สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ประกาศแนวปฏิบัติ

ที่ นป. 4 /2566

เรื่อง แนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า

ตามที่ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 35/2556 เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงาน และการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 6 กันยายน พ.ศ. 2556 และที่แก้ไขเพิ่มเติม ("ประกาศที่ ทธ. 35/2556") ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 35/2557 เรื่อง หลักเกณฑ์ในรายละเอียดเกี่ยวกับการติดต่อและให้บริการลูกค้าสำหรับผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 10 พฤศจิกายน พ.ศ. 2557 และที่แก้ไขเพิ่มเติม ("ประกาศ ที่ สธ. 35/2557") ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 14/2562 เรื่อง หลักเกณฑ์ในรายละเอียดเกี่ยวกับการให้บริการสำหรับผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 12 กุมภาพันธ์ พ.ศ. 2562 และที่แก้ไขเพิ่มเติม ("ประกาศ ที่ สธ. 14/2562") และประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 28 กันยายน พ.ศ. 2565 ("ประกาศ ที่ สธ. 38/2565") กำหนดให้ผู้ประกอบธุรกิจรวบรวมและประเมินข้อมูลของลูกค้าก่อนเริ่มให้บริการ เพื่อวัตถุประสงค์ในการทำความรู้จักลูกค้า โดยรวบรวมข้อมูลและพิจารณาข้อมูลดังกล่าวด้วยการพิสูจน์และยืนยันตัวตนของลูกค้าเพื่อระบุตัวตนที่แท้จริงของลูกค้าหรือผู้รับประโยชน์ที่แท้จริง ซึ่งผู้ประกอบธุรกิจสามารถพิจารณาการนำเทคโนโลยีมาปรับใช้ในการดำเนินการ นอกจากนี้ ผู้ประกอบธุรกิจต้องมีการจัดการและจัดเก็บข้อมูลของลูกค้าที่รัดกุม และมีการบริหารจัดการเทคโนโลยีสารสนเทศที่นำมาใช้ในการรวบรวมและประเมินข้อมูลของลูกค้าที่มีประสิทธิภาพ รวมทั้งดำเนินการควบคุมดูแล ติดตาม และตรวจสอบให้มีการปฏิบัติตามนโยบายมาตรการและระบบงานที่กำหนดขึ้นเพื่อรองรับในเรื่องดังกล่าว ตลอดจนมีการทบทวนความเหมาะสมเป็นประจำนั้น

เพื่อประโยชน์ในการปฏิบัติตามข้อกำหนดเกี่ยวกับการทำความรู้จักลูกค้า การจัดการและจัดเก็บข้อมูลของลูกค้า และการบริหารจัดการระบบเทคโนโลยีสารสนเทศ อาศัยอำนาจตามข้อ 5(3) ประกอบกับข้อ 11 ข้อ 12(3) (3/1) (6) (11) และ (12) ข้อ 13 ข้อ 14 ข้อ 30(1) และ (2) ข้อ 25/4 ข้อ 31 ข้อ 32 ข้อ 33 ข้อ 36 และข้อ 37 แห่งประกาศ ที่ ทธ. 35/2556 จึงกำหนดแนวปฏิบัติไว้ดังต่อไปนี้

ข้อ 1 ให้ยกเลิกประกาศแนวปฏิบัติ ที่ นป. 5/2563 เรื่อง แนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า ลงวันที่ 23 ธันวาคม พ.ศ. 2563

ข้อ 2 แนวปฏิบัตินี้เป็นแนวทางเกี่ยวกับการรวบรวมและประเมินข้อมูลของลูกค้าโดยการนำเทคโนโลยีมาใช้เพื่อทำความรู้จักลูกค้าและจัดประเภทลูกค้า รวมทั้งการจัดให้มีระบบงานที่เกี่ยวข้องเพื่อรองรับการดำเนินการในเรื่องดังกล่าว ทั้งนี้ โดยมีรายละเอียดปรากฏตามแนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้าที่แนบท้ายประกาศนี้

ในกรณีที่ผู้ประกอบธุรกิจได้ดำเนินการรวบรวมและประเมินข้อมูลของลูกค้าโดยใช้เทคโนโลยีและจัดให้มีระบบงานตามแนวทางปฏิบัติที่แนบท้ายประกาศนี้ สำนักงานจะพิจารณาว่าผู้ประกอบธุรกิจได้ปฏิบัติตามประกาศ ที่ ทธ. 35/2556 ประกาศ ที่ สธ. 35/2557 ประกาศ ที่ สธ. 14/2562 และประกาศ ที่ สธ. 38/2565 ในส่วนที่เกี่ยวข้องแล้ว ทั้งนี้ หากผู้ประกอบธุรกิจดำเนินการด้วยวิธีที่แตกต่างจากที่กำหนดในแนวทางปฏิบัติดังกล่าว ผู้ประกอบธุรกิจมีภาระที่จะต้องพิสูจน์ให้เห็นว่าวิธีการนั้นเป็นไปตามหลักการและข้อกำหนดที่ผู้ประกอบธุรกิจต้องปฏิบัติตามที่กล่าวไว้ข้างต้น

ข้อ 3 แนวปฏิบัติตามข้อ 2 มีรายละเอียดในเรื่องดังต่อไปนี้

(1) แนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า

(ก) การพิสูจน์ตัวตน (identity proofing)

(ข) การยืนยันตัวตน (authentication)

(ค) การทำความรู้จักลูกค้าในเชิงลึก (client due diligence)

(ง) การทบทวนข้อมูลลูกค้า (ongoing / enhanced KYC)

(2) ระบบงานที่เกี่ยวข้องกับการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า

(ก) การบริหารความเสี่ยงด้าน IT

(ข) การจัดการและจัดเก็บข้อมูล

ข้อ 4 ในกรณีที่ผู้ประกอบธุรกิจรายใดใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล National Digital ID (NDID) ระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA-Digital ID (ThaID) ระบบการพิสูจน์และยืนยันตัวตนด้วยรูปแบบบัตรประจำตัวอิเล็กทรอนิกส์บนโทรศัพท์เคลื่อนที่ (Mobile ID) หรือระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลอื่นใด ซึ่งสามารถพิสูจน์ได้ว่าเป็นไปตามมาตรฐานที่สำนักงานกำหนดเพื่อพิสูจน์ตัวตนและยืนยันตัวตนของลูกค้าตามแนวทางที่แนบท้ายประกาศนี้ สำนักงานจะพิจารณาว่าผู้ประกอบธุรกิจรายนั้นได้ปฏิบัติตามประกาศ ที่ ทธ. 35/2556 และประกาศ ที่ สธ. 35/2557 ในเรื่องการทำความรู้จักลูกค้าในส่วนที่เป็นการพิสูจน์ตัวตนและการยืนยันตัวตนแล้ว

ข้อ 5 ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ 16 กรกฎาคม พ.ศ. 2566 เป็นต้นไป

ประกาศ ณ วันที่ 3 กรกฎาคม พ.ศ. 2566

(นายธวัชชัย พิทยโสภณ)

รองเลขาธิการ

รักษาการแทนเลขาธิการ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

แนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

กรกฎาคม 2566

บทนำ

การก้าวเข้าสู่ยุคดิจิทัลทำให้ผู้ประกอบธุรกิจต้องปรับตัวและแข่งขันกันนำเสนอบริการที่สะดวก รวดเร็วและตอบโจทย์วิถีในการใช้ชีวิตประจำวัน (lifestyle) ของลูกค้าให้ได้มากที่สุด สำนักงานตระหนักถึงความเปลี่ยนแปลงในเรื่องดังกล่าวและเห็นสัญญาณของการปรับตัวเข้าสู่ยุคดิจิทัลของผู้ประกอบธุรกิจในตลาดทุน โดยเฉพาะอย่างยิ่งการปรับเปลี่ยนวิธีการเปิดบัญชีและทำความรู้จักลูกค้า (Know Your Client: KYC) ด้วยวิธีอิเล็กทรอนิกส์ ("e-KYC") ซึ่งตามกฎเกณฑ์ของสำนักงานในเรื่องดังกล่าวกำหนดในลักษณะที่เป็นหลักการ (principle-based) ไม่ได้กำหนดวิธีการใดวิธีการหนึ่งเป็นการเฉพาะ ทั้งนี้ เพื่อให้เกิดความยืดหยุ่นในทางปฏิบัติสำหรับผู้ประกอบธุรกิจ เนื่องจากผู้ประกอบธุรกิจในตลาดทุนมีรูปแบบธุรกิจ ขนาด กลุ่มลูกค้า และจำนวนลูกค้าแตกต่างกัน ซึ่งหลักการตามกฎเกณฑ์ของสำนักงานกำหนดไว้ว่า ก่อนให้บริการแก่ลูกค้า ผู้ประกอบธุรกิจต้องรวบรวมและประเมินข้อมูลต่าง ๆ ของลูกค้าเพื่อให้ทราบว่าลูกค้าเป็นใคร รวมถึงการทำความรู้จักลูกค้าในเชิงลึก (Client Due Diligence : CDD) เพื่อให้ทราบถึงรายได้และแหล่งที่มาของรายได้ ฐานะการเงิน ความรู้ความเข้าใจ ประสบการณ์และวัตถุประสงค์ในการลงทุน รวมถึงความเสี่ยงที่ยอมรับได้ของลูกค้า เพื่อสามารถให้บริการแก่ลูกค้าได้อย่างมีประสิทธิภาพ ปกป้องผลประโยชน์และคุ้มครองลูกค้า อย่างไรก็ดี ผู้ประกอบธุรกิจหลายรายอาจมีความกังวลเนื่องจากไม่แน่ใจว่าการทำ e-KYC ในรูปแบบใดหรือวิธีการใดยังคงเป็นไปตามหลักการตามกฎเกณฑ์ของสำนักงาน

