ประกาศแนวปฏิบัติ
ที่ นป. 5 /2563
เรื่อง แนวทางปฏิบัติในการนำเทคโนโลยี
มาใช้ในการทำความรู้จักลูกค้า

ตามที่ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 35/2556 เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงาน และการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 6 กันยายน พ.ศ. 2556 ("ประกาศ ที่ ทธ. 35/2556") ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 35/2557 เรื่อง หลักเกณฑ์ในรายละเอียดเกี่ยวกับการติดต่อและให้บริการลูกค้าสำหรับผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 10 พฤศจิกายน พ.ศ. 2557 ("ประกาศ ที่ สธ. 35/2557") ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 37/2559 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 12 กันยายน พ.ศ. 2559 ("ประกาศ ที่ สธ. 37/2559") และประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 14/2562 เรื่อง หลักเกณฑ์ในรายละเอียดเกี่ยวกับการให้บริการสำหรับผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 12 กุมภาพันธ์ พ.ศ. 2562 ("ประกาศ ที่ สธ. 14/2562") กำหนดให้ผู้ประกอบธุรกิจรวบรวมและประเมินข้อมูลของลูกค้าก่อนเริ่มให้บริการ โดยมีการจัดการและจัดเก็บข้อมูลของลูกค้าที่รัดกุม และมีการบริหารจัดการเทคโนโลยีสารสนเทศที่นำมาใช้ในการรวบรวมและประเมินข้อมูลของลูกค้าที่มีประสิทธิภาพ รวมทั้งดำเนินการควบคุมดูแล ติดตาม และตรวจสอบให้มีการปฏิบัติตามนโยบาย มาตรการ และระบบงานที่กำหนดขึ้นเพื่อรองรับในเรื่องดังกล่าว ตลอดจนมีการทบทวนความเหมาะสมเป็นประจำ นั้น

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. 9/2562 เรื่อง แนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า ลงวันที่ 26 ธันวาคม พ.ศ. 2562

ข้อ 2 แนวปฏิบัตินี้เป็นแนวทางเกี่ยวกับการรวบรวมและประเมินข้อมูลของลูกค้าโดยการนำเทคโนโลยีมาใช้เพื่อทำความรู้จักลูกค้าและจัดประเภทลูกค้า รวมทั้งการจัดให้มีระบบงานที่เกี่ยวข้องเพื่อรองรับการดำเนินการในเรื่องดังกล่าว ทั้งนี้ โดยมีรายละเอียดปรากฏตามแนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้าที่แนบท้ายประกาศนี้

ในกรณีที่ผู้ประกอบธุรกิจได้ดำเนินการรวบรวมและประเมินข้อมูลของลูกค้าโดยใช้เทคโนโลยีและจัดให้มีระบบงานตามแนวทางปฏิบัติที่แนบท้ายประกาศนี้ สำนักงานจะพิจารณาว่าผู้ประกอบธุรกิจได้ปฏิบัติตามประกาศ ที่ ทธ. 35/2556 ประกาศ ที่ สธ. 35/2557 ประกาศ ที่ สธ. 37/2559 และประกาศ ที่ สธ. 14/2562 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 (National Digital ID : NDID) เพื่อพิสูจน์ตัวตนและยืนยันตัวตนของลูกค้า สำนักงานจะพิจารณาว่าผู้ประกอบธุรกิจรายนั้นได้ปฏิบัติตามประกาศ ที่ ทธ. 35/2556 และประกาศ ที่ สธ. 35/2557 ในเรื่องการทำความรู้จักลูกค้าในส่วนที่เป็นการพิสูจน์ตัวตนและการยืนยันตัวตนแล้ว

ข้อ 5 ในกรณีที่ผู้ประกอบธุรกิจรายใดได้เข้าร่วมโครงการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (National Digital ID : NDID) และมีหนังสือแจ้งต่อสำนักงานแล้ว สำนักงานจะพิจารณาว่าในระหว่างระยะเวลา 6 เดือนนับแต่วันที่ประกาศนี้มีผลใช้บังคับ ผู้ประกอบธุรกิจรายนั้นได้ปฏิบัติตามประกาศ ที่ ทธ. 35/2556 และประกาศ ที่ สธ. 35/2557 ในเรื่องการทำความรู้จักลูกค้าในส่วนที่เป็น

การพิสูจน์ตัวตนและการยืนยันตัวตนแล้ว ทั้งนี้ เมื่อพ้นระยะเวลาดังกล่าว หากผู้ประกอบธุรกิจไม่สามารถใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (National Digital ID : NDID) ในการพิสูจน์ตัวตนและการยืนยันตัวตนของลูกค้าได้ ให้ผู้ประกอบธุรกิจยังคงต้องปฏิบัติให้เป็นไปตามข้อ 2 และข้อ 3 ด้วย

ข้อ 6 ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ 1 มกราคม พ.ศ. 2564 เป็นต้นไป

ประกาศ ณ วันที่ 23 ธันวาคม พ.ศ. 2563

(นางสาวรื่นวดี สุวรรณมงคล)
เลขาธิการ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

แนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ธันวาคม 2563

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 ของลูกค้า เพื่อให้ทราบว่าลูกค้าเป็นใคร รวมถึงการทำความรู้จักลูกค้าในเชิงลึก (Client Due Diligence : CDD) เพื่อให้ทราบถึงรายได้และแหล่งที่มาของรายได้ ฐานะการเงิน ความรู้ความเข้าใจ ประสบการณ์และวัตถุประสงค์ในการลงทุนรวมถึงความเสี่ยงที่ยอมรับได้ของลูกค้า เพื่อสามารถให้บริการแก่ลูกค้าได้อย่างมีประสิทธิภาพ ปกป้องผลประโยชน์และคุ้มครองลูกค้า อย่างไรก็ดี ผู้ประกอบธุรกิจหลายรายอาจมีความกังวลเนื่องจากไม่แน่ใจว่าการทำ e-KYC ในรูปแบบใดหรือวิธีการใดยังคงเป็นไปตามหลักการตามกฎเกณฑ์ของสำนักงาน

นอกจากนี้ ในปี 2561 ประเทศไทยได้มีการวางโครงสร้างพื้นฐานในการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทาง digital (Digital ID) ขึ้น ซึ่งจะเป็นระบบที่ช่วยให้ขั้นตอนพิสูจน์ตัวตน (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</u>

(non face-to-face) โดยใช้เครื่องมือหรือเทคโนโลยีเข้ามาช่วยให้การดำเนินการได้คุณภาพเทียบเท่าแบบพบเห็นลูกค้าต่อหน้า โดยหลักการที่นำเสนอในแนวทางปฏิบัติฯ นี้บางส่วนอ้างอิงจากข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ("ข้อเสนอแนะมาตรฐานฯ") ที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ("สพธอ.") จัดทำขึ้น ซึ่งผู้ประกอบธุรกิจควรศึกษาข้อเสนอแนะมาตรฐานฯ ดังกล่าวเพิ่มเติมเพื่อให้เข้าใจถึงหลักการของตัวอย่างวิธีการ เทคนิคต่าง ๆ ในแต่ละเรื่องให้ชัดเจนยิ่งขึ้นก่อนการนำไปใช้เพื่อกำหนดวิธีการทำ e-KYC ของตนเอง และการกำหนดตัวอย่างวิธีการในแนวทางปฏิบัติฯ นี้ สำนักงานได้ร่วมหารือกับหน่วยงานที่เกี่ยวข้อง* จัดการประชุมผู้ประกอบธุรกิจแบบ focus group รวมถึงเปิดรับฟังความคิดเห็นผ่านเว็บไซต์ของสำนักงานแล้ว

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**กำหนดมาตรฐานขั้นต่ำในการพิสูจน์ตัวตน (Identity proofing) สำหรับขั้นตอนการเปิดบัญชี** โดยพิจารณาอ้างอิงจาก**ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level : IAL) ในข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย (ภาพรวมและอภิธานศัพท์ การลงทะเบียนและพิสูจน์ตัวตน และการยืนยันตัวตน) ("ข้อเสนอแนะมาตรฐานฯ") ที่จัดทำโดย สพธอ.**[1] ซึ่งได้ข้อสรุปว่ามาตรฐานของผู้ประกอบธุรกิจในภาคการเงิน การลงทุน**ไม่ควรจะมีมาตรฐานที่แตกต่างกัน** อย่างไรก็ดี ในระยะแรกที่จะมีการบังคับใช้ระดับความน่าเชื่อถือดังกล่าว ควรพิจารณาถึงความพร้อมของผู้ประกอบธุรกิจและเทคโนโลยีที่ใช้อยู่ในปัจจุบันด้วย ดังนั้น เพื่อเป็นการปรับระดับความพร้อมของผู้ให้บริการในธุรกิจการเงินการลงทุนในระยะแรก**จึงเห็นควรกำหนดระดับ IAL ขั้นต่ำสำหรับการเปิดบัญชีในธุรกิจตลาดทุนที่สำนักงานยอมรับ คือ IAL ระดับ 2.1 ตามข้อเสนอแนะมาตรฐานฯ ของ สพธอ. พร้อมจัดให้มีการตรวจสอบหลักฐานแสดงตนกับแหล่งที่มาของข้อมูลหลักฐานหรือผู้ให้ข้อมูลที่น่าเชื่อถือแบบ online เพิ่มเติมด้วย (รวมเรียกว่า IAL 2.1+)**

ดังนั้น หากผู้ประกอบธุรกิจเลือกใช้บริการพิสูจน์ตัวตนผ่านระบบ digital ID ก็สามารถเลือกใช้ผู้ให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider หรือ "IdP") ที่มี IAL ระดับ 2.1 ได้ แต่ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบหลักฐานแสดงตนกับแหล่งที่มาของข้อมูลหลักฐานหรือผู้ให้ข้อมูลที่น่าเชื่อถือแบบ online เพิ่มเติมด้วย หรือหากผู้ประกอบธุรกิจเลือกใช้ IdP ระดับ 2.2 ขึ้นไปแล้ว ให้ถือว่าผู้ประกอบธุรกิจปฏิบัติตามที่สำนักงานกำหนดในเรื่องการพิสูจน์ตัวตนแล้ว โดยไม่ต้องตรวจสอบหลักฐานแสดงตนกับแหล่งที่มาของข้อมูลหลักฐานหรือผู้ให้ข้อมูลที่น่าเชื่อถือแบบ online เพิ่มเติม

อย่างไรก็ดี หากสถานการณ์เปลี่ยนไปโดยสำนักงานพิจารณาแล้วเห็นว่า ผู้ประกอบธุรกิจมีความพร้อม มีเทคโนโลยีที่เหมาะสม สำนักงานอาจปรับเปลี่ยนระดับ IAL เพื่อเป็นการคุ้มครองผู้ลงทุนและสร้างความน่าเชื่อถือในตลาดทุนให้เป็นที่ยอมรับตามมาตรฐานต่อไปได้ในอนาคต

[1] รายละเอียดตามภาคผนวก 1 ความหมายของ KYC และ ECOSYSTEM ในหัวข้อมาตรฐานการพิสูจน์และยืนยันตัวตนของไทย

การกำหนดมาตรฐานขั้นต่ำในการพิสูจน์ตัวตนข้างต้นนั้น เพื่อให้การรวบรวมและตรวจสอบข้อมูล หลักฐานของลูกค้า (identification และ verification) มีคุณภาพเพียงพอที่จะให้มั่นใจว่า

1) ลูกค้ามีตัวตนจริง มีเพียงคนเดียว

2) หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง

3) ลูกค้ารายดังกล่าวเป็นเจ้าของหลักฐานที่นำมาแสดงจริง

การพิสูจน์ตัวตนลูกค้าด้วย IAL ระดับ 2.1 พร้อมจัดให้มีการตรวจสอบหลักฐานแสดงตนกับแหล่งที่มาของข้อมูลหลักฐานหรือผู้ให้ข้อมูลที่น่าเชื่อถือแบบ online (IAL 2.1+) นั้น แบ่งการดำเนินการได้ 4 ขั้นตอน ดังนี้

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

ในการทำ e-KYC นั้น การรวบรวมข้อมูลและหลักฐานของลูกค้าอาจมีการใช้เทคโนโลยีเข้ามาช่วยในการรวบรวมและตรวจสอบข้อมูล เช่น การให้ลูกค้ากรอกข้อมูลพร้อมแนบไฟล์หลักฐานผ่านระบบอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์แทนการลงนามด้วยปากกา โดยไม่ต้องส่งเป็นกระดาษเช่นเดิม (paperless) หรือการตรวจสอบหลักฐานด้วยอุปกรณ์อิเล็กทรอนิกส์ (การ dip chip) หรือการตรวจสอบหลักฐานแสดงตนกับแหล่งที่มาของข้อมูลหลักฐานหรือผู้ให้ข้อมูลที่น่าเชื่อถือแบบ online

แม้จะมีการใช้วิธีการที่แตกต่างไปจากเดิม แต่เพื่อให้ผู้ประกอบธุรกิจยังคงมั่นใจว่า รู้จักตัวตนของลูกค้าได้เช่นเดียวกับวิธีการเดิม ข้อมูล หลักฐานที่ผู้ประกอบธุรกิจจะรวบรวมจากลูกค้า ทั้งเอกสารที่แปลงเป็นไฟล์อิเล็กทรอนิกส์ ภาพถ่ายหลักฐาน หรือภาพถ่ายบุคคล จะต้องมีความละเอียด ความชัดเจนเพียงพอที่จะนำไปใช้งานต่อได้[2] นอกจากนี้ การตรวจสอบหลักฐานต่าง ๆ ยังต้องมีคุณภาพเทียบเท่าแบบเดิม (หรือมากกว่า ในกรณีที่ผู้ประกอบธุรกิจไม่ได้พบเห็นลูกค้าต่อหน้า หรือได้พูดคุยกับลูกค้าในช่วงเวลาที่ให้บริการ)

