรับเรื่องร้องเรียนและมีการวางกลไกในการทำงานร่วมกันอย่างเป็นระบบโดยทุกหน่วยงานดำเนินการบนหลักการที่คำนึงถึงการรักษาข้อมูลส่วนบุคคลซึ่งเป็นสิทธิที่ผู้บริโภคต้องได้รับการคุ้มครอง

[1] https://www.channelnewsasia.com/singapore/more-than-201-million-cheated-top-10-scam-types-2020-police-339081

[2] https://www.ofcom.org.uk/news-centre/2021/45-million-people-targeted-by-scams

[3] https://www.legislation.gov.au/Details/C2013C00021

[4] https://www.imda.gov.sg/for-community/Infocomm-regulation-and-guides/unsolicited-communications

[5] https://www.dnc.gov.sg/index.html

[6] https://www.scamshield.org.sg/setup-guide/

[7] https://www.channelnewsasia.com/singapore/ocbc-scam-block-website-sms-spoof-2499146

[8] https://www.legislation.gov.uk/uksi/2003/2426/regulation/21/made

[9] https://www.fcc.gov/spoofed-robocalls

[10] https://www.cnbc.com/2021/03/17/spam-callers-get-record-225-million-fine-from-fcc.html

[11] https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letters-3-more-companies

[12] https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

[13] https://www.ftc.gov/news-events/blogs/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021

[14] https://www.zdnet.com/article/acma-deals-sportsbet-with-the-largest-fine-ever-issued-for-spam-offences-in-australia/

[15] https://www.channelnewsasia.com/singapore/anti-sms-spoofing-registry-shut-replaced-full-fledged-system-imda-2543611