นอกจากนี้ ในปี 2561 ประเทศไทยได้มีการวางโครงสร้างพื้นฐานในการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทาง digital (Digital ID) ขึ้น ซึ่งจะเป็นระบบที่ช่วยให้ขั้นตอนการพิสูจน์ตัวตน (identity proofing) ไปจนถึงการทำ KYC ในขั้นตอนอื่น ๆ ของผู้ประกอบธุรกิจง่ายขึ้น ซึ่งการใช้บริการระบบดังกล่าว ผู้ประกอบธุรกิจต้องมีการกำหนดระดับความน่าเชื่อถือในการพิสูจน์และยืนยันตัวตน ผู้ประกอบธุรกิจจึงมีคำถามว่าต้องกำหนดระดับความน่าเชื่อถือระดับใดที่บรรลุหลักการที่สำนักงานเห็นว่าเหมาะสม เพียงพอ

ประกอบกับนโยบายของสำนักงานในการสนับสนุนให้นำเทคโนโลยีมาปรับใช้ในการประกอบธุรกิจ ซึ่งรวมถึงการทำ e-KYC ที่ยังคงเป็นไปตามหลักการของกฎเกณฑ์สำนักงาน ซึ่งผู้ประกอบธุรกิจสามารถพัฒนาวิธีการของตนเอง หรือเข้าใช้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ตามที่กล่าวข้างต้นได้ ดังนั้น เพื่อลดความกังวลและสร้างความเชื่อมั่นให้กับผู้ประกอบธุรกิจ สำนักงานจึงจัดทำแนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า ("แนวทางปฏิบัติฯ") ฉบับนี้ขึ้น <u>เพื่อให้ผู้ประกอบธุรกิจใช้เป็นแนวทางในการพัฒนารูปแบบการเปิดบัญชีและทำ e-KYC ทั้งนี้ เนื้อหาในแนวทางปฏิบัติฯ นี้ครอบคลุมการทำ KYC ทั้งแบบพบเห็นลูกค้าต่อหน้า (face-to-face) โดยมีการใช้เครื่องมือหรือเทคโนโลยีเข้ามาเสริมให้การดำเนินการมีประสิทธิภาพ บรรลุหลักการที่สำนักงานกำหนด และการทำ KYC แบบ online ที่ไม่ได้พบเห็นลูกค้าต่อหน้า (non face-to-face) โดยใช้เครื่องมือหรือเทคโนโลยีเข้ามาช่วยให้การดำเนินการได้คุณภาพเทียบเท่าแบบพบเห็น</u>

ลูกค้าต่อหน้า โดยหลักการที่นำเสนอในแนวทางปฏิบัติฯ นี้บางส่วนอ้างอิงข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (“ข้อเสนอแนะมาตรฐานฯ”) ที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (“สพธอ.”) จัดทำขึ้น ซึ่งผู้ประกอบธุรกิจควรศึกษาข้อเสนอแนะมาตรฐานฯ ดังกล่าวเพิ่มเติมเพื่อให้เข้าใจถึงหลักการของตัวอย่างวิธีการ เทคนิคต่าง ๆ ในแต่ละเรื่องให้ชัดเจนยิ่งขึ้นก่อนการนำไปใช้เพื่อกำหนดวิธีการทำ e-KYC ของตนเอง และการกำหนดตัวอย่างวิธีการในแนวทางปฏิบัติฯ นี้ สำนักงานได้ร่วมหารือกับหน่วยงานที่เกี่ยวข้อง* แล้ว

หากผู้ประกอบธุรกิจใช้วิธีการตามตัวอย่างในแนวทางปฏิบัติฯ นี้ ก็ถือว่าเป็นการทำ e-KYC ที่สอดคล้องกับหลักการของสำนักงาน **อย่างไรก็ดี วิธีการที่แสดงในแนวทางปฏิบัติฯ นี้เป็นเพียงตัวอย่างวิธีการขั้นต่ำ เนื่องจากไม่มีรูปแบบวิธีการทำ e-KYC ใดที่สามารถรองรับการจัดการความเสี่ยงที่อาจจะเกิดขึ้นได้ทั้งหมดสำหรับทุก business model ทุกกลุ่มลูกค้า หรือทุกสถานการณ์ ผู้ประกอบธุรกิจจึงสามารถปรับเปลี่ยนวิธีการได้ตามที่เห็นว่าเหมาะสมกับ business model ของตนเอง หรือสอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงไปได้ หากวิธีการที่เลือกใช้สามารถพิสูจน์ได้ว่าบรรลุหลักการของสำนักงานได้เช่นกัน** นอกจากนี้ การที่เทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็วจนทำให้ตัวอย่างวิธีการในแนวทางปฏิบัติฯ นี้อาจไม่เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป สำนักงานจึงอาจปรับปรุงแนวทางปฏิบัติฯ ให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงต่อไปได้

สำนักงานหวังว่าแนวทางปฏิบัติฯ นี้จะช่วยให้ผู้ประกอบธุรกิจสามารถเลือกวิธีการหรือเทคโนโลยีมาช่วยในการทำความรู้จักลูกค้าได้อย่างเหมาะสม ปลอดภัยและน่าเชื่อถือ ซึ่งจะส่งผลให้สามารถเข้าถึงลูกค้าและส่งเสริมให้เกิดการลงทุนในตลาดทุนได้อย่างสะดวก และช่วยยกระดับมาตรฐานการให้บริการในตลาดทุนไทย

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

---

*สมาคมบริษัทหลักทรัพย์ไทย (ASCO) และตัวแทนบริษัทหลักทรัพย์ สมาคมบริษัทจัดการลงทุน (AIMC) และตัวแทนบริษัทจัดการลงทุน ตลาดหลักทรัพย์แห่งประเทศไทย (ตลท.) รวมถึงสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

สารบัญ

1. แนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า

1.1 การพิสูจน์ตัวตน (IDENTITY PROOFING)

เพื่อเป็นการยกมาตรฐานในการปฏิบัติงานโดยเฉพาะในส่วนที่เกี่ยวกับการทำความรู้จักลูกค้าของผู้ประกอบธุรกิจในตลาดทุน และเพื่อให้สอดคล้องกับมาตรฐานที่เป็นที่ยอมรับ สำนักงานจึงได้หารือกับหน่วยงานต่าง ๆ ที่เกี่ยวข้อง เช่น สมาคมบริษัทหลักทรัพย์ไทย สมาคมบริษัทจัดการลงทุน และตลาดหลักทรัพย์แห่งประเทศไทย เพื่อร่วมกัน**กำหนดระดับความน่าเชื่อถือขั้นต่ำของการพิสูจน์ตัวตน (identity proofing) สำหรับขั้นตอนการเปิดบัญชี โดยพิจารณาอ้างอิงจากระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity Assurance Level : IAL) ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (“ข้อเสนอแนะมาตรฐานฯ”) ที่จัดทำโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (“สพธอ.”)**[1] ซึ่งได้ข้อสรุปว่า ระดับความน่าเชื่อถือขั้นต่ำของการพิสูจน์ตัวตนของผู้ประกอบธุรกิจในภาคการเงินการลงทุน **ไม่ควรแตกต่างกัน**

สำนักงานจึงกำหนดมาตรฐานขั้นต่ำในการพิสูจน์ตัวตน เพื่อให้การรวบรวมและตรวจสอบข้อมูลหลักฐานของลูกค้า (identification และ verification) มีคุณภาพเพียงพอที่จะให้มั่นใจว่า