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

[2] รายละเอียดตาม ภาคผนวก 4 ตัวอย่างมาตรฐานขั้นต่ำทางเทคนิค เรื่อง มาตรฐานขั้นต่ำสำหรับความละเอียด (Resolution) ของภาพหลักฐานที่ลูกค้าส่งให้ผู้ประกอบธุรกิจผ่านระบบอิเล็กทรอนิกส์ และมาตรฐานขั้นต่ำของภาพถ่ายและวิดีโอสำหรับบันทึกการทำธุรกรรม

การรวบรวมข้อมูลโดยพิจารณาจากหลักฐานที่หลากหลายจะช่วยให้ผู้ประกอบธุรกิจสามารถพิจารณาความสอดคล้องของข้อมูลลูกค้าจากหลักฐานเหล่านั้น (cross verification) เพื่อให้มั่นใจว่าลูกค้ามีตัวตนจริง ตัวอย่างหลักฐานที่ผู้ประกอบธุรกิจอาจกำหนดให้ลูกค้าส่งให้ เช่น

1) หลักฐานประเภท long-term คือ สิ่งที่อยู่กับลูกค้าเป็นระยะเวลายาวนาน เช่น บัตรประชาชน หรือ passport

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)</u>

การทำ e-KYC ยังมีความเสี่ยงที่ลูกค้าจะให้ข้อมูลหรือหลักฐานเท็จได้ ผู้ประกอบธุรกิจจึงต้องกำหนดวิธีการตรวจสอบข้อมูลหลักฐานของลูกค้าได้อย่างมีประสิทธิภาพ แนวทางปฏิบัติฯ นี้จึงเป็นเพียงการยกตัวอย่างวิธีการที่เห็นว่าอาจช่วยจัดการความเสี่ยงดังกล่าวได้

ที่ผ่านมา ในการตรวจสอบหลักฐาน หากผู้ประกอบธุรกิจไม่ได้พบเห็นลูกค้าต่อหน้าก็จะขอเพียงสำเนาบัตรประชาชนจากลูกค้า หรือหากมีโอกาสได้พบเห็นลูกค้าต่อหน้าก็จะขอ บัตรประชาชนตัวจริงจากลูกค้ามาทำสำเนา ซึ่งกรณีหลังนี้ ผู้ประกอบธุรกิจสามารถสังเกตดูบัตรประชาชนดังกล่าวว่ามีจุดใดที่ผิดปกติ หรือปลอมแปลงมาหรือไม่ อย่างไรก็ดี เทคโนโลยีสมัยใหม่อาจทำให้การปลอมข้อมูลบนหน้าบัตรประชาชนทำได้ง่ายและสังเกตความผิดปกติได้ยาก **ดังนั้น เพื่อให้ผู้ประกอบธุรกิจมั่นใจว่าหลักฐานนั้นเป็นของจริง ไม่ว่าจะเป็นการเปิดบัญชีแบบพบเห็น หรือไม่พบเห็นลูกค้าต่อหน้า จึงต้องมีการตรวจสอบโดยใช้เทคโนโลยีเข้ามาช่วย ด้วยการนำบัตรประชาชนมาเสียบกับเครื่องอ่านบัตร (smart card reader) เพื่อตรวจสอบข้อมูลจากชิพในบัตรว่า ตรงกับข้อมูลหน้าบัตร รวมถึงเทียบใบหน้าจริงของลูกค้ากับใบหน้าบนหน้าบัตร และใบหน้าที่ได้จากชิพว่า ตรงกันหรือไม่** ซึ่งเจ้าหน้าที่ที่ทำหน้าที่ในขั้นตอนนี้ควรมีความชำนาญและมีความระมัดระวังเพื่อให้มั่นใจว่าการตรวจสอบมีคุณภาพ

กรณีลูกค้าใช้หลักฐานที่ไม่สามารถใช้เครื่องอ่านบัตรตรวจสอบได้ เช่น บัตรประชาชนรุ่นเก่าซึ่งไม่มีชิพ หรือชิพในบัตรชำรุด ให้ผู้ประกอบธุรกิจกำหนดกระบวนการบริหารความเสี่ยงเพิ่มเติมอย่างเหมาะสมเป็นลายลักษณ์อักษรไว้รองรับ เช่น การขอหลักฐานที่ออกจากหน่วยงานที่น่าเชื่อถืออื่นซึ่งมีรูปถ่ายของลูกค้ามาตรวจสอบเพิ่มเติม

กรณีการเปิดบัญชีนอกที่ทำการของผู้ประกอบธุรกิจให้กับผู้ลงทุนที่เข้านิยามตามประกาศว่าด้วยการกำหนดบทนิยามผู้ลงทุนสถาบัน ผู้ลงทุนรายใหญ่พิเศษ และผู้ลงทุนรายใหญ่ และผู้ลงทุนที่เป็นนิติบุคคลนอกเหนือจากนิยามตามประกาศข้างต้น ซึ่งผู้ประกอบธุรกิจได้จัดให้มีเจ้าหน้าที่ดูแลลูกค้ารายดังกล่าวเป็นการเฉพาะอยู่แล้ว ผู้ประกอบธุรกิจสามารถให้เจ้าหน้าที่ดูแลลูกค้าตรวจสอบข้อมูลหลักฐานของลูกค้ารายดังกล่าวว่ามีความถูกต้องและมีข้อมูลเป็นปัจจุบันแทนการใช้เครื่องอ่านบัตรได้ โดยให้จัดทำกระบวนการทำความรู้จักลูกค้าประเภทดังกล่าวไว้เป็นลายลักษณ์อักษร เช่น กระบวนการในการพิสูจน์ตัวตน กระบวนการในการบริหารจัดการความเสี่ยง หรือกระบวนการในการติดตามธุรกรรมต้องสงสัย เป็นต้น

นอกเหนือจากการตรวจสอบหลักฐานด้วยเครื่องอ่านบัตรแล้ว **ผู้ประกอบธุรกิจต้องตรวจสอบหลักฐานกับผู้ออกหลักฐาน (issuing source) หรือแหล่งข้อมูลที่น่าเชื่อถือ (authoritative source)** เพื่อให้รู้ว่าหลักฐานนั้นยังใช้ได้ตามปกติ เช่น การตรวจสอบบัตรประชาชนกับกรมการปกครองผ่านช่องทาง online ด้วยการกรอกข้อมูลบนบัตรประชาชน 5 อย่าง ได้แก่ ชื่อ นามสกุล วันเดือนปีเกิด เลขที่บัตรประชาชน และ laser code หลังบัตร ผ่านระบบ web-service ของกรมการปกครอง โดยระบบจะแจ้งสถานะบัตรให้ผู้ตรวจสอบทราบ เช่น ใช้งานได้ปกติ ถูกแจ้งหาย หรือถูกออกบัตรใหม่ เป็นต้น ทั้งนี้ หากเกิดปัญหาไม่สามารถตรวจสอบหลักฐานกับผู้ออกหลักฐานหรือแหล่งข้อมูลที่น่าเชื่อถือ online ได้อันเนื่องมาจากความบกพร่องของระบบของผู้ออกหลักฐานหรือแหล่งข้อมูลที่น่าเชื่อถือ ให้ผู้ประกอบธุรกิจมีการบริหารความเสี่ยงเพิ่มเติมเพื่อให้มั่นใจว่าหลักฐานนั้นยังมีสถานะใช้งานได้ตามปกติจริง

อย่างไรก็ดี การตรวจสอบหลักฐานกับผู้ออกหลักฐานกรณีที่เป็นการตรวจสอบบัตรประชาชนกับกรมการปกครองนั้น ระบบของกรมการปกครองจะไม่แสดงรูปถ่ายของบุคคลผู้ที่เป็นเจ้าของบัตร วิธีการนี้จึงยังมีความเสี่ยงที่ลูกค้าที่นำหลักฐานดังกล่าวมาใช้เปิดบัญชีจะไม่ใช่เจ้าของบัตรที่แท้จริง ผู้ประกอบธุรกิจจึงต้องมีการตรวจสอบตัวบุคคลเพิ่มเติมโดยจะกล่าวต่อไปในขั้นตอนที่ 3. การตรวจสอบบุคคล

สำหรับลูกค้าที่ใช้หนังสือเดินทาง (passport) เพื่อเปิดบัญชี ซึ่ง passport จะมีชิพที่บรรจุทั้งข้อมูลที่แสดงถึงตัวตนและรูปถ่ายของผู้ถือ ซึ่งมีความน่าเชื่อถือสูงตามมาตรฐาน International Civil Aviation Organization (ICAO) ดังนั้นในการตรวจสอบ passport ให้ผู้ประกอบธุรกิจตรวจสอบไปถึงข้อมูลที่อยู่ในชิพ โดยใช้เทคโนโลยี Near Field Communication (NFC) ที่อยู่ใน smart phone หรือเทคโนโลยีอื่นที่สามารถอ่านข้อมูลในชิพเพื่อป้องกันการปลอมแปลงข้อมูลบนหน้า passport

3. <u>การตรวจสอบตัวบุคคล</u>

เมื่อได้ตรวจสอบข้อมูลหลักฐานตาม 2. ว่าเป็นข้อมูลถูกต้องและเป็นหลักฐานจริงแล้ว ผู้ประกอบธุรกิจยังต้องตรวจสอบตัวบุคคลต่อว่า ลูกค้าเป็นบุคคลที่เป็นเจ้าของข้อมูลหลักฐานดังกล่าวจริง โดย<u>พิจารณาความสอดคล้องของข้อมูลหลักฐานที่ได้รับกับตัวตนที่แท้จริงของลูกค้า</u> เพื่อลดความเสี่ยงกรณีการใช้หลักฐานของผู้อื่นมาเปิดบัญชี และกรณีปลอมรูปบนหน้าบัตรประชาชนเพื่อใช้ในการเปิดบัญชี ดังนั้น <u>รูปถ่ายที่ใช้ประกอบการพิจารณาต้องมาจากแหล่งข้อมูลที่น่าเชื่อถือ (trusted source)</u> เช่น การใช้รูปถ่ายจากชิพในบัตรประชาชนหรือ passport หรือใช้วิธีการอื่นใดเพื่อให้ได้รูปถ่ายของลูกค้าจากแหล่งข้อมูลที่น่าเชื่อถืออื่น เป็นต้น และเจ้าหน้าที่ที่ทำหน้าที่พิจารณาว่าใบหน้าลูกค้าตรงกันกับรูปถ่ายจากแหล่งข้อมูลที่น่าเชื่อถือนั้น (physical comparison) ควรมีความชำนาญ ได้รับการอบรมในเรื่องที่เกี่ยวข้องอย่างเพียงพอ หรือหากต้องการเพิ่มความมั่นใจยิ่งขึ้นสามารถนำเทคโนโลยีการเปรียบเทียบใบหน้า (facial recognition) มาใช้ โดยมีความแม่นยำในการเปรียบเทียบในระดับสูง

นอกจากนี้ ผู้ประกอบธุรกิจอาจพัฒนาการเปรียบเทียบข้อมูลอื่นเท่าที่เทคโนโลยีหรือฐานข้อมูลที่ใช้เปรียบเทียบจะเอื้ออำนวย เช่น การเปรียบเทียบลายนิ้วมือของลูกค้ากับลายนิ้วมือที่อยู่ในหลักฐาน ซึ่งจะช่วยเพิ่มความน่าเชื่อถือได้อีกระดับ ทั้งยังช่วยแก้ปัญหาที่การเทียบใบหน้ากับรูปถ่ายอาจไม่สามารถทำได้ คือ การแยกแยะคู่แฝดที่อาจนำบัตรประชาชนของอีกคนมาใช้ เป็นต้น

ตามที่ได้กล่าวแล้ว นอกจากการตรวจสอบตัวบุคคลที่ใช้รูปถ่ายจากชิพในบัตรประชาชนหรือ passport แล้ว นั้น ผู้ประกอบธุรกิจยังสามารถเลือกใช้วิธีการอื่นเช่น การใช้บริการจากระบบ NDID โดยเลือกใช้ IdP ที่มีระดับความน่าเชื่อถือในการพิสูจน์และยืนยันตัวตนตามที่สำนักงานกำหนด หรือการมอบหมายให้บุคคลอื่นเป็นผู้รับดำเนินการ (outsource) ทั้งนี้ บุคคลอื่นนั้นจะต้องมีมาตรฐานในการพิสูจน์และยืนยันตัวตนตามที่สำนักงานกำหนดเช่นกัน

นอกจากการเปรียบเทียบใบหน้ากับรูปถ่ายที่ได้จากแหล่งข้อมูลที่น่าเชื่อถือแล้ว ในกรณีที่ผู้ประกอบธุรกิจอาจใช้วิธี VDO conference เพื่อพูดคุยกับลูกค้า ซึ่งเป็นช่องทางให้เกิดการสื่อสารระหว่างกัน เป็นโอกาสให้ผู้ประกอบธุรกิจสามารถสังเกตหน้าตา ท่าทาง พฤติกรรมผ่านการพูดคุยตอบคำถาม ซึ่งจะช่วยให้สังเกตเห็นความสอดคล้องของตัวลูกค้ากับข้อมูลหลักฐาน และความรู้ ประสบการณ์ลงทุนที่แจ้งไว้ รวมถึงสามารถให้ลูกค้าแสดงบัตรประชาชนด้านหน้า-หลัง ผ่านหน้ากล้องให้เจ้าหน้าที่สังเกตรายละเอียดต่าง ๆ เพิ่มเติมได้ นอกจากนี้ ผู้ประกอบธุรกิจยังสามารถจัดเก็บ VDO ที่บันทึกการพูดคุยกับลูกค้าเพื่อใช้เป็นหลักฐานอ้างอิงในอนาคตได้อีกด้วย

อย่างไรก็ดี การทำ VDO conference อาจมีความเสี่ยงที่ไม่สามารถตรวจสอบการปลอมแปลงตัวตนของผู้ขอเปิดบัญชีได้ ผู้ประกอบธุรกิจจึงต้องมีการติดตามรูปแบบ วิธีการ รวมถึงเทคนิคต่าง ๆ ในการปลอมแปลงตัวตนอย่างต่อเนื่องเพื่อให้รู้เท่าทัน 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

ผู้ประกอบธุรกิจสามารถศึกษามาตรฐานขั้นต่ำด้านเทคนิคในเรื่องคุณภาพของภาพถ่ายลูกค้า และ การทำ VDO conference ได้ที่ภาคผนวก 4 ตัวอย่างมาตรฐานขั้นต่ำด้านเทคนิคในเรื่องคุณภาพของภาพหลักฐาน ภาพถ่ายลูกค้า และการทำ VDO conference เพื่อให้การบริหารความเสี่ยงเพิ่มเติมด้วยวิธีการดังกล่าวมีคุณภาพเพียงพอที่จะนำมาประกอบการทำความรู้จักลูกค้าได้อย่างแท้จริง

อย่างไรก็ดี หากผู้ประกอบธุรกิจพิจารณาว่า ลูกค้าจัดอยู่ในกลุ่มเสี่ยงสูงหรือวงเงินสูง ก็ควรพิจารณานัดพบกับลูกค้าเพื่อพูดคุย และขอดูหลักฐานตัวจริง เพื่อให้เป็นไปตามกรอบการบริหารความเสี่ยงที่เหมาะสม

4. การตรวจสอบช่องทางติดต่อ

ผู้ประกอบธุรกิจควรมีการตรวจสอบช่องทางการติดต่อของลูกค้าที่ได้ให้ไว้ในขั้นตอนการเปิดบัญชีว่าสามารถติดต่อลูกค้าได้จริง ลูกค้าคือเจ้าของช่องทางที่ใช้ในการติดต่อจริง รวมถึงมั่นใจว่า

ผู้ประกอบธุรกิจจะสามารถติดต่อหรือส่งข้อมูลข่าวสารสำคัญไปยังลูกค้าผ่านช่องทางดังกล่าวได้จริง 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 หรือกรณีที่ผู้ขอใช้บริการต้องการพิสูจน์และยืนยันตัวตนผ่าน NDID ซึ่งทั้ง 2 กรณี ผู้ขอใช้บริการจะต้องทำการยืนยันตัวตนกับระบบของผู้ประกอบธุรกิจ หรือกับระบบของ IdP แล้วแต่กรณี **สำนักงานและหน่วยงานที่เกี่ยวข้องได้ร่วมกันกำหนดความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level : AAL) ที่ระดับ 2.1 ตามข้อเสนอแนะมาตรฐานฯ ของ สพธอ. คือให้ใช้ปัจจัยยืนยันตัวตนในประเภทที่แตกต่างกันมากกว่า 1 ปัจจัย** อย่างไรก็ดี หากสถานการณ์เปลี่ยนไปโดยสำนักงานพิจารณาแล้วเห็นว่าผู้ประกอบธุรกิจมีความพร้อม มีเทคโนโลยีที่เหมาะสม สำนักงานอาจปรับเปลี่ยนระดับ AAL เพื่อเป็นการคุ้มครองผู้ลงทุนและสร้างความน่าเชื่อถือในตลาดทุนให้เป็นที่ยอมรับตามมาตรฐานต่อไปได้ในอนาคต

2. การยืนยันตัวตนเพื่อเข้าทำธุรกรรมในระบบ online : เมื่อผู้ขอใช้บริการเปิดบัญชีกับผู้ประกอบธุรกิจแล้วและต้องการเข้าระบบเพื่อทำธุรกรรม จะต้องมีขั้นตอนการยืนยันตัวตนเพื่อให้มั่นใจได้ว่าลูกค้าหรือผู้ได้รับมอบอำนาจจากลูกค้าเป็นผู้เข้ามาใช้งานระบบด้วยตนเอง เพื่อให้ผู้ประกอบธุรกิจบรรลุวัตถุประสงค์ตามหลักเกณฑ์ของสำนักงาน[3] ในเรื่องการให้บริการลูกค้าอย่างเหมาะสม ซึ่งความน่าเชื่อถือในการยืนยันตัวตนในขั้นตอนนี้ **สำนักงานกำหนดความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนขั้นต่ำในระดับ AAL 2.1 ตามข้อเสนอแนะมาตรฐานฯ ของ สพธอ. คือ ให้ใช้ปัจจัยยืนยันตัวตนในประเภทที่แตกต่างกันมากกว่า 1 ปัจจัย (ดูรายละเอียดเรื่องประเภทของปัจจัยยืนยันตัวตนได้ในข้อ 3) สำหรับการ log in เข้าสู่ระบบเพื่อทำธุรกรรมประเภทดังต่อไปนี้จนกว่าจะ log-off ไปจากระบบ โดยจะให้มีการยืนยันตัวตนเป็นรายธุรกรรมอีกหรือไม่ก็ได้**

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

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

[3] ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 35/2557 เรื่อง หลักเกณฑ์ในรายละเอียดเกี่ยวกับการติดต่อและให้บริการลูกค้าสำหรับผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 10 พฤศจิกายน 2554 กำหนดให้ผู้ประกอบธุรกิจต้องมีกระบวนการในการยืนยันตัวตนของลูกค้า (authentication) ที่เหมาะสมและน่าเชื่อถือ เพื่อให้มั่นใจว่าการลงทุนหรือการทำธุรกรรมในผลิตภัณฑ์ในตลาดทุนได้กระทำโดยลูกค้าหรือผู้ได้รับมอบอำนาจจากลูกค้าที่ผู้ประกอบธุรกิจติดต่อและให้บริการ

(3) ธุรกรรมที่เกี่ยวข้องกับการให้ลูกค้าลงนามผูกพันในสัญญาที่เกี่ยวเนื่องกับการใช้บริการธุรกิจหลักทรัพย์และธุรกิจสัญญาซื้อขายล่วงหน้า

(4) ธุรกรรมที่เกี่ยวข้องกับการขอความยินยอม (consent) จากลูกค้า

(5) ธุรกรรมที่เกี่ยวข้องกับการเปลี่ยนแปลงข้อมูลดังต่อไปนี้

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

โดยธุรกรรมอื่นที่มิได้กล่าวถึง ให้ผู้ประกอบธุรกิจกำหนดความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนขั้นต่ำในระดับ AAL 1 ตามข้อเสนอแนะมาตรฐานฯ ของ สพธอ. คือให้ใช้ปัจจัยยืนยันตัวตนอย่างน้อย 1 ปัจจัย

<u>ข้อเสนอแนะเกี่ยวกับการกำหนดวิธีการยืนยันตัวตน</u>

ปัจจัยในการยืนยันตัวตน : การใช้บริการแบบ online นั้น เมื่อลูกค้าต้องการจะเข้าระบบผู้ประกอบธุรกิจจะต้องมีการกำหนดขั้นตอนการยืนยันตัวตนก่อนการเข้าใช้บริการระบบ โดยใช้สิ่งที่เรียกว่าปัจจัยยืนยันตัวตน

การยืนยันตัวตนในโลก online นั้น ตามปกติมักใช้ปัจจัย <u>3 ประเภท</u>ในการยืนยันตัวตน ได้แก่

1. something you have หรือสิ่งที่คุณมี เช่น มือถือที่ลงทะเบียนไว้กับผู้ประกอบธุรกิจ OTP
2. something you know หรือสิ่งที่คุณรู้ เช่น username/password, pin code
3. something you are หรือสิ่งที่คุณเป็น เช่น ลายนิ้วมือ เสียง ม่านตา ใบหน้า

ปัจจัยเหล่านี้ลูกค้าอาจได้รับจากผู้ประกอบธุรกิจ เช่น username/password หรือลงทะเบียนไว้กับผู้ประกอบธุรกิจ เช่น บันทึกลายนิ้วมือไว้ตั้งแต่ขั้นตอนการลงทะเบียนและพิสูจน์ตัวตน เพื่อให้ลูกค้านำกลับมาใช้ในการยืนยันตัวตนเพื่อเข้าใช้ระบบในภายหลัง ซึ่งการกำหนดให้ลูกค้าใช้ปัจจัยยืนยันตัวตนเพื่อเข้าใช้ระบบผู้ประกอบธุรกิจอาจกำหนดวิธีการที่มีความน่าเชื่อถือ ดังต่อไปนี้

ก. กำหนดจำนวนปัจจัยในการยืนยันตัวตนเพื่อเข้าระบบให้เหมาะสมกับความเสี่ยงของธุรกรรม

ปัจจัยในการยืนยันตัวตนแต่ละประเภทมีหลายชนิด ผู้ประกอบธุรกิจสามารถเลือกผสมผสาน ปัจจัยมากกว่า 1 อย่างเพื่อช่วยเพิ่มความน่าเชื่อถือในการยืนยันตัวตน ทั้งนี้ การจะเลือกใช้ปัจจัยประเภทหรือชนิดใดมาประกอบกันนั้น ผู้ประกอบธุรกิจอาจพิจารณาว่า ปัจจัยทั้ง 2 อย่างนั้น เมื่อใช้ร่วมกันแล้วจะช่วยให้การยืนยันตัวตนมีความน่าเชื่อถือเพิ่มขึ้น เช่น การใช้ username/password (something you know)

ประกอบกับ OTP (something you have) เพราะหากมีผู้ไม่ประสงค์ดีขโมย username/password ของลูกค้าไปได้ แต่ไม่ได้รับ OTP ก็ไม่สามารถทำธุรกรรมได้ เป็นต้น

นอกจากนั้น หากสามารถใช้ช่องทางที่แตกต่างกันในการยืนยันตัวตน (out-of-band devices) ก็จะยิ่งเพิ่มความน่าเชื่อถือได้มากยิ่งขึ้น เช่น ส่ง OTP ผ่าน SMS (ระบบ cellular) ให้ลูกค้านำไปกรอกผ่านโปรแกรมบนระบบอินเตอร์เน็ต ซึ่งหากมีผู้ไม่ประสงค์ดีขโมย username/password ของลูกค้าไปได้ แต่ไม่ได้ขโมยโทรศัพท์มือถือที่ใช้รับ SMS OTP ไปด้วย ก็ไม่สามารถทำธุรกรรมได้เช่นกัน

ข. กำหนดคุณภาพของปัจจัยให้เหมาะสม[4]

นอกเหนือจากการใช้ปัจจัยมากกว่า 1 ประเภทแล้ว ผู้ประกอบธุรกิจสามารถกำหนดคุณภาพของปัจจัยแต่ละชนิดให้เหมาะสมเพื่อให้มั่นใจว่าการยืนยันตัวตนนั้นมีความน่าเชื่อถือ ยกตัวอย่างเช่น

- password : ควรกำหนดตัวเลขผสมตัวอักษร เล็ก-ใหญ่ มีความยาว 8 ตัวขึ้นไป โดยไม่เป็นรหัสผ่านที่อยู่ในรายชื่อรหัสลับที่ไม่ปลอดภัย เช่น รหัสผ่านที่เคยถูกโจมตีในอดีต เป็นต้น
- OTP : มีความยาว 6 ตัวขึ้นไป และมีอายุจำกัด เป็นต้น
- มีการจำกัดจำนวนครั้งในการยืนยันตัวตนผิดพลาด เช่น ไม่ให้มีความผิดพลาดต่อเนื่องเกิน 100 ครั้ง (เพื่อป้องกัน online guessing attack) และระงับการยืนยันตัวตนของลูกค้าดังกล่าว

ผู้ประกอบธุรกิจสามารถป้องกันการโจมตีที่ทำให้ผู้ใช้บริการถูกระงับการใช้บริการเนื่องจากยืนยันตัวตนผิดพลาดครบจำนวนที่กำหนด โดยอาจเลือกวิธีการป้องกัน เช่น ให้ลูกค้าผ่านแบบทดสอบ CAPTCHA ก่อนการยืนยันตัวตนแต่ละครั้ง หรือหน่วงเวลาของการยืนยันตัวตนเพิ่มขึ้นทุกครั้งที่ลูกค้ายืนยันตัวตนผิดพลาด หรือยอมรับการยืนยันตัวตนจาก IP address ที่ลูกค้าเคยยืนยันตัวตนสำเร็จมาแล้วเท่านั้น