1) ลูกค้ามีตัวตนจริง มีเพียงคนเดียว

2) หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง

3) ลูกค้ารายดังกล่าวเป็นเจ้าของหลักฐานที่นำมาแสดงจริง

การพิสูจน์ตัวตนลูกค้า แบ่งการดำเนินการได้ 4 ขั้นตอน ดังนี้

1. <u>การรวบรวมข้อมูลเพื่อระบุตัวตน (identification)</u>

ในการทำ e-KYC นั้น การรวบรวมข้อมูลและหลักฐานของลูกค้าอาจมีการใช้เทคโนโลยีเข้ามาช่วยในการรวบรวมและตรวจสอบข้อมูล เช่น การให้ลูกค้ากรอกข้อมูลพร้อมแนบไฟล์หลักฐานผ่านระบบอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์แทนการลงนามด้วยปากกา โดยไม่ต้องส่งเป็นกระดาษเช่นเดิม (paperless)

แม้จะมีการใช้วิธีการที่แตกต่างไปจากเดิม แต่เพื่อให้ผู้ประกอบธุรกิจยังคงมั่นใจว่ารู้จักตัวตนของลูกค้าได้เช่นเดียวกับวิธีการเดิม ข้อมูลหลักฐานที่ผู้ประกอบธุรกิจจะรวบรวมจากลูกค้า ทั้งเอกสารที่แปลงเป็นไฟล์อิเล็กทรอนิกส์ ภาพถ่ายหลักฐาน หรือภาพถ่ายบุคคล จะต้องมีความละเอียด ความชัดเจนเพียงพอ

[1] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (ขมธอ. 19-2566 เวอร์ชัน 3.0)

ที่จะนำไปใช้งานต่อได้ นอกจากนี้ การตรวจสอบหลักฐานต่าง ๆ ยังต้องมีคุณภาพเทียบเท่าแบบเดิม (หรือมากกว่า ในกรณีที่ผู้ประกอบธุรกิจไม่ได้พบเห็นลูกค้าต่อหน้า หรือได้พูดคุยกับลูกค้าในช่วงเวลาที่ให้บริการ)

นอกจากการขอข้อมูล หลักฐานจากลูกค้าแล้ว หากเทคโนโลยีและกฎหมายเอื้ออำนวย ผู้ประกอบธุรกิจอาจใช้**วิธีการเชื่อมโยงข้อมูลกับแหล่งที่มาของข้อมูลหรือผู้ให้ข้อมูลหรือหน่วยงานต่าง ๆ ที่น่าเชื่อถือ** ซึ่งมีข้อมูลของลูกค้าอยู่แล้ว เมื่อลูกค้ามาเปิดบัญชี สามารถดึงข้อมูลลูกค้าจากฐานข้อมูลเหล่านั้นมากรอกลงแบบคำขอเปิดบัญชีอัตโนมัติแทนการให้ลูกค้ากรอกข้อมูลเอง ทั้งนี้ จะต้องได้รับความยินยอมจากลูกค้าก่อน หรือหากลูกค้าต้องการปรับปรุงข้อมูลที่ได้จากฐานข้อมูลที่น่าเชื่อถือ ก็ควรมีหลักฐานประกอบการเปลี่ยนแปลงข้อมูลนั้น วิธีนี้นอกจากข้อมูลที่ได้รับจะมีความน่าเชื่อถือมากขึ้นแล้ว ยังเพิ่มความสะดวกให้ลูกค้าได้ แต่ผู้ประกอบธุรกิจต้องมั่นใจว่าแหล่งข้อมูลนั้นน่าเชื่อถือ มีข้อมูลที่ถูกต้องและเป็นปัจจุบัน

การรวบรวมข้อมูลโดยพิจารณาจากหลักฐานที่หลากหลายจะช่วยให้ผู้ประกอบธุรกิจสามารถพิจารณาความสอดคล้องของข้อมูลลูกค้าจากหลักฐานเหล่านั้น (cross verification) เพื่อให้มั่นใจว่าลูกค้ามีตัวตนจริง ตัวอย่างหลักฐานที่ผู้ประกอบธุรกิจอาจกำหนดให้ลูกค้าส่งให้ เช่น

1) หลักฐานประเภท long-term คือ สิ่งที่อยู่กับลูกค้าเป็นระยะเวลายาวนาน เช่น บัตรประชาชน หรือหนังสือเดินทาง

2) หลักฐานประเภท routine คือ สิ่งที่ลูกค้าได้รับอย่างสม่ำเสมอ เช่น บิลค่าสาธารณูปโภค ใบแจ้งยอดบัตรเครดิต ช่วยให้เห็นความมีตัวตนจริงของลูกค้า

3) หลักฐานประเภทครั้งคราว คือ สิ่งที่ลูกค้าต้องไปขอเป็นครั้งคราวและมีอายุจำกัด เช่น บัญชีเงินฝากธนาคาร/ statement หนังสือรับรองจากนายจ้างอายุไม่เกิน 6 เดือน หรือ ใบอนุญาตทำงานของคนต่างด้าว (work permit) ช่วยให้เห็นว่าลูกค้ามีตัวตนจริงและข้อมูลในหลักฐานเป็นปัจจุบัน

การปรับเปลี่ยนวิธีการรวบรวมข้อมูลหลักฐานที่ได้รับในรูปแบบอิเล็กทรอนิกส์ ซึ่งรวมถึงการลงลายมือชื่ออิเล็กทรอนิกส์ ผู้ประกอบธุรกิจอาจกังวลถึงการมีผลทางกฎหมาย ในกรณีดังกล่าว**กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์**ได้มีบทบัญญัติรองรับไว้แล้ว โดยวิธีการที่เลือกใช้ต้องเป็นไปตามที่กฎหมายดังกล่าวกำหนด

2. <u>การตรวจสอบข้อมูลหลักฐาน (verification) มีการดำเนินการใน 2 ขั้นตอน ดังนี้</u>

2.1 การตรวจสอบข้อมูลของหลักฐานแสดงตน เนื่องจากการทำ e-KYC ยังมีความเสี่ยงที่ลูกค้าจะให้ข้อมูลหรือหลักฐานเท็จได้ ผู้ประกอบธุรกิจจึงต้องกำหนดวิธีการตรวจสอบข้อมูลหลักฐานของลูกค้าได้อย่างมีประสิทธิภาพ แนวทางปฏิบัติฯ นี้จึงเป็นเพียงการยกตัวอย่างวิธีการที่เห็นว่าอาจช่วยจัดการความเสี่ยงดังกล่าวได้ **ซึ่งการตรวจสอบข้อมูลของหลักฐานแสดงตนสามารถดำเนินการได้หลายวิธี เช่น**

2.1.1 ตรวจสอบด้วยเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ (dip chip)

ที่ผ่านมา ผู้ประกอบธุรกิจจะขอบัตรประจำตัวประชาชนตัวจริงจากลูกค้ามาทำสำเนา ซึ่งผู้ประกอบธุรกิจจะสามารถสังเกตดูบัตรประจำตัวประชาชนดังกล่าวว่ามีจุดใดที่ผิดปกติ หรือปลอมแปลงมาหรือไม่ อย่างไรก็ดี เทคโนโลยีสมัยใหม่อาจทำให้การปลอมข้อมูลบนหน้าบัตร ประจำตัวประชาชนทำได้ง่ายและสังเกตความผิดปกติได้ยาก **ดังนั้น เพื่อให้ผู้ประกอบธุรกิจมั่นใจว่าหลักฐานนั้นเป็นของจริง จึงต้องมีการตรวจสอบโดยใช้เทคโนโลยีเข้ามาช่วย ด้วยการตรวจสอบข้อมูลบัตรประจำตัวประชาชนด้วยเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ เพื่อตรวจสอบข้อมูลจากชิปในบัตรว่าตรงกับข้อมูลหน้าบัตร รวมถึงเทียบใบหน้าจริงของลูกค้ากับใบหน้าบนหน้าบัตรและใบหน้าที่ได้จากชิปว่าตรงกันหรือไม่** ซึ่งเจ้าหน้าที่ที่ทำหน้าที่ในขั้นตอนนี้ควรมีความชำนาญและมีความระมัดระวังเพื่อให้มั่นใจว่าการตรวจสอบมีคุณภาพ

กรณีลูกค้าใช้หลักฐานที่ไม่สามารถใช้เครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ตรวจสอบได้ เช่น บัตรประจำตัวประชาชนรุ่นเก่าซึ่งไม่มีชิป หรือชิปในบัตรชำรุด ให้ผู้ประกอบธุรกิจกำหนดกระบวนการบริหารความเสี่ยงเพิ่มเติมอย่างเหมาะสมเป็นลายลักษณ์อักษรไว้รองรับ เช่น การขอหลักฐานที่ออกจากหน่วยงานที่น่าเชื่อถืออื่นซึ่งมีรูปถ่ายของลูกค้ามาตรวจสอบเพิ่มเติม

นอกจากนี้ กรณีการเปิดบัญชีนอกที่ทำการของผู้ประกอบธุรกิจให้กับผู้ลงทุนที่เข้านิยามตามประกาศว่าด้วยการกำหนดบทนิยามผู้ลงทุนสถาบัน ผู้ลงทุนรายใหญ่พิเศษ และผู้ลงทุนรายใหญ่ รวมถึงผู้ลงทุนที่เป็นนิติบุคคลนอกเหนือจากนิยามตามประกาศข้างต้น ซึ่งผู้ประกอบธุรกิจได้จัดให้มีเจ้าหน้าที่ดูแลลูกค้ารายดังกล่าวเป็นการเฉพาะอยู่แล้ว ผู้ประกอบธุรกิจสามารถให้เจ้าหน้าที่ดูแลลูกค้าตรวจสอบข้อมูลหลักฐานของลูกค้ารายดังกล่าวว่ามีความถูกต้องและมีข้อมูลเป็นปัจจุบันแทนการใช้เครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ได้ โดยให้จัดทำกระบวนการทำความรู้จักลูกค้าประเภทดังกล่าวไว้เป็นลายลักษณ์อักษร เช่น กระบวนการในการพิสูจน์ตัวตน กระบวนการในการบริหารจัดการความเสี่ยง หรือกระบวนการในการติดตามธุรกรรมต้องสงสัย

2.1.2 ตรวจสอบโดยการใช้บริการระบบ digital ID ที่มีความน่าเชื่อถือสูงตามมาตรฐาน เช่น NDID Mobile ID ThaID[2] หรือระบบ digital ID อื่น ซึ่งลูกค้าได้เคยพิสูจน์และยืนยันตัวตนกับระบบดังกล่าวไว้แล้ว

2.1.3 สำหรับลูกค้าที่ใช้หนังสือเดินทาง (passport) เพื่อเปิดบัญชี ซึ่งหนังสือเดินทางจะมีชิปที่บรรจุทั้งข้อมูลที่แสดงถึงตัวตนและรูปถ่ายของผู้ถือตามมาตรฐาน International Civil Aviation Organization (ICAO) ดังนั้น ในการตรวจสอบหนังสือเดินทาง ให้ผู้ประกอบธุรกิจตรวจสอบไปถึงข้อมูลที่อยู่ในชิปโดยใช้เทคโนโลยี Near Field Communication (NFC) ที่อยู่ใน smart phone หรือเทคโนโลยีอื่นที่สามารถอ่านข้อมูลในชิปเพื่อป้องกันการปลอมแปลงข้อมูลบนหน้าหนังสือเดินทาง หากไม่สามารถใช้ NFC เพื่อตรวจสอบข้อมูลได้ ผู้ประกอบธุรกิจสามารถใช้วิธีการอื่นใดที่ช่วยให้มั่นใจว่าข้อมูลที่ลูกค้าแสดงเป็นข้อมูลจริงและเป็นปัจจุบัน

2.2 การตรวจสอบสถานะของหลักฐานแสดงตน

เพื่อให้รู้ว่าหลักฐานนั้นยังใช้ได้ตามปกติ ผู้ประกอบธุรกิจจึงต้องตรวจสอบสถานะของหลักฐานแสดงตนกับหน่วยงานภาครัฐหรือแหล่งข้อมูลที่น่าเชื่อถือ (authoritative source) เช่น การตรวจสอบบัตรประจำตัวประชาชนกับกรมการปกครองผ่านช่องทาง online ด้วยการกรอกข้อมูลบนบัตรประจำตัวประชาชน 5 อย่าง ได้แก่ ชื่อ นามสกุล วันเดือนปีเกิด เลขที่บัตรประชาชน และ laser code หลังบัตร ผ่านระบบ web-service ของกรมการปกครอง โดยระบบจะแจ้งสถานะบัตรให้ผู้ตรวจสอบทราบ เช่น ใช้งานได้ปกติ ถูกแจ้งหาย หรือถูกออกบัตรใหม่ หรือวิธีการอื่นใดที่มีคุณภาพเทียบเท่า สามารถบรรลุวัตถุประสงค์ในการตรวจสอบสถานะบัตรประจำตัวประชาชนได้ ทั้งนี้ หากเกิดปัญหาไม่สามารถตรวจสอบหลักฐานกับผู้ออกหลักฐานหรือแหล่งข้อมูลที่น่าเชื่อถือ online ได้อันเนื่องมาจากความบกพร่องของระบบของผู้ออกหลักฐานหรือแหล่งข้อมูลที่น่าเชื่อถือ ให้ผู้ประกอบธุรกิจมีการบริหารความเสี่ยงเพิ่มเติมเพื่อให้มั่นใจว่าหลักฐานนั้นยังมีสถานะใช้งานได้ตามปกติจริง

อย่างไรก็ดี การตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานภาครัฐหรือแหล่งข้อมูลที่น่าเชื่อถือ (authoritative source) นั้น ผู้ประกอบธุรกิจอาจไม่สามารถตรวจสอบไปถึงรูปถ่ายของบุคคลผู้ที่เป็นเจ้าของบัตรประชาชน วิธีการนี้จึงยังมีความเสี่ยงที่ลูกค้าที่นำหลักฐานดังกล่าวมาใช้เปิดบัญชีจะไม่ใช่เจ้าของบัตรประชาชนที่แท้จริง ผู้ประกอบธุรกิจจึงต้องมีการตรวจสอบตัวบุคคลเพิ่มเติมโดยจะกล่าวต่อไปในขั้นตอนที่ 3. การตรวจสอบบุคคล

[2] ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA-Digital ID ผ่าน mobile application “ThaID” ของกรมการปกครอง
ระบบการพิสูจน์และยืนยันตัวตนด้วยรูปแบบบัตรประจำตัวอิเล็กทรอนิกส์บนโทรศัพท์เคลื่อนที่ หรือ “Mobile ID” ของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (“กสทช.”) ร่วมกับผู้ให้บริการโทรศัพท์เคลื่อนที่
การพัฒนาและให้บริการระบบพิสูจน์และยืนยันตัวตนด้วยใบหน้าทางดิจิทัล (Face Verification Service – FVS) ของกรมการปกครอง (ปัจจุบันให้บริการ เฉพาะหน่วยงานรัฐและผู้พิสูจน์และยืนยันตัวตน (IdP))

3. <u>การตรวจสอบตัวบุคคลด้วยการเปรียบเทียบใบหน้าลูกค้ากับภาพใบหน้าจากชิปที่ได้จากบัตรประชาชน หรือระบบอื่นที่มีความน่าเชื่อถือเทียบเท่า</u>

เมื่อได้ตรวจสอบข้อมูลหลักฐานตาม 2. ว่าเป็นข้อมูลถูกต้องและเป็นหลักฐานจริงแล้ว ผู้ประกอบธุรกิจยังต้องตรวจสอบตัวบุคคลด้วยว่า ลูกค้าเป็นบุคคลที่เป็นเจ้าของข้อมูลหลักฐานดังกล่าวจริง โดย<u>พิจารณาความสอดคล้องของข้อมูลหลักฐานที่ได้รับกับตัวตนที่แท้จริงของลูกค้า</u> เพื่อลดความเสี่ยงกรณีการใช้หลักฐานของผู้อื่นมาเปิดบัญชี และกรณีปลอมรูปบนหน้าบัตรประชาชนเพื่อใช้ในการเปิดบัญชี ดังนั้น <u>รูปถ่ายที่ใช้ประกอบการพิจารณาต้องมีความน่าเชื่อถือ</u> เช่น การใช้รูปถ่ายจากชิปในบัตรประชาชนหรือหนังสือเดินทาง หรือใช้วิธีการอื่นใดเพื่อให้ได้รูปถ่ายที่มีความน่าเชื่อถืออื่น เป็นต้น และเจ้าหน้าที่ที่ทำหน้าที่พิจารณาว่าใบหน้าลูกค้าตรงกันกับรูปถ่ายนั้น (visual comparison) ควรมีความชำนาญ ได้รับการอบรมในเรื่องที่เกี่ยวข้องอย่างเพียงพอ หรือหากต้องการเพิ่มความมั่นใจยิ่งขึ้นสามารถนำเทคโนโลยีการเปรียบเทียบข้อมูลชีวมิติ (biometric comparision) มาใช้ โดยมีความแม่นยำในการเปรียบเทียบในระดับสูง