เมื่อลูกค้ายืนยันตัวตนสำเร็จ ผู้ประกอบธุรกิจควรล้างข้อมูลการยืนยันตัวตนผิดพลาดของลูกค้าจาก IP address ที่ใช้ยืนยันตัวตนสำเร็จ

- Biometric : เป็นปัจจัยที่มีโอกาสเกิดความผิดพลาดในการยอมรับ (false matching) เนื่องจากอยู่บนพื้นฐานของความน่าจะเป็น ในขณะที่การยืนยันตัวตนด้วยปัจจัยประเภทอื่นใช้การเปรียบเทียบว่าข้อมูลตรงกัน ไม่เป็นข้อมูลลับ เช่น ใบหน้าหรือลายนิ้วมือที่สามารถถูกขโมยได้ ทำให้การใช้งานปัจจัยประเภทนี้ทำได้จำกัด เช่น
  - ควรใช้เป็นส่วนหนึ่งของการยืนยันตัวตนแบบหลายปัจจัย โดยใช้ร่วมกับสิ่งที่คุณมี (something you have) เท่านั้น

[4] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน DIGITAL IDENTITY GUIDELINE FOR THAILAND AUTHENTICATION เวอร์ชัน 1.0 https://standard.etda.or.th/rec (ขมธอ. 20-2561)

- ควรมีการเก็บตัวอย่าง biometric ที่มีคุณภาพ
- เทคโนโลยีที่ใช้เปรียบเทียบควรมีความแม่นยำในระดับสูงสอดคล้องกับมาตรฐานของภาคการเงินและมาตรฐานสากล
- ควรจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดได้ไม่เกิน 5 ครั้ง

ค. การใช้ช่องทางรับส่งปัจจัยยืนยันตัวตนที่มีความมั่นคงปลอดภัยสูง

การยืนยันตัวตนผ่านระบบอิเล็กทรอนิกส์นั้น มีความเสี่ยงที่ผู้ไม่ประสงค์ดีจะกระทำการด้วยวิธีการต่าง ๆ ที่จะทำให้เกิดความผิดพลาดในการยืนยันตัวตน เนื่องมาจากกระบวนการให้บริการลูกค้าผ่านระบบอิเล็กทรอนิกส์นั้น ต้องมีการรับ-ส่งข้อมูลระหว่างกันผ่านระบบอิเล็กทรอนิกส์ซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่ประสงค์ดีจะใช้วิธีการต่าง ๆ ที่จะทำให้เกิดความผิดพลาดในการยืนยันตัวตน เช่น เข้ามาแก้ไขข้อมูลหรือแอบดักขโมยข้อมูล เช่น username/password หรือ OTP ที่รับ-ส่งระหว่างกัน เป็นต้น ดังนั้น ผู้ประกอบธุรกิจจึงควรพัฒนาช่องทางการรับ-ส่งข้อมูลยืนยันตัวตนที่มีความมั่นคงปลอดภัยสูง เช่น ช่องทางที่มีการเข้ารหัส (encrypt) เพื่อสร้างความน่าเชื่อถือในการให้บริการ และผู้ประกอบธุรกิจควรติดตามความเปลี่ยนแปลงทางเทคโนโลยีอยู่ตลอด เพื่อปรับเปลี่ยนมาตรฐานหรือวิธีการป้องกันการโจมตีให้ทันต่อสถานการณ์อยู่เสมอ เพื่อให้ระบบคงความมั่นคงปลอดภัยสูงได้ตลอดเวลา

รายละเอียดเกี่ยวกับการยืนยันตัวตนนั้นยังมีอีกหลายเรื่อง ผู้ประกอบธุรกิจสามารถศึกษาข้อมูลเพิ่มเติมได้ที่ แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน (Digital Identity Guideline for Thailand – Authentication)[5] ซึ่งจัดทำโดย สพธอ.

[5] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน DIGITAL IDENTITY GUIDELINE FOR THAILAND AUTHENTICATION เวอร์ชัน 1.0 https://standard.etda.or.th/rec (ขมธอ. 20-2561)

1.3 การทำความรู้จักลูกค้าในเชิงลึก (CLIENT DUE DILIGENCE : CDD)

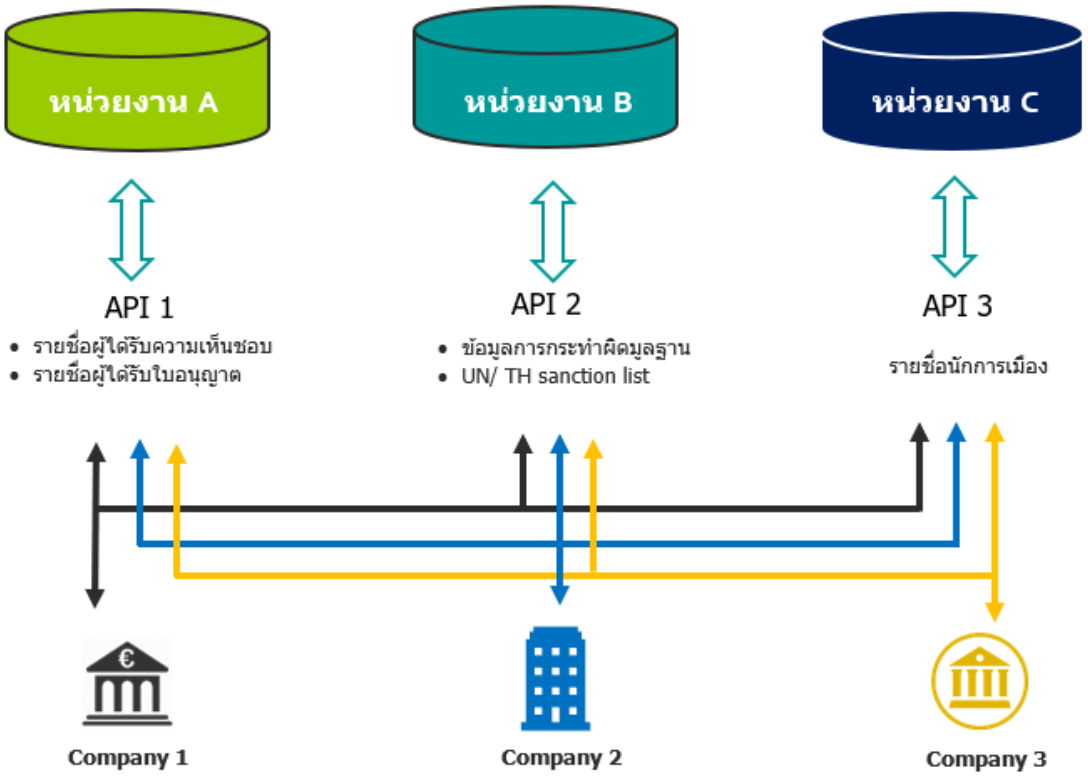
การทำ CDD นั้น ผู้ประกอบธุรกิจอาจใช้เทคโนโลยีเข้ามาช่วยเพื่อลดภาระในการดำเนินการในขั้นตอนนี้ เช่น การใช้ Application Program Interface: API เชื่อมโยงข้อมูลกับหน่วยงานที่เป็นเจ้าของข้อมูลที่ต้องการตรวจสอบโดยตรงเพื่อดึงข้อมูลที่เกี่ยวข้องกับการทำ CDD ลูกค้ามาตรวจสอบ จากเดิมที่ต้องค้นหาข้อมูลแต่ละเรื่องที่กระจายอยู่ตามเว็บไซต์ของหน่วยงานรัฐต่าง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

ในอนาคตหากมีฐานข้อมูลกลางของหน่วยงานรัฐหรือระบบที่เอกชนพัฒนาขึ้น หรือหน่วยงานกลางที่อาจมีการจัดตั้งขึ้นโดยเฉพาะเพื่อรวบรวมหรือเป็นศูนย์กลางในการเชื่อมโยงข้อมูลดังกล่าว เช่น ระบบ Digital ID ที่หน่วยงานรัฐและเอกชนซึ่งมีข้อมูลที่น่าเชื่อถือจะพิจารณาเข้ามาร่วมเป็นสมาชิกในฐานะ 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 ความเสี่ยงที่ระบบหรือบัญชีลูกค้าจะถูก hack ขโมยข้อมูลจากผู้ไม่ประสงค์ดี 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[6] ที่ผู้ประกอบธุรกิจสามารถนำมาปรับใช้เพิ่มเติมในการกำหนดในเรื่องอื่น ๆ ที่เกี่ยวข้อง เช่น การกำหนดให้มีการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ การควบคุมการเข้ารหัสข้อมูล การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (outsource) การบริหารจัดการ

[6] ประกาศแนวปฏิบัติ ที่ นป. 3/2559 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 12 กันยายน 2559

เหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เป็นต้น

2.2 การจัดการและจัดเก็บข้อมูล

<u>การคุ้มครองข้อมูลของลูกค้า</u>

การรวบรวมข้อมูลลูกค้าเพื่อประกอบการทำ KYC นี้ ผู้ประกอบธุรกิจต้องคำนึงถึงการคุ้มครองข้อมูลของลูกค้า โดยต้องมีการจัดการและจัดเก็บข้อมูลอย่างเหมาะสม ป้องกันการเข้าถึงข้อมูลอย่างไม่ถูกต้องหรือขัดกับกฎหมาย ตามเกณฑ์ที่สำนักงานกำหนด

กฎเกณฑ์ของสำนักงาน[7] กำหนดให้ผู้ประกอบธุรกิจจัดเก็บข้อมูลที่เกี่ยวข้องในการให้บริการลูกค้าไว้ในรูปแบบที่เหมาะสม เช่น มีระบบจัดเก็บข้อมูลลูกค้าที่รัดกุม เป็นระเบียบ มีความปลอดภัยในการจัดเก็บ สามารถป้องกันการแก้ไข หรือถูกทำลาย หรือมีการเข้ารหัสข้อมูล (data encryption) เพื่อสร้างความปลอดภัยให้กับข้อมูล กำหนดสิทธิในการเข้าถึงข้อมูลเพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าดูข้อมูล และมีการสำรองข้อมูลเพื่อป้องกันการสูญหาย เป็นต้น โดยเฉพาะอย่างยิ่งหากมีการเก็บข้อมูล sensitive ของลูกค้า เช่น ข้อมูลส่วนบุคคล ข้อมูลภาพถ่ายหรือ biometric ของลูกค้า ต้องใช้ระบบที่มีความปลอดภัยสูงในการจัดเก็บข้อมูลเหล่านี้ เพราะหากรั่วไหลไปสู่บุคคลอื่นจะสร้างความเสียหายต่อเจ้าของข้อมูลได้มาก นอกจากนั้น ผู้ประกอบธุรกิจต้องเก็บรักษาข้อมูลตามระยะเวลาที่สำนักงานประกาศกำหนด เพื่อสามารถใช้อ้างอิงหรือเพื่อการตรวจสอบได้ในอนาคต

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

นอกจากกฎหมายของไทยที่ผู้ประกอบธุรกิจต้องปฏิบัติตามแล้ว ผู้ประกอบธุรกิจควรพิจารณาระมัดระวังการดำเนินการกับข้อมูลส่วนบุคคลของลูกค้าที่ได้รับการคุ้มครองโดยกฎหมายอื่น เช่น General Data Protection Regulation[8] หรือ GDPR ซึ่งผู้ประกอบธุรกิจที่มีสถานประกอบการอยู่ภายในสหภาพยุโรป หรือมีการประมวลผลข้อมูลที่เกี่ยวข้องกับการเสนอสินค้าหรือบริการให้แก่บุคคลผู้พำนักในสหภาพยุโรป หรือมีการประมวลผลข้อมูลซึ่งเกี่ยวข้องกับการเฝ้าสังเกตพฤติกรรมที่เกิดขึ้นในสหภาพยุโรปและรวมถึงประเทศที่มีผลผูกพันทางกฎหมายกับประเทศสหภาพยุโรป ต้องระมัดระวังการดำเนินการเกี่ยวกับข้อมูลลูกค้า โดยต้องดำเนินการให้เป็นไปตาม GDPR ด้วย ทั้งนี้ แม้ข้อมูล หลักฐานต่าง ๆ ที่จะเกิดขึ้นในกระบวนการ e-KYC นั้น

[7] ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 35/2556 เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงานและการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า (ฉบับประมวล)

[8] https://gdpr-info.eu/

จะอยู่ในรูปแบบที่แตกต่างจากการทำ KYC ในรูปแบบเดิมที่เป็นกระดาษ ใช้วิธีการจัดเก็บข้อมูล หลักฐานต่าง ๆ ที่แตกต่างกัน แต่ยังคงใช้หลักการเดียวกัน

ผู้ประกอบธุรกิจควรศึกษารายละเอียดในกฎหมาย/กฎเกณฑ์ต่าง ๆ ให้ชัดเจนเพื่อให้การดำเนินการเก็บรักษาข้อมูลมีประสิทธิภาพเหมาะสมและหลีกเลี่ยงโทษที่อาจเกิดขึ้นจากความผิดพลาดได้