นอกจากนี้ ผู้ประกอบธุรกิจอาจพัฒนาการเปรียบเทียบข้อมูลอื่นเท่าที่เทคโนโลยีหรือฐานข้อมูลที่ใช้เปรียบเทียบจะเอื้ออำนวย เช่น การเปรียบเทียบลายนิ้วมือของลูกค้ากับลายนิ้วมือที่อยู่ในหลักฐาน ซึ่งจะช่วยเพิ่มความน่าเชื่อถือได้อีกระดับ ทั้งยังช่วยแก้ปัญหาที่การเทียบใบหน้ากับรูปถ่ายอาจไม่สามารถทำได้ คือ การแยกแยะคู่แฝดที่อาจนำบัตรประชาชนของอีกคนมาใช้

ตามที่ได้กล่าวแล้ว นอกจากการตรวจสอบตัวบุคคลที่ใช้รูปถ่ายจากชิปในบัตรประชาชนหรือหนังสือเดินทางแล้วนั้น ผู้ประกอบธุรกิจยังสามารถเลือกใช้วิธีการอื่น เช่น การใช้บริการจากระบบ Digital ID ต่าง ๆ โดยเลือกใช้ Identity Provider (IdP) ที่มีวิธีการพิสูจน์และยืนยันตัวตนตามที่สำนักงานกำหนด การใช้บริการระบบ FVS หรือการมอบหมายให้บุคคลอื่นเป็นผู้รับดำเนินการ (outsource) ทั้งนี้ บุคคลอื่นนั้นจะต้องมีมาตรฐานในการพิสูจน์และยืนยันตัวตนตามที่สำนักงานกำหนดเช่นกัน

กรณีการพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า ต้องมีการจัดเก็บรูปถ่ายใบหน้าลูกค้าเพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง

นอกจากการเปรียบเทียบใบหน้ากับรูปถ่ายที่มีความน่าเชื่อถือแล้ว หากผู้ประกอบธุรกิจจะใช้การทำ VDO conference เพื่อพูดคุยกับลูกค้า เพิ่มเติมจากวิธีการที่กำหนดข้างต้นก็สามารถทำได้ ซึ่งเป็นช่องทางที่ช่วยให้เกิดการสื่อสารระหว่างกัน เป็นโอกาสให้ผู้ประกอบธุรกิจสามารถสังเกตหน้าตา ท่าทาง พฤติกรรมผ่านการพูดคุยตอบคำถาม ซึ่งจะช่วยให้สังเกตเห็นความสอดคล้องของตัวลูกค้ากับข้อมูลหลักฐาน และความรู้ประสบการณ์ลงทุนที่แจ้งไว้ นอกจากนี้ ผู้ประกอบธุรกิจยังสามารถจัดเก็บ VDO ที่บันทึกการพูดคุยกับลูกค้าเพื่อใช้เป็นหลักฐานอ้างอิงในอนาคตได้อีกด้วย

อย่างไรก็ดี การทำ VDO conference อาจมีความเสี่ยงที่ไม่สามารถตรวจสอบการปลอมแปลงตัวตนของผู้ขอเปิดบัญชีได้ ผู้ประกอบธุรกิจจึงต้องมีการติดตามรูปแบบ วิธีการ รวมถึงเทคนิคต่าง ๆ ในการ

ปลอมแปลงตัวตนอย่างต่อเนื่องเพื่อให้รู้เท่าทัน และปรับเปลี่ยนวิธีการในการป้องกันการปลอมแปลงที่เกิดขึ้น และผู้ประกอบธุรกิจสามารถใช้เทคนิคต่อไปนี้ ในการเพิ่มคุณภาพการทำ VDO conference

- ควรดำเนินการอย่างต่อเนื่อง ไม่ขาดช่วงตลอดการทำ VDO conference
- เจ้าหน้าที่ต้องเห็นภาพลูกค้าและหลักฐาน และได้ยินเสียงลูกค้าชัดเจนทุกขั้นตอน (กำหนดความสว่างของภาพและความดังของเสียงให้เพียงพอ)
- มีระยะเวลาในการพูดคุยนานเพียงพอที่จะทำความรู้จักลูกค้าได้
- ใช้เจ้าหน้าที่ที่ได้รับการอบรมมาโดยเฉพาะ สามารถสังเกตพฤติกรรมและคุ้นเคยกับรายละเอียดในหลักฐานที่ลูกค้านำมาแสดง
- เจ้าหน้าที่ถามคำถามที่มีคุณภาพ ไม่ใช่แค่ข้อมูลในบัตรประชาชน และเป็นคำถามปลายเปิด
- อาจตรวจสอบการใช้โปรแกรมปลอมแปลงตัวตน เช่น ให้ลูกค้าหันหน้าซ้าย/ ขวา และตรวจสอบหลักฐาน เช่น ให้ลูกค้าขยับหลักฐานเพื่อดูลายน้ำต่าง ๆ
- ใช้ช่องทางการสื่อสารที่มี security สูง
- อาจเก็บภาพ screen shot ระหว่างการสนทนา หรือจัดเก็บไฟล์บันทึกการสนทนาทั้งหมดไว้เพื่อใช้ประโยชน์ในการอ้างอิงหรือตรวจสอบในอนาคต

อย่างไรก็ดี หากผู้ประกอบธุรกิจพิจารณาว่า ลูกค้าจัดอยู่ในกลุ่มเสี่ยงสูงหรือวงเงินสูง ก็ควรพิจารณานัดพบกับลูกค้าเพื่อพูดคุย และขอดูหลักฐานตัวจริง เพื่อให้เป็นไปตามกรอบการบริหารความเสี่ยงที่เหมาะสม

4. <u>การตรวจสอบช่องทางติดต่อ</u>

ผู้ประกอบธุรกิจควรมีการตรวจสอบช่องทางการติดต่อของลูกค้าที่ได้ให้ไว้ในขั้นตอนการเปิดบัญชีว่าสามารถติดต่อลูกค้าได้จริง ลูกค้าคือเจ้าของช่องทางที่ใช้ในการติดต่อจริง รวมถึงมั่นใจว่าผู้ประกอบธุรกิจจะสามารถติดต่อหรือส่งข้อมูลข่าวสารสำคัญไปยังลูกค้าผ่านช่องทางดังกล่าวได้จริง ตัวอย่างวิธีการตรวจสอบ เช่น

- การส่งข้อความไปยังอีเมลที่ลูกค้าแจ้งไว้ พร้อมแนบ link ให้ลูกค้าคลิกยืนยันกลับมายังผู้ประกอบธุรกิจ
- การส่ง SMS OTP ไปยังหมายเลขโทรศัพท์มือถือให้ลูกค้ากรอกเข้าระบบของผู้ประกอบธุรกิจ

ตัวอย่างวิธีการพิสูจน์ตัวตนที่กล่าวมาข้างต้นนี้ เป็นตัวอย่างวิธีการที่สำนักงานเห็นว่ามีความเหมาะสมที่จะช่วยให้การพิสูจน์ตัวตนลูกค้าบรรลุหลักการตามประกาศของสำนักงานได้ **อย่างไรก็ดี กรณีการให้บริการธุรกรรมดังต่อไปนี้**

1. การให้บริการแก่ลูกค้าแบบครั้งคราว เช่น การจองซื้อหลักทรัพย์โดยลูกค้ามีบัญชีซื้อขายหลักทรัพย์กับผู้ประกอบธุรกิจรายอื่นอยู่ก่อนแล้ว

2. การให้บริการที่ปรึกษาการลงทุน เช่น การให้คำแนะนำหลักทรัพย์ผ่าน social media บทวิเคราะห์ งานสัมมนา รายการโทรทัศน์ หรือเว็บไซต์

3. การให้บริการเสนอขายผลิตภัณฑ์กรมธรรม์ประกันชีวิตควบหน่วยลงทุน (unit linked insurance policy)

ให้ผู้ประกอบธุรกิจทำความรู้จักลูกค้าด้วยวิธีการที่เห็นว่าเหมาะสมและสามารถบรรลุวัตถุประสงค์ได้ตามที่สำนักงานกำหนดในหลักเกณฑ์ว่าด้วยมาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงานและการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า โดยไม่ต้องใช้วิธีการตามตัวอย่างในแนวทางปฏิบัติ e-KYC

ทั้งนี้ เทคโนโลยีมีการเปลี่ยนแปลงที่รวดเร็ว จึงมีความเป็นไปได้ว่า ในอนาคตตัวอย่างวิธีการในการพิสูจน์ตัวตนนี้อาจไม่มีประสิทธิภาพเพียงพอ สำนักงานจึงขอให้ผู้ประกอบธุรกิจมีการทบทวนวิธีการของตนเองให้เหมาะสมตามสถานการณ์ที่เปลี่ยนแปลงไป เพื่อให้วิธีการที่เลือกใช้บรรลุหลักการของสำนักงานได้อย่างต่อเนื่อง