ภาคผนวก

ภาคผนวก 1: ความหมายของ KYC และ Ecosystem

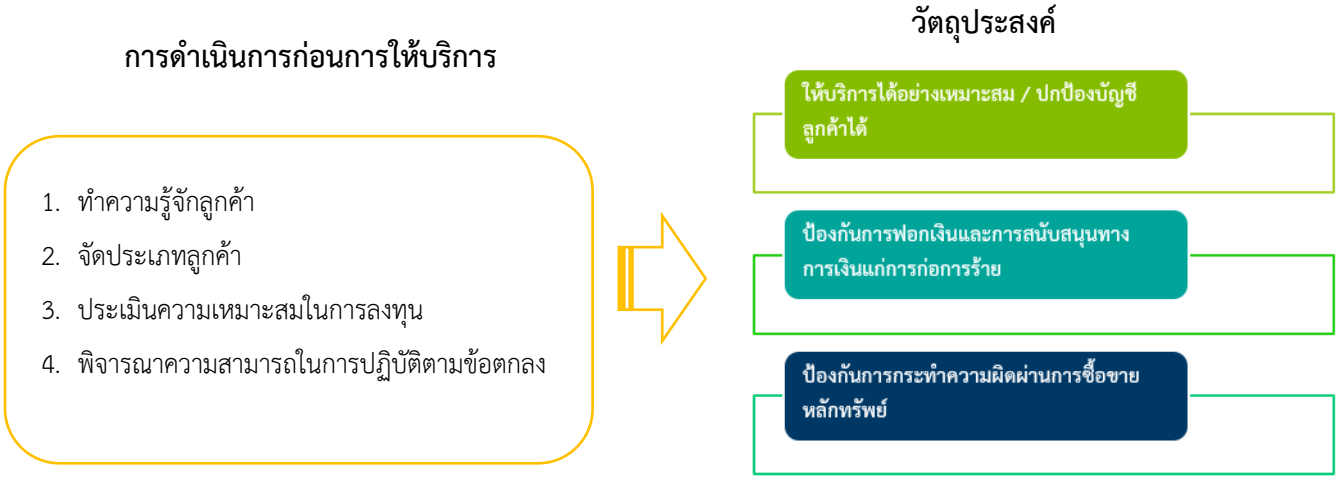
การทำความรู้จักลูกค้า (Know Your Client : KYC) คือ การรวบรวมและประเมินข้อมูลต่าง ๆ ของลูกค้าก่อนที่ผู้ประกอบธุรกิจจะให้บริการ โดยจะต้องรวบรวมข้อมูลส่วนบุคคลเพื่อให้รู้ว่าลูกค้าเป็นใคร

นอกจากนี้ ในการทำ KYC ยังหมายความรวมถึง การทำความรู้จักลูกค้าในเชิงลึก (Client Due Diligence : CDD) ด้วย โดยการรวบรวมข้อมูลต่าง ๆ ของลูกค้า ได้แก่ รายได้และแหล่งที่มาของรายได้ ฐานะการเงิน ความรู้ ความเข้าใจและประสบการณ์ลงทุน วัตถุประสงค์ในการลงทุน ไปจนถึงความเสี่ยงที่ยอมรับได้ เพื่อสามารถให้บริการในธุรกิจหลักทรัพย์และสัญญาซื้อขายล่วงหน้าตามขอบเขตที่ผู้ประกอบธุรกิจได้รับ อนุญาตจากสำนักงาน เช่น การประเมินความเหมาะสมในการลงทุน การให้คำแนะนำ การให้วงเงิน การให้บริการซื้อขายหลักทรัพย์ได้อย่างเหมาะสม มีประสิทธิภาพ ปกป้องผลประโยชน์และคุ้มครองลูกค้า ซึ่งมักจะเรียกรวมกันว่า การทำ KYC/CDD

KYC framework ของสำนักงาน

สำนักงานกำหนดให้ผู้ประกอบธุรกิจต้องทำ KYC ก่อนที่จะให้บริการอย่างน้อยเพื่อวัตถุประสงค์หลัก 3 ประการ คือ 1) การทำความรู้จักตัวตนที่แท้จริงของลูกค้าเพื่อสามารถให้บริการลูกค้าได้อย่างเหมาะสม เช่น การประเมินความเหมาะสมในการลงทุนในผลิตภัณฑ์ตลาดทุนเพื่อที่จะให้บริการที่สอดคล้องกับความเสี่ยงที่ลูกค้าจะยอมรับได้ 2) การป้องกันการฟอกเงินและการสนับสนุนทางการเงินแก่การก่อการร้าย และ 3) การป้องกันการกระทำความผิดผ่านการใช้บัญชีในการซื้อขายหลักทรัพย์

โดยกฎเกณฑ์เกี่ยวกับการทำ KYC ของสำนักงาน กำหนดให้ต้องดำเนินการเพื่อให้เป็นไปตามวัตถุประสงค์ข้างต้นซึ่งสรุปได้ ดังนี้



เดิมการทำ KYC ผู้ประกอบธุรกิจส่วนใหญ่จะใช้วิธีการรวบรวมข้อมูลจากลูกค้าผ่านใบคำขอเปิดบัญชี และขอหลักฐานเป็นสำเนาบัตรประชาชน สำเนาหน้าสมุดบัญชีธนาคาร และ statement ทางการเงินย้อนหลัง นอกจากนี้ ยังให้ลูกค้าทำแบบประเมินความเหมาะสมในการลงทุน (suitability test) โดยทุกขั้นตอนทำบนเอกสารที่เป็นกระดาษ (paper work) หลังจากนั้น ผู้ประกอบธุรกิจก็จะนำข้อมูลที่ได้รับมาตรวจสอบความมีตัวตนของลูกค้า เช่น ดูว่าข้อมูลในใบคำขอฯ ตรงกับสำเนาบัตรประชาชน มีการโทรศัพท์ยืนยันการเปิดบัญชีกับลูกค้าหรือบุคคลอ้างอิงตามข้อมูลที่ได้รับมีการประเมินความเหมาะสมในการลงทุน แล้วจึงจัดกลุ่มความเสี่ยง กำหนดวงเงิน และอนุมัติเปิดบัญชี รวมถึงจัดเก็บเอกสารเปิดบัญชีดังกล่าวไว้เพื่อการตรวจสอบตามความจำเป็นในภายหลัง

การพิสูจน์และยืนยันตัวตนที่ผู้ประกอบธุรกิจปฏิบัติเปรียบเทียบกับเกณฑ์ KYC

	การพิสูจน์ตัวตนลูกค้า (Identity proofing)+ การทำความรู้จักลูกค้าเชิงลึก (CDD)	Authentication (ยืนยันตัวตนเพื่อเข้าใช้ระบบ)
กฎเกณฑ์ ก.ล.ต.	**ทำความรู้จักลูกค้า และผู้รับผลประโยชน์ที่แท้จริง + จัดประเภท/ ประเมินความเหมาะสมในการลงทุน/ พิจารณาความสามารถในการปฏิบัติตามข้อตกลง**	**ตรวจสอบว่าลูกค้าเป็นผู้เข้าใช้ระบบ**
วิธีปฏิบัติของผู้ประกอบธุรกิจ	**<u>ลูกค้า</u> - กรอกข้อมูล แนบหลักฐาน + ลายเซ็นจริง ส่งเป็น hard copy ให้ บล. - ทำ suitability test (บนกระดาษ / ระบบ) <u>บล.</u> - ตรวจสอบข้อมูลกับหลักฐาน, ตรวจสอบรายชื่อที่กฎหมายกำหนด, พิจารณาอาชีพ รายได้ ฐานะการเงิน, วัตถุประสงค์ในการลงทุน, โทรสอบยัน - ประเมิน + แจ้งผล suitability test + ให้คำแนะนำ**	**<u>ตัวอย่างวิธีการ</u> - บล. ส่ง password ในการเข้าระบบครั้งแรกให้ลูกค้าทางอีเมล - ลูกค้าใช้ password + OTP ที่ บล. ส่งให้เข้าระบบ + ยืนยันตัวตนด้วยวันเดือนปีเกิด**

ปัจจุบันแม้เทคโนโลยีจะพัฒนาอย่างก้าวกระโดด ลูกค้าปรับเปลี่ยนวิถีชีวิตเข้าสู่รูปแบบ online lifestyle มากขึ้น และผู้ประกอบธุรกิจให้ความสนใจปรับเปลี่ยนการให้บริการต่าง ๆ เข้าสู่รูปแบบ online อย่างไรก็ดี การทำ e-KYC ในตลาดทุนในช่วงเริ่มต้นเป็นการนำมาใช้ในขั้นตอนที่ไม่ซับซ้อน เช่น เพื่อจัดเก็บข้อมูลหรือลดการใช้กระดาษ แต่ก็ยังไม่สามารถอำนวยความสะดวกให้แก่ลูกค้าได้มากนัก เนื่องจากยังมีประเด็นข้อกฎหมายเข้ามาเกี่ยวข้องซึ่งมีกรณีตัวอย่างเกิดขึ้นน้อย และมีความเสี่ยงในการนำเรื่องเข้าสู่การพิจารณาของศาล นอกจากนี้ หากเป็นการทำธุรกรรมเปิดบัญชีผ่านช่องทาง online โดยไม่ได้พบเห็นลูกค้าต่อหน้า จะมีประเด็นเกี่ยวกับกระบวนการและระบบงานในการทำ KYC ที่เข้มงวดมากเพื่อให้รู้จักตัวตนลูกค้าที่มาใช้บริการ เพื่อสามารถให้บริการได้อย่างเหมาะสม ป้องกันการกระทำความผิด และปกป้องคุ้มครองทรัพย์สินของลูกค้า เนื่องจากหากเกิดความผิดพลาด เช่น มีการใช้

ตัวตนปลอมหรือใช้ข้อมูลบุคคลอื่นในการเปิดบัญชี มีการซื้อขายแทนกันหรือการถูกลักลอบใช้บัญชีซื้อขาย การถูกยักยอกเงินโดยเจ้าของบัญชีไม่รู้ตัว จะก่อให้เกิดความไม่น่าเชื่อถือในการให้บริการในตลาดทุนได้

อย่างไรก็ดี ด้วยสภาพแวดล้อมที่ความก้าวหน้าด้านเทคโนโลยีมีการพัฒนาอย่างรวดเร็ว ลูกค้าให้ความสำคัญกับบริการที่สะดวก รวดเร็วมากขึ้นเรื่อย ๆ ในระยะ 2 ปีที่ผ่านมา การเปิดบัญชีซื้อขายหลักทรัพย์ online และการทำ e-KYC จึงถูกหยิบยกขึ้นมาหารือกันระหว่างสำนักงานและผู้ประกอบธุรกิจอย่างต่อเนื่อง โดยผู้ประกอบธุรกิจหลายรายมีแนวคิดที่ต้องการพัฒนาระบบเปิดบัญชี online และทำ e-KYC ทั้งกระบวนการแบบไร้กระดาษ (paperless) หรือใช้เทคโนโลยีมาช่วยในการพิสูจน์ตัวตน เพื่อแข่งขันกันตอบสนองต่อ lifestyle ของลูกค้าที่เปลี่ยนแปลงไป

เมื่อจะปรับเปลี่ยนการทำ KYC รูปแบบเดิมเป็น e-KYC สำหรับการให้บริการธุรกรรมทางการเงินการลงทุนนั้น ประเด็นสำคัญที่ผู้ประกอบธุรกิจต้องมั่นใจได้ คือ จะต้องมีวิธีการที่น่าเชื่อถือที่สามารถระบุตัวตน (identify) ของบุคคลในโลก digital ได้ว่าเป็นบุคคลใดในโลก physical

การพิสูจน์ตัวตนบุคคลด้วยวิธีการอิเล็กทรอนิกส์ที่ใช้กันทั่วไป เริ่มจากผู้ให้บริการต้องตรวจสอบตัวตนทางกายภาพ (physical) ของลูกค้าก่อน (เช่น การตรวจสอบบัตรประชาชนกับบุคคลจริง) เมื่อได้ข้อมูลตัวตนของลูกค้ามาแล้ว จึงสร้างตัวตนในโลกดิจิทัลที่สามารถอ้างอิงกันและกันได้ และออกสิ่งที่ใช้ยืนยันตัวตน (authenticator เช่น username/password) ให้ตัวตนในโลกดิจิทัลนำกลับมาใช้ยืนยันว่าตนเองเป็นบุคคลคนเดียวกันกับตัวตนในโลก physical ที่ผู้ประกอบธุรกิจได้เคยตรวจสอบตัวตนไว้

ตัวอย่างกระบวนการพิสูจน์ตัวตนแบบง่าย เช่น เมื่อลูกค้าต้องการเปิดบัญชีกับบริษัทหลักทรัพย์ (“บล.”) จะจัดส่งใบคำขอเปิดบัญชีที่กรอกข้อมูลต่าง ๆ และแนบหลักฐาน คือ สำเนาบัตรประชาชนให้ บล. เพื่อให้ บล. ใช้ประกอบการตรวจสอบตัวตนลูกค้าว่าเป็นใคร โดยอ้างอิงจากข้อมูลในใบคำขอฯ และข้อมูลจากบัตรประชาชน (อาจใช้วิธีการตรวจสอบเพิ่มเติมไปยังฐานข้อมูลกรมการปกครอง เพื่อให้มั่นใจมากขึ้นว่าบัตรดังกล่าวยังสามารถใช้ได้ และไม่ถูกปลอมแปลง) เมื่อ บล. ตรวจสอบตัวตนจนมั่นใจแล้วว่า ผู้มาสมัครใช้บริการกับข้อมูลที่มีในหลักฐานเป็นคนเดียวกัน จึงจะออก username/password ให้ลูกค้าใช้ในการทำธุรกรรมในระบบดิจิทัลของ บล. ซึ่งทำให้ บล. สามารถอ้างอิงไปยังตัวตนของลูกค้าคนนั้นได้ เมื่อลูกค้าเข้าทำธุรกรรม online ด้วย username/password ดังกล่าว บล. จึงรู้ว่าผู้ที่ใช้ username/password นี้ในระบบดิจิทัลของ บล. เป็นใครในโลก physical