1.2 การยืนยันตัวตน (AUTHENTICATION)

การยืนยันตัวตนในธุรกรรมตลาดทุนนั้น เป็นอีกเรื่องสำคัญที่สำนักงานกำหนดแนวทางไว้ โดยมีวัตถุประสงค์ 2 ประการ ได้แก่

1. การยืนยันตัวตนเพื่อการเปิดบัญชี : เมื่อผู้ขอใช้บริการต้องการเปิดบัญชีกับผู้ประกอบธุรกิจ โดยได้ทำการพิสูจน์ตัวตนแล้ว หากต่อมาจะเข้าระบบของผู้ประกอบธุรกิจเพื่อวัตถุประสงค์ในการเปิดบัญชี เช่น นำส่งข้อมูลหลักฐานเพิ่มเติม หรือกรณีที่ผู้ขอใช้บริการต้องการพิสูจน์และยืนยันตัวตนผ่านระบบ Digital ID ต่างๆ ซึ่งทั้ง 2 กรณีผู้ขอใช้บริการจะต้องทำการยืนยันตัวตนกับระบบของผู้ประกอบธุรกิจ หรือกับระบบของ IdP แล้วแต่กรณี **สำนักงานและหน่วยงานที่เกี่ยวข้องได้ร่วมกันกำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยยืนยันตัวตน (authentication factor) ที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย ตามข้อเสนอแนะมาตรฐานฯ ของ สพธอ.**[3] อย่างไรก็ดี หากสถานการณ์เปลี่ยนไปโดยสำนักงานพิจารณาแล้วเห็นว่า ผู้ประกอบธุรกิจมีความพร้อม มีเทคโนโลยีที่เหมาะสม สำนักงานอาจปรับเปลี่ยนข้อกำหนดให้เหมาะสมยิ่งขึ้น เพื่อเป็นการคุ้มครองผู้ลงทุนและสร้างความน่าเชื่อถือในตลาดทุนให้เป็นที่ยอมรับตามมาตรฐานต่อไปได้ในอนาคต

2. การยืนยันตัวตนเพื่อเข้าทำธุรกรรมในระบบ online : เมื่อผู้ขอใช้บริการเปิดบัญชีกับผู้ประกอบธุรกิจแล้วและต้องการเข้าระบบเพื่อทำธุรกรรม จะต้องมีขั้นตอนการยืนยันตัวตนเพื่อให้มั่นใจได้ว่าลูกค้าหรือผู้ได้รับมอบอำนาจจากลูกค้าเป็นผู้เข้ามาใช้งานระบบด้วยตนเอง เพื่อให้ผู้ประกอบธุรกิจบรรลุวัตถุประสงค์ตามหลักเกณฑ์ของสำนักงาน[4] ในเรื่องการให้บริการลูกค้าอย่างเหมาะสม **สำนักงานจึงกำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยยืนยันตัวตน (authentication factor) ที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย ตามข้อเสนอแนะมาตรฐานฯ ของ สพธอ.**[5] **สำหรับการ log-in เข้าสู่ระบบเพื่อทำธุรกรรมประเภทดังต่อไปนี้ จนกว่าจะ log-off ไปจากระบบ โดยจะให้มีการยืนยันตัวตนเป็นรายธุรกรรมอีกหรือไม่ก็ได้**

(1) ธุรกรรมที่เกี่ยวข้องกับการซื้อ ขาย หรือแลกเปลี่ยนหลักทรัพย์หรือสัญญาซื้อขายล่วงหน้า ซึ่งรวมถึงการใช้สิทธิเพื่อวัตถุประสงค์ในการทำธุรกรรมข้างต้น (เช่น จองซื้อหลักทรัพย์ IPO) หรือการใช้สิทธิที่เกิดจากการถือครองหลักทรัพย์เดิมอยู่ก่อนแล้ว (เช่น การเข้าร่วมประชุมผู้ถือหุ้น)

---

[3] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (ขมธอ. 20-2566 เวอร์ชัน 3.0)

[4] ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 35/2557 เรื่อง หลักเกณฑ์ในรายละเอียดเกี่ยวกับการติดต่อและให้บริการลูกค้าสำหรับผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 10 พฤศจิกายน 2557 กำหนดให้ผู้ประกอบธุรกิจต้องมีกระบวนการในการยืนยันตัวตนลูกค้า (authentication) ที่เหมาะสมและน่าเชื่อถือ เพื่อให้มั่นใจว่าการลงทุนหรือการทำธุรกรรมในผลิตภัณฑ์ในตลาดทุนได้กระทำโดยลูกค้าหรือผู้ได้รับมอบอำนาจจากลูกค้าที่ผู้ประกอบธุรกิจติดต่อและให้บริการ

(2) ธุรกรรมที่เกี่ยวข้องกับการฝาก ถอน หรือโอนเงินสด ซึ่งรวมถึงการเพิ่ม ลด หรือเปลี่ยนแปลงบัญชีธนาคารเพื่อการรับเงินค่าขาย ดอกเบี้ย หรือเงินปันผล และการสมัครหักบัญชีเงินฝากอัตโนมัติ (ATS)

(3) ธุรกรรมที่เกี่ยวข้องกับการให้ลูกค้าลงนามผูกพันในสัญญาที่เกี่ยวเนื่องกับการใช้บริการธุรกิจหลักทรัพย์และธุรกิจสัญญาซื้อขายล่วงหน้า

(4) ธุรกรรมที่เกี่ยวข้องกับการขอความยินยอม (consent) จากลูกค้า

(5) ธุรกรรมที่เกี่ยวข้องกับการเปลี่ยนแปลงข้อมูลดังต่อไปนี้

- ข้อมูลตัวตนของลูกค้า เช่น ชื่อ นามสกุล
- ช่องทางติดต่อกับลูกค้า เช่น ที่อยู่ในการจัดส่งเอกสาร เบอร์โทรศัพท์ อีเมล
- ปัจจัยที่ใช้ยืนยันตัวตน เช่น password หรือ pin

สำหรับธุรกรรมอื่นที่มิได้กล่าวถึง ให้ผู้ประกอบธุรกิจใช้การยืนยันตัวตนแบบปัจจัยเดียว (single-factor authentication) เป็นขั้นต่ำ

ทั้งนี้ ข้อเสนอแนะต่าง ๆ เกี่ยวกับการยืนยันตัวตนให้เป็นไปตามข้อเสนอแนะมาตรฐานของ สพธอ. ในเรื่องที่เกี่ยวข้อง

1.3 การทำความรู้จักลูกค้าในเชิงลึก (CLIENT DUE DILIGENCE : CDD)

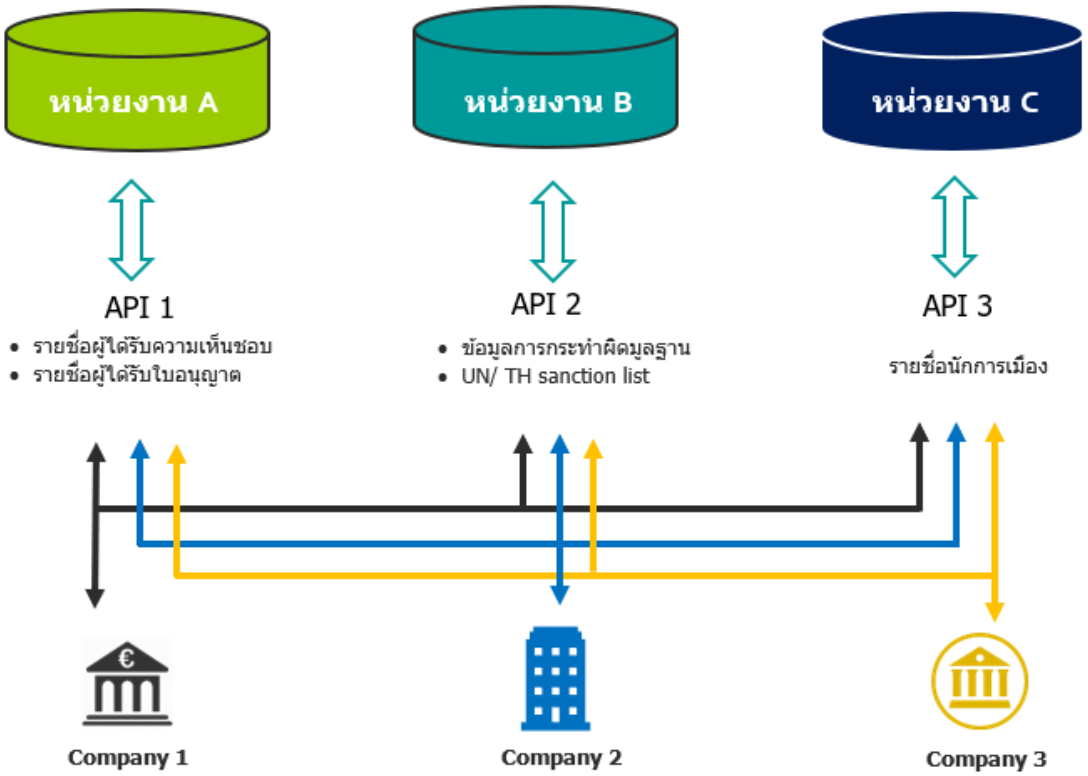
การทำ CDD นั้น ผู้ประกอบธุรกิจอาจใช้เทคโนโลยีเข้ามาช่วยเพื่อลดภาระในการดำเนินการในขั้นตอนนี้ เช่น การใช้ Application Program Interface: API เชื่อมโยงข้อมูลกับหน่วยงานที่เป็นเจ้าของข้อมูลที่ต้องการตรวจสอบโดยตรงเพื่อดึงข้อมูลที่เกี่ยวข้องกับการทำ CDD ลูกค้ามาตรวจสอบ จากเดิมที่ต้องค้นหาข้อมูลแต่ละเรื่องที่กระจายอยู่ตามเว็บไซต์ของหน่วยงานรัฐต่าง ๆ แต่ละเว็บไซต์ก็มีความซับซ้อน หาข้อมูลยาก