กระบวนการที่กล่าวข้างต้น ไม่ว่าจะเป็นการทำในรูปแบบเดิมคือ ทำบนกระดาษ หรือทำแบบ online ทั้งกระบวนการก็ต้องมีประสิทธิภาพ น่าเชื่อถือ เพื่อให้มั่นใจว่าไม่มีการปลอมแปลงตัวตนเป็นบุคคลอื่น ซึ่งก็ตามมาด้วยความยุ่งยาก เสียเวลาและค่าใช้จ่ายสูง

อย่างไรก็ดี ปัจจุบันมีแนวคิดที่ช่วยสร้างเครื่องมือที่ช่วยตอบโจทย์การพิสูจน์และยืนยันตัวตนบนโลกดิจิทัลให้ง่ายขึ้นในหลายประเทศ เช่น อินเดีย สิงคโปร์ และอังกฤษ สรุปได้ดังนี้

อินเดีย : Aadhaar

ปัญหาการระบุตัวตนของประชากรอินเดีย เกิดขึ้นจากความแตกต่างด้านการเมืองและเศรษฐกิจที่ซับซ้อนของอินเดียที่มีจำนวนประชากรมากกว่าพันล้านคน เงินอุดหนุนจากรัฐสำหรับคนยากจนไม่สามารถไปถึงมือผู้ที่ควรได้รับจริง ๆ อีกทั้งการเข้าถึงบริการที่สำคัญ ๆ เช่น สถาบันการเงิน ก็เป็นไปได้ยาก รัฐบาลอินเดียเล็งเห็นถึงปัญหานี้จึงจัดตั้งหน่วยงาน Unique Identification Authority of India (UIDAI)[9] ขึ้นเพื่อแก้ปัญหาดังกล่าว ในปี 2551 โดย UIDAI ได้ออกแบบการระบุตัวตนของบุคคลและการจัดเก็บข้อมูล และร่วมกับหน่วยงานอื่น ๆ ดำเนินการขึ้นทะเบียนและจัดเก็บข้อมูลประชากร (ชื่อ-นามสกุล อายุ เพศ และที่อยู่ที่ติดต่อได้ รวมถึงลายนิ้วมือ 10 นิ้ว และม่านตา) เพื่อระบุตัวตนคนอินเดีย โดยทุกคนที่มาลงทะเบียนจะได้รับบัตรที่มีชื่อว่า Aadhaar ซึ่งมีหมายเลขประจำตัว 12 หลัก โดยมีการจัดเก็บข้อมูลที่ประชาชนลงทะเบียนไว้ในฐานข้อมูลกลาง (centralized model) และมีหน่วยงานของรัฐเป็นผู้ดูแล

Aadhaar ช่วยให้การระบุตัวตนคนอินเดียทำได้ง่ายและรวดเร็วมากยิ่งขึ้น คนอินเดียไม่ต้องเตรียมเอกสารระบุตัวตนซ้ำแล้วซ้ำเล่าในการติดต่อขอใช้บริการ แต่เปลี่ยนเป็นการระบุตัวตนผ่านวิธีการทางอิเล็กทรอนิกส์แทนซึ่งใช้เวลาไม่นาน Aadhaar สามารถใช้ประโยชน์ในการเข้าถึงบริการจากสถาบันการเงิน เช่น การเปิดบัญชีธนาคารและการใช้ micro ATMs รวมไปถึงการขอรับสวัสดิการจากรัฐที่เมื่อระบุตัวตนประชาชนที่เข้าข่ายสมควรได้รับความช่วยเหลือได้ สวัสดิการก็ไปถึงมือได้ นอกจากนั้น Aadhaar ยังสามารถใช้ในการทำใบขับขี่ หรือลงทะเบียนโทรศัพท์มือถือ ช่วยให้ประชาชนสามารถเข้าถึงระบบสาธารณูปโภคได้ง่ายขึ้นอีกด้วย

สิงคโปร์ : MyInfo

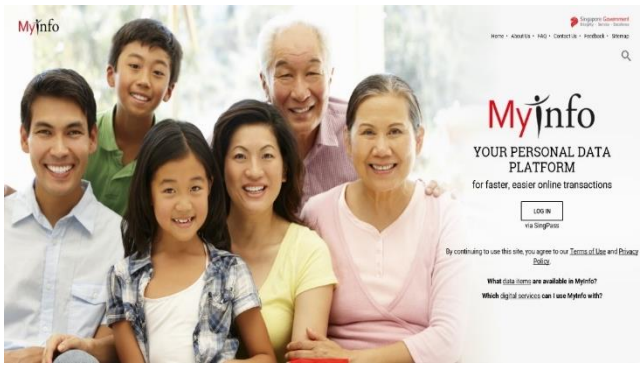
รัฐบาลสิงคโปร์เองก็มีแนวคิดในการผลักดันการพิสูจน์และยืนยันตัวตนให้เข้าสู่รูปแบบดิจิทัลเพื่อเพิ่มความสะดวกและลดความซ้ำซ้อนในการใช้บริการ โดยได้พัฒนาระบบ MyInfo[10] ซึ่งเป็นระบบที่สามารถแชร์ข้อมูลประชาชนระหว่างหน่วยงานรัฐและเอกชน เช่น ธนาคาร ช่วยให้ประชาชนที่ต้องการใช้บริการต่าง ๆ ไม่ต้องกรอกข้อมูลซ้ำ ๆ ช่วยลดความผิดพลาดในการกรอกข้อมูลลงในแบบฟอร์มด้วยตนเอง และไม่ต้องยื่นหลักฐานจริงแต่ใช้การแชร์ข้อมูลจากฐานข้อมูลกลางแทน โดยข้อมูลสำคัญ ๆ เช่น รายได้ จะต้องมีการให้ความยินยอมก่อนการแชร์ข้อมูล

[9] https://uidai.gov.in/

[10] www.myinfo.gov.sg.

ข้อมูลในฐานข้อมูลของระบบ MyInfo ได้แก่ ข้อมูลส่วนบุคคลต่าง ๆ เช่น ชื่อ-นามสกุล เลขที่บัตรประจำตัวประชาชน วันเดือนปีเกิด ช่องทางติดต่อ (เช่น หมายเลขโทรศัพท์มือถือ อีเมล ที่อยู่) รายได้ การศึกษาและการทำงาน ครอบครัว ไปจนถึงการครอบครองยานพาหนะ

ปัจจุบันมีหน่วยงานภาครัฐ 53 หน่วยงาน และเอกชนกว่า 200 บริษัท (ข้อมูล ณ ธ.ค. 2562) เชื่อมต่อระบบกับ MyInfo เช่น การสมัคร Public Housing Flats หรือ Baby Bonus Scheme นอกเหนือจากบริการภาครัฐ ยังมีธนาคารหลายแห่งที่ให้ลูกค้าใช้ข้อมูลจาก MyInfo เพื่อการเปิดบัญชีธนาคารได้โดยไม่ต้องกรอกแบบฟอร์มหรือแสดงหลักฐานอีก ช่วยให้การเปิดบัญชีธนาคารทำได้รวดเร็วยิ่งขึ้นด้วย



อังกฤษ : GOV.UK Verify

อังกฤษเป็นอีกประเทศหนึ่งที่รัฐบาลพัฒนาระบบการพิสูจน์ตัวตนที่ช่วยลดความซ้ำซ้อนและสร้างความรวดเร็วในการใช้บริการภาครัฐในรูปแบบ online ได้ รัฐบาลโดยหน่วยงาน Government Digital Service (GDS) ได้จัดทำระบบที่มีชื่อว่า GOV.UK Verify ซึ่งเริ่มใช้งานในปี 2016

กระบวนการพิสูจน์ตัวตนของระบบดังกล่าว คือ เมื่อมีผู้ต้องการใช้บริการภาครัฐทาง online บุคคลผู้นั้นต้องไปพิสูจน์ตัวตนและสร้างตัวตนดิจิทัลกับผู้ให้บริการยืนยันตัวตน หรือ Identity Providers ก่อน โดยเลือก Identity Provider ที่ต้องการจาก Identity Providers (ปัจจุบันมีจำนวน 5 ราย (ข้อมูล ณ ธ.ค. 2562)) ที่ได้รับความเห็นชอบจากรัฐให้ทำหน้าที่พิสูจน์ตัวตน โดย Identity Provider จะขอข้อมูลจากผู้ที่ต้องการใช้บริการและทำการตรวจสอบข้อมูลนั้นกับแหล่งข้อมูลที่น่าเชื่อถือ ซึ่ง Identity Provider แต่ละรายจะมีวิธีการพิสูจน์ตัวตนที่แตกต่างกันไป อย่างไรก็ดี กระบวนการพิสูจน์ตัวตนนี้จะใช้เวลาเพียง 5-15 นาทีเท่านั้น หลังจากนั้นผู้ใช้บริการก็จะสามารถใช้ตัวตน digital นั้นเข้าใช้บริการภาครัฐที่ต้องการในครั้งต่อ ๆ ไปโดยไม่ต้องพิสูจน์ตัวตนอีก

ปัจจุบันมีบริการภาครัฐมากกว่า 16 บริการ (ข้อมูล ณ ธ.ค. 2562) ที่สามารถใช้การพิสูจน์ตัวตนผ่าน GOV.UK Verify ได้ เช่น การตรวจสอบภาษีเงินได้ ตรวจสอบสวัสดิการของรัฐ หรือการดูข้อมูลใบขับขี่ เป็นต้น

การพัฒนา GOV.UK Verify ช่วยลดภาระทั้งผู้ขอใช้บริการและหน่วยงานภาครัฐที่เดิมต้องพิสูจน์ตัวตนซ้ำ ๆ ช่วยลดระยะเวลาการเข้าใช้บริการ ช่วยให้การพิสูจน์ตัวตนมีความปลอดภัย เนื่องจากไม่มีการรวมศูนย์ข้อมูลไว้ที่เดียว ไม่มีการแชร์ข้อมูลโดยไม่จำเป็น และได้มาตรฐาน เนื่องจาก Identity Providers มีขั้นตอนการพิสูจน์ตัวตนที่ได้มาตรฐานของรัฐและมาตรฐานสากลในเรื่องความมั่นคงปลอดภัยและการคุ้มครองข้อมูลของผู้ขอใช้บริการด้วย

ระบบ Digital ID ตัวช่วยพิสูจน์และยืนยันตัวตนของไทย

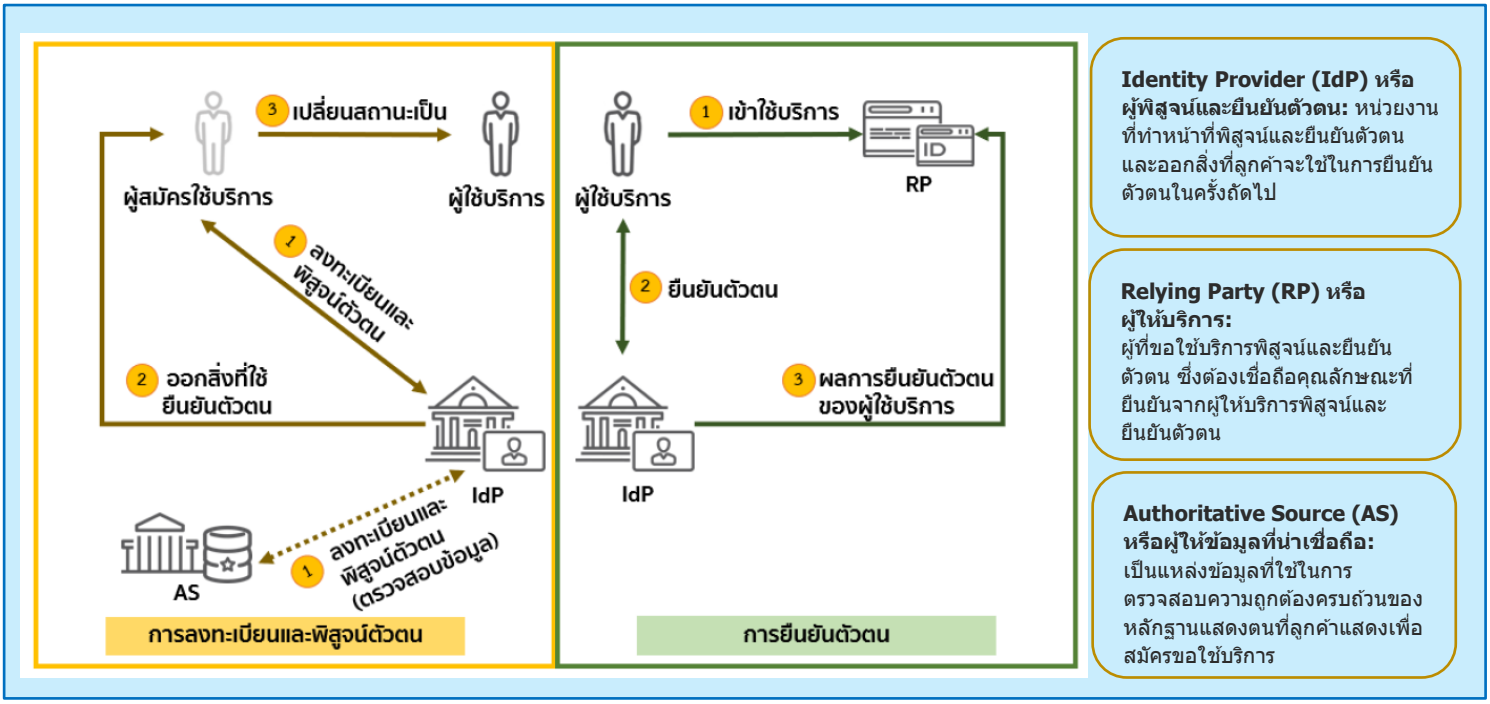
สำหรับประเทศไทย ในปี 2561 รัฐบาลได้สนับสนุนให้เกิดการพัฒนาโครงสร้างพื้นฐานของประเทศที่ใช้ในการพิสูจน์และยืนยันตัวตนผ่านระบบอิเล็กทรอนิกส์ คือ ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล หรือระบบ Digital ID

ระบบ Digital ID[11] คือ โครงสร้างพื้นฐานของประเทศไทย ที่เชื่อมต่อการพิสูจน์และยืนยันตัวตนจากทุกภาคส่วนเพื่อเพิ่มความสะดวก รวดเร็วในการใช้บริการของประชาชน และลดการปลอมแปลงตัวตน ช่วยให้การพิสูจน์และยืนยันตัวตนน่าเชื่อถือยิ่งขึ้น ซึ่งรัฐบาลโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและกระทรวงการคลังเป็นหน่วยงานรับผิดชอบในการพัฒนาระบบดังกล่าว

ระบบนี้จะรองรับการยืนยันตัวตนของบุคคลธรรมดาและนิติบุคคลในรูปแบบอิเล็กทรอนิกส์ในการรับบริการต่าง ๆ ของรัฐและเอกชน โดยอ้างอิงข้อมูลจากแหล่งข้อมูลที่น่าเชื่อถือ เพื่อให้แน่ใจว่าข้อมูลที่บุคคลนั้นแสดงถูกต้องเชื่อถือได้ และบุคคลที่ต้องการใช้บริการเป็นบุคคลที่อ้างถึงจริง ถือเป็นโครงสร้างพื้นฐานสำคัญที่จะช่วยอำนวยความสะดวกให้การทำธุรกิจในยุคดิจิทัล มีความรวดเร็ว มั่นคงปลอดภัย และน่าเชื่อถือในระดับสากล เนื่องจากมีการกำหนดมาตรฐานในการพิสูจน์และยืนยันตัวตน โดยอ้างอิงมาตรฐานสากล คือ Digital Identity Guidelines ของ National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา ระบบนี้จะช่วยให้การทำ e-KYC ของผู้ประกอบธุรกิจง่ายยิ่งขึ้นโดยผู้ประกอบธุรกิจสามารถพัฒนาระบบของตนเองแล้วเชื่อมโยงข้อมูลกับระบบนี้เพื่อใช้บริการได้ โดยมีค่าใช้จ่ายตามที่กำหนด ผู้ประกอบธุรกิจสามารถศึกษาข้อมูลเกี่ยวกับระบบ Digital ID เพิ่มเติมได้ที่เว็บไซต์ http://www.digitalid.or.th/

[11] http://www.digitalid.or.th/

กระบวนการลงทะเบียน การพิสูจน์และยืนยันตัวตนลูกค้าด้วยระบบ Digital ID[12]



ด้านซ้ายของรูป : แสดงกระบวนการลงทะเบียนและพิสูจน์ตัวตน ซึ่งมีขั้นตอนทั่วไป ดังนี้

(1) ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของ IdP ซึ่ง IdP จะพิสูจน์ตัวตนของผู้สมัครใช้บริการตามระดับความน่าเชื่อถือของไอเดนทิตี[13] ที่กำหนด โดยอาจตรวจสอบข้อมูลกับผู้ให้ข้อมูลที่น่าเชื่อถือ (Authoritative Source : AS)

(2) หากการพิสูจน์ตัวตนสำเร็จ IdP จะสร้างหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตน และสร้างสิ่งที่ใช้รับรองตัวตนซึ่งเป็นข้อมูลเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ

(3) ผู้สมัครใช้บริการเปลี่ยนสถานะเป็น “ผู้ใช้บริการ” โดย IdP จะเก็บรักษาสิ่งที่ใช้รับรองตัวตน สถานะของสิ่งที่ใช้รับรองตัวตน และข้อมูลที่ผู้ใช้บริการใช้ลงทะเบียนตลอดอายุการใช้งานของสิ่งที่ใช้รับรองตัวตน (เป็นอย่างน้อย) ส่วนผู้ใช้บริการเก็บรักษาสิ่งที่ใช้ยืนยันตัวตน

ด้านขวาของรูป : แสดงกระบวนการยืนยันตัวตนที่เกิดขึ้นเมื่อผู้ใช้บริการต้องการเข้าใช้บริการ หรือทำธุรกรรมกับ RP ซึ่งมีขั้นตอนทั่วไปดังนี้

(1) ผู้ใช้บริการขอเข้าใช้บริการหรือทำธุรกรรมออนไลน์กับ RP โดยใช้ดิจิทัลไอดีที่มีระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนตรงตามความต้องการของ RP

---

[12] ที่มา : ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - ภาพรวมและอภิธานศัพท์ DIGITAL IDENTITY GUIDELINE FOR THAILAND – OVERVIEW AND GLOSSARY เวอร์ชัน 1.0 https://standard.etda.or.th/rec (ขมธอ. 18-2561)

[13] ไอเดนทิตี (identity หรือ ID) หมายถึง คุณลักษณะ (attribute) หรือชุดของคุณลักษณะที่ใช้ระบุตัวบุคคลในบริบทที่กำหนด

(2) ผู้ใช้บริการยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยพิสูจน์ให้ IdP เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีที่ IdP กำหนด

(3) IdP ตรวจสอบความถูกต้องและสถานะของสิ่งที่ใช้ยืนยันตัวตนและสิ่งที่ใช้รับรองตัวตน แล้วส่งผลการยืนยันตัวตนให้กับ RP ซึ่ง RP สามารถใช้ข้อมูลที่อยู่ในผลการยืนยันตัวตนนี้พิจารณาสิทธิต่าง ๆ ของผู้ใช้บริการ

(4) RP ทำการเชื่อมต่อกับผู้ใช้บริการ

<u>ตัวอย่างกระบวนการลงทะเบียนและการพิสูจน์และยืนยันตัวตนลูกค้าด้วยระบบ Digital ID</u>

ขั้นตอนแรก ลูกค้าไปเปิดบัญชีกับธนาคารพาณิชย์ (ธพ.) ซึ่ง ธพ. จะมีวิธีการในการรับลงทะเบียนและพิสูจน์ตัวตนที่มีความน่าเชื่อถือในระดับที่ ธพ. กำหนดก่อนเปิดบัญชีธนาคารให้ลูกค้าใช้เป็นหลักฐานสำหรับทำธุรกรรมและออก username/password ให้ลูกค้าเพื่อใช้ยืนยันตนเองเมื่อต้องการทำธุรกรรมกับ ธพ. แบบ online ด้วย

หลังจากนั้นหากลูกค้าต้องการเปิดบัญชีกับ บล. (โดยที่ ธพ. ที่ลูกค้าเคยเปิดบัญชีธนาคารดังกล่าวไว้ได้ให้บริการเป็นผู้พิสูจน์และยืนยันตัวตนในระบบ Digital ID หรือ IdP) กรณีนี้ บล. สามารถให้ลูกค้ายืนยันตัวตนกับ ธพ. ที่ตนเองเคยลงทะเบียนและพิสูจน์ตัวตนมาแล้วผ่านระบบ digital ID ในขั้นตอนนี้ ธพ. จะทำหน้าที่เป็น IdP ส่วน บล. คือ RP ที่ขอใช้บริการ โดยให้ IdP พิสูจน์ตัวตนลูกค้าให้ โดย ธพ. จะให้ลูกค้าเข้าระบบ online ของ ธพ. ด้วย username/password ที่ ธพ. เคยให้ไว้เพื่อยืนยันว่า ลูกค้ารายนี้ คือคนเดียวกับที่เคยมาลงทะเบียนและพิสูจน์ตัวตนกับ ธพ. มาแล้ว หากกระบวนการทั้งหมดสำเร็จ ธพ. จะแจ้ง บล. ว่าลูกค้ารายนี้เป็นบุคคลที่กล่าวอ้างจริง เมื่อ บล. ได้รับการยืนยันจาก ธพ. แล้ว บล. จึงดำเนินการทำ KYC ในขั้นตอนต่อไปตามปกติ โดย บล. อาจขอข้อมูลเพิ่มเติมจาก AS ประกอบการทำ KYC ได้โดยได้รับความยินยอมจากลูกค้าก่อนขอข้อมูล

กฎเกณฑ์/มาตรฐานการพิสูจน์และยืนยันตัวตนของต่างประเทศ

เพื่อให้ผู้ประกอบธุรกิจพัฒนาการเปิดบัญชี online และการทำ e-KYC ได้อย่างมีประสิทธิภาพ องค์กรกำกับดูแลทั้ง **International Organization of Securities Commission Organization** หรือ **IOSCO** ซึ่งเป็นเสมือน ก.ล.ต. โลก และ **Banking for International Settlements (BIS)** หรือ**ธนาคารเพื่อการชำระหนี้ระหว่างประเทศ** ได้กำหนดเป็นหลักการว่า การเปิดบัญชีผ่านระบบอิเล็กทรอนิกส์นั้น ผู้ประกอบธุรกิจต้องมีกระบวนการที่เทียบเท่าหรือมากกว่าวิธีการแบบเดิม

ในการนี้ ยังมีหน่วยงานในต่างประเทศอีกหลายหน่วยงานกำหนดมาตรฐานในการพิสูจน์และยืนยันตัวตน เช่น International Organization for Standardization ได้จัดทำ ISO/IEC 29115:2013 Information technology -Security techniques - Entity authentication assurance framework

ซึ่งมีความน่าเชื่อถือ เป็นที่ยอมรับในระดับสากล นอกจากนั้น ยังมีอีกหลายประเทศที่กำหนดแนวทางปฏิบัติในเรื่องการพิสูจน์ตัวตน เช่น รัฐบาลออสเตรเลีย ได้ออก Trusted Digital Identity Framework – Identity Proofing Requirements หรือ Swiss Financial Market Supervisory Authority (FINMA) ของประเทศสวิตเซอร์แลนด์ได้ออก Circular 2016/7 Video and online identification- Due diligence requirement for client onboarding via digital channels เป็นต้น

สำหรับประเทศไทย สพธอ. ได้นำหลักการของ National Institute of Standards and Technology (NIST) ซึ่งเป็นหน่วยงานของประเทศสหรัฐอเมริกามาใช้เป็นแนวทางในการกำหนดข้อเสนอแนะมาตรฐานของไทย ในที่นี้จึงขอเล่ามาตรฐานของ NIST โดยสรุป ดังนี้

National Institute of Standards and Technology (NIST)

NIST หรือสถาบันมาตรฐานเทคโนโลยีสารสนเทศแห่งชาติของสหรัฐอเมริกา จัดทำ Digital Identity Guidelines[14] ที่กำหนด

(1) ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level : IAL)

(2) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level : AAL)

(3) การยืนยันตัวตนลูกค้าแทนกันในกลุ่ม (Federation Assertion)

โดยแต่ละเรื่องจะกำหนดระดับความน่าเชื่อถือใน 3 ระดับ คือ ระดับ 1 คือน่าเชื่อถือต่ำที่สุด ระดับ 2 คือ น่าเชื่อถือสูง และระดับ 3 คือน่าเชื่อถือสูงมาก ซึ่งแนวทางปฏิบัติฯ นี้จะอ้างอิงเฉพาะเรื่อง IAL ในข้อ (1) และ AAL ในข้อ (2)

(1) ระดับความน่าเชื่อถือของไอเดนทิตี (IAL) คือ การพิสูจน์ตัวตนลูกค้าว่า ลูกค้าเป็นบุคคลที่กล่าวอ้าง และเป็นเจ้าของหลักฐานที่นำมาแสดง ซึ่งระดับความน่าเชื่อถือจะเกิดจาก (ก) วิธีการตรวจสอบข้อมูล (ข) คุณภาพของหลักฐาน (ค) จำนวนหลักฐานที่ลูกค้านำมาแสดง และ (ง) การพบเห็นลูกค้าต่อหน้าเพื่อดูพฤติกรรม โดยสรุปดังนี้