ในอนาคตหากมีฐานข้อมูลกลางของหน่วยงานรัฐหรือระบบที่เอกชนพัฒนาขึ้น หรือหน่วยงานกลางที่อาจมีการจัดตั้งขึ้นโดยเฉพาะเพื่อรวบรวมหรือเป็นศูนย์กลางในการเชื่อมโยงข้อมูลดังกล่าว เช่น ระบบ Digital ID ที่หน่วยงานรัฐและเอกชนซึ่งมีข้อมูลที่น่าเชื่อถือจะพิจารณาเข้ามาร่วมเป็นสมาชิกในฐานะ แหล่งข้อมูลที่น่าเชื่อถือ (authoritative Source หรือ “AS”) โดยหากผู้ประกอบธุรกิจที่เป็นสมาชิกในระบบ Digital ID แล้วต้องการข้อมูลของลูกค้าเพื่อใช้ในการพิจารณาประกอบการเปิดบัญชีและทำ KYC ก็สามารถ request ผ่านระบบ Digital ID ไปยัง AS ที่มีข้อมูลที่ต้องการเพื่อให้ส่งข้อมูลหรือยืนยันข้อมูลของลูกค้าได้ การตรวจสอบข้อมูลลูกค้าจึงทำได้อย่างสะดวก รวดเร็ว และน่าเชื่อถือ

อย่างไรก็ดี การใช้ข้อมูลลูกค้าจากแหล่งข้อมูลต่าง ๆ นั้น ผู้ประกอบธุรกิจควรคำนึงถึงการปฏิบัติให้เป็นไปตามกฎหมายอื่นที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่กำหนดให้ลูกค้าต้องให้ความยินยอมในการเปิดเผยข้อมูลก่อน หรือกฎหมายเฉพาะอื่น ๆ ด้วย (ถ้ามี) รวมถึงต้องมั่นใจว่าแหล่งข้อมูลที่ใช้ในการตรวจสอบเป็นแหล่งข้อมูลที่น่าเชื่อถือ และข้อมูลที่จะใช้มีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพราะแม้ว่าผู้ประกอบธุรกิจจะสามารถทำ CDD โดยการเชื่อมโยงข้อมูลกับแหล่งต่าง ๆ ก็เป็นเพียงการช่วยให้สามารถดำเนินการได้สะดวก รวดเร็ว และน่าเชื่อถือยิ่งขึ้นกว่าวิธีการเดิม แต่ความรับผิดยังคงอยู่ที่ผู้ประกอบธุรกิจตามที่กฎหมายกำหนดเช่นเดิม

ข้อมูลขั้นต่ำในการทำความรู้จักในเชิงลึก (ตามประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 35/2556 เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงานและการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์ และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 6 กันยายน 2556)
- ความสามารถและแหล่งที่มารายได้ - ฐานะการเงิน - ประสบการณ์ในการลงทุนหรือการทำธุรกรรม - ความรู้เกี่ยวกับการลงทุนหรือการทำธุรกรรม - วัตถุประสงค์ในการลงทุนหรือการทำธุรกรรม - ความเสี่ยงที่ยอมรับได้ - ผู้รับผลประโยชน์ที่แท้จริง

ตัวอย่างการเชื่อมโยงข้อมูลด้วย API



1.4 การทบทวนข้อมูลลูกค้า (ONGOING / ENHANCED KYC)

การทบทวนข้อมูลลูกค้านั้น ผู้ประกอบธุรกิจสามารถใช้เทคโนโลยีเข้ามาช่วยลดภาระในการดำเนินการได้ เช่น การใช้โปรแกรมอัตโนมัติต่าง ๆ ที่ช่วยให้การทำงานง่ายขึ้น อาทิ การแจ้งเตือนอัตโนมัติเมื่อลูกค้าครบกำหนดต้องทบทวนข้อมูล KYC หรือโปรแกรมวิเคราะห์ข้อมูลความเสี่ยงลูกค้า เป็นต้น เครื่องมือทางอิเล็กทรอนิกส์เหล่านี้จะช่วยลดภาระของผู้ประกอบธุรกิจ ลดความเสี่ยงที่จะทำผิดกฎหมาย/กฎเกณฑ์ ใช้เวลาทำงานน้อยลง มีความถูกต้องมากขึ้น โปรแกรมเหล่านี้มีบริษัทผู้พัฒนาขึ้นมาให้บริการมากมาย ซึ่งการเลือกใช้โปรแกรมใดนั้น ผู้ประกอบธุรกิจต้องพิจารณาถึงความน่าเชื่อถือ หรือผู้ประกอบธุรกิจสามารถพัฒนาโปรแกรมได้เอง ซึ่งถือได้ว่าเป็นการใช้ Regulatory Technology หรือ RegTech เข้ามาช่วยในการดำเนินงานนั่นเอง

สำนักงานสนับสนุนให้ผู้ประกอบธุรกิจใช้เทคโนโลยีเข้ามาช่วยในการทบทวนข้อมูลลูกค้า เนื่องจากช่วยสร้างประสิทธิภาพ ความถูกต้อง และรวดเร็วในการดำเนินงาน ช่วยลดโอกาสที่จะเกิดการกระทำผิดในตลาดทุนได้ เนื่องจากลูกค้าที่เปิดบัญชีแบบ online เป็นลูกค้ากลุ่มที่ผู้ประกอบธุรกิจอาจไม่ได้พบเจอตัวจริงเลย ผู้ประกอบธุรกิจจึงควรให้ความสำคัญกับลูกค้ากลุ่มนี้สูงขึ้น เช่น กำหนดนโยบายให้มีการติดตามธุรกรรมใกล้ชิด พิจารณา trade volume กับวงเงินที่ได้รับว่าสอดคล้องกันหรือไม่ มีการกำหนดเงื่อนไข enhanced KYC เข้มขึ้นเมื่อพบธุรกรรมผิดปกติ เช่น ซื้อขายเกินวงเงิน ไม่เหมาะสม ไม่สอดคล้องกับ profile เป็นต้น นโยบายเหล่านี้จะช่วยป้องกันทั้งตัวผู้ประกอบธุรกิจเองจากความเสี่ยงที่ลูกค้าจะใช้บัญชีเป็นช่องทางกระทำผิด และช่วยให้ผู้ประกอบธุรกิจตรวจจับพฤติกรรมผิดปกติที่เกิดจากการถูก hack เข้ามาทำธุรกรรมที่เจ้าของบัญชีไม่ได้เป็นผู้ดำเนินการได้อีกด้วย

2. ระบบงานที่เกี่ยวข้องกับการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า

2.1 การบริหารความเสี่ยงด้าน IT

การใช้เทคโนโลยีเข้ามาช่วยให้เกิดการเปิดบัญชีแบบ online และ ทำ e-KYC นั้น แน่นอนว่ามีประโยชน์มากต่อผู้ประกอบธุรกิจที่ช่วยลดต้นทุนในการดำเนินการ สามารถให้บริการลูกค้าได้อย่างรวดเร็ว และตรวจสอบข้อมูลลูกค้าได้ถูกต้อง แม่นยำยิ่งขึ้น ด้านผู้ลงทุนก็ได้รับประโยชน์ไม่น้อยในเรื่องความสะดวก รวดเร็ว มีค่าใช้จ่ายในการใช้บริการลดลง และเพิ่มโอกาสให้ลูกค้ากลุ่มใหม่ ๆ เช่น กลุ่มที่อยู่ห่างไกลสามารถเข้าถึงบริการด้านการลงทุนได้ง่ายขึ้น

อย่างไรก็ดี เหรียญมี 2 ด้าน เทคโนโลยีก็เช่นกัน หากนำมาปรับใช้ให้ดี ก็จะก่อประโยชน์มหาศาล แต่หากนำไปใช้โดยไม่ระมัดระวัง อาจจะเป็นช่องโหว่ที่ก่อให้เกิดความเสียหายด้านชื่อเสียง และความเชื่อมั่นได้อย่างมากเช่นเดียวกัน การบริหารความเสี่ยงในเรื่องที่เกี่ยวข้องอย่างเหมาะสมตลอดทั้งกระบวนการที่จะดำเนินการจึงเป็นเรื่องที่ผู้ประกอบธุรกิจควรคำนึงถึงอยู่เสมอ

ทั้งนี้ ในช่วงต้นของแนวทางปฏิบัติฯ นี้ได้กล่าวถึงความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้นในการทำ e-KYC พร้อมทั้งยกตัวอย่างวิธีการที่สำนักงานเห็นว่าสามารถช่วยลดความเสี่ยงดังกล่าวไว้บ้างแล้ว อย่างไรก็ดี ยังมี **ความเสี่ยงที่เกิดจากการใช้เทคโนโลยี** เช่น ความเสี่ยงที่ระบบหรือบัญชีลูกค้าจะถูกลักลอบขโมยข้อมูลจากผู้ไม่ประสงค์ดี ความเสี่ยงที่ระบบที่บริษัทได้ลงทุนพัฒนาไว้จะล้าสมัย เนื่องจากเทคโนโลยีและสภาพแวดล้อมเปลี่ยนแปลงรวดเร็ว ความเสี่ยงที่ระบบการให้บริการของบริษัทจะเกิดปัญหาด้านเทคนิคจนไม่สามารถให้บริการได้อย่างต่อเนื่อง เป็นต้น ความเสี่ยงจากการพึ่งพาเทคโนโลยีในสัดส่วนที่มากนี้อาจก่อให้เกิดความเสียหายต่อผู้ประกอบธุรกิจได้มหาศาล จึงจำเป็นที่ผู้ประกอบธุรกิจต้องให้ความสำคัญไม่น้อยไปกว่าการตรวจสอบตัวตนลูกค้าในกระบวนการ e-KYC

สำนักงานตระหนักถึงความสำคัญในการบริหารความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับการเปิดบัญชี online และการทำ e-KYC นี้ จึงได้แนะนำข้อกำหนดด้านเทคนิคต่าง ๆ ไว้แล้วบ้างในแต่ละขั้นตอน อย่างไรก็ดี สำหรับการบริหารความเสี่ยงอื่น ๆ ด้านเทคโนโลยีสารสนเทศนั้น สำนักงานมีการกำหนดแนวทางดำเนินการไว้ในประกาศเรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ[5] ที่ผู้ประกอบธุรกิจสามารถนำมาปรับใช้เพิ่มเติมในการกำหนดในเรื่องอื่น ๆ ที่เกี่ยวข้อง เช่น การกำหนดให้มีการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ การควบคุมการเข้ารหัสข้อมูล การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (outsource) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เป็นต้น

[5] ประกาศแนวปฏิบัติ ที่ นป. 7/2565 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 28 กันยายน 2565

2.2 การจัดการและจัดเก็บข้อมูล

<u>การคุ้มครองข้อมูลของลูกค้า</u>

การรวบรวมข้อมูลลูกค้าเพื่อประกอบการทำ KYC นี้ ผู้ประกอบธุรกิจต้องคำนึงถึงการคุ้มครองข้อมูลของลูกค้า โดยต้องมีการจัดการและจัดเก็บข้อมูลอย่างเหมาะสม ป้องกันการเข้าถึงข้อมูลอย่างไม่ถูกต้องหรือขัดกับกฎหมาย ตามเกณฑ์ที่สำนักงานกำหนด

กฎเกณฑ์ของสำนักงานกำหนดให้ผู้ประกอบธุรกิจจัดเก็บข้อมูลที่เกี่ยวข้องในการให้บริการลูกค้าไว้ในรูปแบบที่เหมาะสม เช่น มีระบบจัดเก็บข้อมูลลูกค้าที่รัดกุม เป็นระเบียบ มีความปลอดภัยในการจัดเก็บ สามารถป้องกันการแก้ไข หรือถูกทำลาย หรือมีการเข้ารหัสข้อมูล (data encryption) เพื่อสร้างความปลอดภัยให้กับข้อมูล กำหนดสิทธิในการเข้าถึงข้อมูลเพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าดูข้อมูล และมีการสำรองข้อมูลเพื่อป้องกันการสูญหาย โดยเฉพาะอย่างยิ่งหากมีการเก็บข้อมูลข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ของลูกค้า เช่น ข้อมูลส่วนบุคคล ข้อมูลภาพถ่ายหรือข้อมูลชีวมิติของลูกค้า ต้องใช้ระบบที่มีความปลอดภัยสูงในการจัดเก็บข้อมูลเหล่านี้เพราะหากรั่วไหลไปสู่บุคคลอื่นจะสร้างความเสียหายต่อเจ้าของข้อมูลได้มาก นอกจากนั้น ผู้ประกอบธุรกิจต้องเก็บรักษาข้อมูลตามระยะเวลาที่สำนักงานประกาศกำหนด เพื่อสามารถใช้อ้างอิงหรือเพื่อการตรวจสอบได้ในอนาคต

ผู้ประกอบธุรกิจยังต้องศึกษาและปฏิบัติตามกฎหมายอื่นที่เกี่ยวข้อง เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลที่กำหนดเรื่องการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลจากลูกค้า เช่น ให้ขอข้อมูลจากลูกค้าเท่าที่จำเป็น ต้องแจ้งวัตถุประสงค์และขอบเขตในการใช้ข้อมูลเหล่านั้นให้ลูกค้าทราบอย่างชัดเจนและเฉพาะเจาะจง และลูกค้าต้องเต็มใจที่จะให้ความยินยอม (consent) ให้ใช้ข้อมูลตามวัตถุประสงค์ที่แจ้ง รวมถึงข้อความที่ระบุในการขอความยินยอมต้องชัดเจน ไม่คลุมเครือ นอกจากนั้น ผู้ประกอบธุรกิจต้องแจ้งให้ลูกค้าทราบถึงสิทธิของลูกค้า เช่น สิทธิในการเข้าถึงข้อมูล สิทธิในการแก้ไขข้อมูล สิทธิในการลบหรือยกเลิกการให้ข้อมูล

นอกจากกฎหมายของไทยที่ผู้ประกอบธุรกิจต้องปฏิบัติตามแล้ว ผู้ประกอบธุรกิจควรพิจารณาระมัดระวังการดำเนินการกับข้อมูลส่วนบุคคลของลูกค้าที่ได้รับการคุ้มครองโดยกฎหมายอื่น เช่น General Data Protection Regulation หรือ GDPR ซึ่งผู้ประกอบธุรกิจที่มีสถานประกอบการอยู่ภายในสหภาพยุโรปหรือมีการประมวลผลข้อมูลที่เกี่ยวข้องกับการเสนอสินค้าหรือบริการให้แก่บุคคลผู้พำนักในสหภาพยุโรป หรือมีการประมวลผลข้อมูลซึ่งเกี่ยวข้องกับการเฝ้าสังเกตพฤติกรรมที่เกิดขึ้นในสหภาพยุโรปและรวมถึงประเทศที่มีผลผูกพันทางกฎหมายกับประเทศสหภาพยุโรป ต้องระมัดระวังการดำเนินการเกี่ยวกับข้อมูลลูกค้า โดยต้องดำเนินการให้เป็นไปตาม GDPR ด้วย ทั้งนี้ แม้ข้อมูล หลักฐานต่าง ๆ ที่จะเกิดขึ้นในกระบวนการ e-KYC นั้นจะอยู่ในรูปแบบที่แตกต่างจากการทำ KYC ในรูปแบบเดิมที่เป็นกระดาษ ใช้วิธีการจัดเก็บข้อมูล หลักฐานต่าง ๆ ที่แตกต่างกัน แต่ยังคงใช้หลักการเดียวกัน

ผู้ประกอบธุรกิจควรศึกษารายละเอียดในกฎหมาย/กฎเกณฑ์ต่าง ๆ ให้ชัดเจนเพื่อให้การเก็บรักษาข้อมูลมีประสิทธิภาพเหมาะสมและหลีกเลี่ยงโทษที่อาจเกิดขึ้นจากความผิดพลาดได้