[14] https://pages.nist.gov/800-63-3/

IAL	ข้อกำหนด
IAL 1	ไม่มีการตรวจสอบหลักฐาน เชื่อในสิ่งที่บุคคลนั้นกล่าวอ้าง เช่น การสร้างบัญชีบน Facebook หรือ Google ที่ให้ผู้สมัครแจ้งข้อมูลของตน
IAL 2	มีการตรวจสอบข้อมูลและขอหลักฐานกับแหล่งข้อมูลที่น่าเชื่อถือเพิ่มเติมเพื่อยืนยันสิ่งที่ลูกค้าอ้าง เช่น การเปิดบัญชีซื้อขายหลักทรัพย์ที่ต้องขอดูบัตรประชาชน เพื่ออ้างอิงตัวตนลูกค้า
IAL 3	ระดับที่มีความน่าเชื่อถือมากที่สุด จะเพิ่มความเข้มงวดให้กับข้อกำหนดที่ระดับ 2 ด้วยการพิจารณาหลักฐานแสดงตนที่น่าเชื่อถืออย่างน้อย 2 ชิ้น และการเก็บข้อมูลชีวมิติ (biometric) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่น การหลอกลวง การลงทะเบียนซ้ำ ทั้งนี้ การพิสูจน์ตัวตนที่ IAL ระดับ 3 สามารถทำได้เฉพาะแบบพบเห็นลูกค้าต่อหน้า หรือหากทำผ่านช่องทางอิเล็กทรอนิกส์ จะต้องมีความน่าเชื่อถือและความมั่นคงปลอดภัยเทียบเท่ากับแบบพบเห็นลูกค้าต่อหน้า โดยคุณลักษณะที่ใช้ลงทะเบียนต้องผ่านการตรวจสอบจากผู้ให้บริการพิสูจน์และยืนยันตัวตน (IdP)

การเลือกใช้ความน่าเชื่อถือในการพิสูจน์ตัวตนในระดับใดนั้น ขึ้นอยู่กับการพิจารณาความเสี่ยงในด้านต่าง ๆ จากการทำธุรกรรมนั้น (ดูตัวอย่างกระบวนการพิจารณาความเสี่ยงเพื่อการเลือกระดับความน่าเชื่อถือที่เหมาะสมได้จาก ภาคผนวก 1)

(2) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) คือ การยืนยันตัวตนเมื่อลูกค้าต้องการเข้าระบบเพื่อทำธุรกรรมต่าง ๆ จะต้องมีการยืนยันตัวตนด้วยวิธีการที่น่าเชื่อถือก่อน จึงจะสามารถเข้าระบบได้ โดยความน่าเชื่อถือจะเกิดจากจำนวนและคุณภาพของปัจจัยที่นำมาใช้ยืนยันตัวตน ซึ่งประกอบด้วยปัจจัย 3 ประเภท คือ 1. something you have เช่น OTP หรือมือถือที่ได้ลงทะเบียนไว้ 2. something you know เช่น username/password หรือ pin code และ 3. something you are คือข้อมูลชีวมิติ (biometric) เช่น ใบหน้า ลายนิ้วมือ ม่านตา เสียง

หลักการในการใช้ปัจจัยยืนยันตัวตน คือ เลือกใช้ปัจจัยยืนยันตัวตนให้เหมาะสมกับความเสี่ยงของธุรกรรมนั้น ๆ ยิ่งใช้ปัจจัยหลายอย่าง หลายประเภท คุณภาพสูง ถูก hack ถูกขโมยได้ยาก ก็ยิ่งน่าเชื่อถือ

ตัวอย่างเช่น ในการยืนยันตัวตนเพื่อเข้า application ของธนาคารบนสมาร์ตโฟนของตนเองเพื่อดูข้อมูลทั่วไป อาจใช้เพียงปัจจัยการยืนยันตัวตนเพียงปัจจัยเดียว (AAL 1) นั่นคือเป็นสมาร์ตโฟนเครื่องที่ได้ลงทะเบียน ไว้กับธนาคารแล้ว โดยไม่ต้องใช้ username/password แต่หากต้องการทำรายการโอนเงิน จะใช้การยืนยันตัวตนด้วย 2 ปัจจัยที่ต่างกัน (AAL 2) คือต้องเป็นสมาร์ตโฟนเครื่องที่ได้ลงทะเบียนไว้กับธนาคารแล้ว ประกอบกับ username/password ส่วน AAL 3 คือ ใช้วิธีการยืนยันตัวตนแบบใช้ 2 ปัจจัยที่ต่างกัน และ

มีปัจจัยหนึ่งเป็นกุญแจเข้ารหัส (cryptographic key) เช่น USB Token ซึ่งบรรจุ Private key ที่สามารถใช้งานได้เมื่อใส่รหัสผ่านถูกต้อง เช่น การใช้ username/password ประกอบกับตัวเลข 6 หลักที่ได้จากอุปกรณ์แบบ hardware เพื่อเข้าระบบในการทำงานที่มี security สูง

(ดูรายละเอียดกฎเกณฑ์และมาตรฐานต่างประเทศเพิ่มเติมได้จาก ภาคผนวก 2)

กล่าวโดยสรุป คือ กฎเกณฑ์และมาตรฐานในต่างประเทศให้ความสำคัญกับการปรับเปลี่ยนวิธีการให้บริการจาก offline เป็นแบบ online ว่าจะต้องมีคุณภาพที่เทียบเท่ากัน มีรูปแบบ วิธีการที่น่าเชื่อถือ ปลอดภัยตามความเหมาะสม โดยแนะนำให้เริ่มจากการประเมินความเสี่ยงหากเกิดความผิดพลาดในการให้บริการแบบ online ว่าจะเกิดผลกระทบอย่างไรได้บ้าง รุนแรงเพียงใด แล้วจึงเลือกวิธีการ เทคนิคที่สามารถบรรเทาหรือ จัดการความเสี่ยงในแต่ละเรื่องมาใช้กับบริการของตนเองเพื่อให้เกิดความน่าเชื่อถือในการยืนยันตัวตนในระดับที่เหมาะสม

มาตรฐานการพิสูจน์และยืนยันตัวตนของไทย

สพธอ. ได้จัดทำข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย (ภาพรวมและอภิธานศัพท์ การลงทะเบียนและพิสูจน์ตัวตน และการยืนยันตัวตน[15] (“ข้อเสนอแนะมาตรฐานฯ”) ขึ้น เพื่อเป็นแนวทางให้หน่วยงานต่าง ๆ ที่ต้องการพัฒนาระบบพิสูจน์และยืนยันตัวตนแบบ online ใช้อ้างอิงได้ รวมถึงเป็นมาตรฐานสำหรับการพิสูจน์และยืนยันตัวตนผ่านระบบ Digital ID โดยข้อเสนอแนะนี้ใช้หลักการที่สอดคล้องกับมาตรฐานของ NIST ในเรื่อง IAL และ AAL และมีการปรับเปลี่ยนให้เข้ากับบริบทของประเทศไทย โดยสรุป IAL และ AAL ของไทยได้ ดังนี้ **(โปรดอ่านข้อเสนอแนะมาตรฐานฯ ฉบับเต็มของ สพธอ. ประกอบการนำไปปรับใช้ในการกำหนดวิธีการทำ e-KYC)**

[15] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ DIGITAL IDENTITY GUIDELINE FOR THAILAND – OVERVIEW AND GLOSSARY เวอร์ชัน 1.0 https://standard.etda.or.th/rec (ขมธอ. 18-2561)
ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน DIGITAL IDENTITY GUIDELINE FOR THAILAND –ENROLMENT AND IDENTITY PROOFING เวอร์ชัน 1.0 https://standard.etda.or.th/rec (ขมธอ. 19-2561)
ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน DIGITAL IDENTITY GUIDELINE FOR THAILAND –Authentication เวอร์ชัน 1.0 https://standard.etda.or.th/rec (ขมธอ. 20-2561)

IAL แบ่งเป็น 3 ระดับ ได้แก่

IAL	ข้อกำหนด
ระดับ 1	
1.1	ไม่มีการตรวจสอบข้อมูล/หลักฐานของลูกค้า ให้ลูกค้ายืนยันข้อมูลของตนเอง
1.2	ขอสำเนาหลักฐานแสดงตนจากลูกค้า แต่ไม่มีการตรวจสอบกับแหล่งที่มาของข้อมูลหลักฐาน หรือผู้ให้ข้อมูลที่น่าเชื่อถือ
1.3	ผู้ประกอบธุรกิจได้จับต้องหลักฐานแสดงตนตัวจริงของลูกค้า แต่ไม่มีการตรวจสอบกับแหล่งที่มาของข้อมูลหลักฐาน หรือผู้ให้ข้อมูลที่น่าเชื่อถือ กรณีไม่ได้พบเห็นลูกค้าต่อหน้า ให้ลูกค้าถ่ายรูปหลักฐานแสดงตนผ่าน application
ระดับ 2	
2.1	ตรวจสอบหลักฐานแสดงตน 1 ชิ้น เช่น ใช้ smart card reader อ่านข้อมูลในชิพในบัตรประชาชน และใช้เจ้าหน้าที่เปรียบเทียบรูปถ่ายจากหลักฐานแสดงตนกับใบหน้าลูกค้า กรณีไม่ได้พบเห็นลูกค้าต่อหน้า เช่น การเปิดบัญชีผ่าน Kiosk หรือเครื่องมือของลูกค้า เช่น สมาร์ตโฟน ต้องถ่ายภาพ* ใบหน้าลูกค้าเพื่อให้เจ้าหน้าที่ใช้เปรียบเทียบกับรูปถ่ายที่ได้จากการตรวจสอบหลักฐานแสดงตน และจัดเก็บเพื่อป้องกันการปฏิเสธธุรกรรมหรือการพิสูจน์ตัวตนในครั้งต่อไป *การเปิดบัญชี online ผ่าน application ลูกค้าต้องถ่ายรูปตนเองผ่าน application ของผู้ประกอบธุรกิจเท่านั้น ไม่สามารถใช้รูปที่ถ่ายเก็บไว้ในอุปกรณ์ลูกค้าได้
2.2	**วิธีการตามที่กำหนดใน 2.1 และดำเนินการเพิ่มเติมในเรื่องต่อไปนี้** (1) ตรวจสอบหลักฐานแสดงตนกับแหล่งที่มาของข้อมูลหลักฐานหรือผู้ให้ข้อมูลที่น่าเชื่อถือแบบ online (2) ถ่ายภาพใบหน้าลูกค้าและจัดเก็บเพื่อป้องกันการปฏิเสธธุรกรรมหรือการพิสูจน์ตัวตนในครั้งต่อไป
2.3	**วิธีการตามที่กำหนดใน 2.2 และดำเนินการเพิ่มเติมในการใช้**เทคโนโลยี Biometric เพื่อเปรียบเทียบกับภาพใบหน้าลูกค้าหรือลายนิ้วมือกับหลักฐานแสดงตน เช่น Facial recognition
ระดับ 3	
	วิธีการตามที่กำหนดใน 2.3 และดำเนินการเพิ่มเติมดังนี้ - ตรวจสอบหลักฐานแสดงตน 2 ชิ้น คือ บัตรประชาชน และ passport - ต้องมีการแสดงตนแบบพบเห็นลูกค้าต่อหน้า หรือหากทำผ่านช่องทางอิเล็กทรอนิกส์ต้องมีความน่าเชื่อถือและความมั่นคงปลอดภัยเสมือนพบเห็นต่อหน้า - จัดเก็บข้อมูล biometric ของผู้สมัครใช้บริการเพื่อป้องกันการปฏิเสธธุรกรรมหรือการพิสูจน์ตัวตนในครั้งต่อไป - ตรวจสอบช่องทางติดต่อของลูกค้าว่าสามารถติดต่อได้จริง

AAL แบ่งเป็น 3 ระดับ ได้แก่

AAL	ข้อกำหนด
ระดับ 1	
	- ใช้ปัจจัยยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย (Single-factor authentication) - มีการป้องกันการโจมตีช่องทางรับส่งข้อมูลระหว่างลูกค้ากับผู้ประกอบธุรกิจ (man-in-the-middle) จากผู้ไม่ประสงค์ดีได้
ระดับ 2	
2.1	- ใช้ปัจจัยยืนยันตัวตนแบบ Multi-factor authentication (หลายปัจจัย) โดยเป็นปัจจัยคนละประเภท - มีการป้องกันการโจมตีช่องทางรับส่งข้อมูลระหว่างลูกค้ากับผู้ประกอบธุรกิจ (man-in-the-middle) จากผู้ไม่ประสงค์ดีได้ และการโจมตีแบบส่งข้อมูลยืนยันตัวตนซ้ำ (replay attack)
2.2	- ใช้ Biometric ร่วมกับปัจจัยยืนยันตัวตนแบบ Multi-factor authentication - มีการป้องกันการโจมตีช่องทางรับส่งข้อมูลระหว่างลูกค้ากับผู้ประกอบธุรกิจ (man-in-the-middle) จากผู้ไม่ประสงค์ดีได้ และการโจมตีแบบส่งข้อมูลยืนยันตัวตนซ้ำ (replay attack)
ระดับ 3	
	- ใช้ปัจจัยยืนยันตัวตนแบบ Multi-factor authentication โดยปัจจัยหนึ่งเป็นอุปกรณ์ (device) และต้องใช้เกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) ด้วย - มีการป้องกันการโจมตีช่องทางรับส่งข้อมูลระหว่างลูกค้ากับผู้ประกอบธุรกิจจากผู้ไม่ประสงค์ดี (man-in-the-middle) การโจมตีแบบส่งข้อมูลยืนยันตัวตนซ้ำ (replay attack) และการปลอมตัวเป็น IdP ที่ออกสิ่งที่ใช้ยืนยันตัวตนได้ (IdP impersonation attack)

ภาคผนวก 2: ตัวอย่างกระบวนการพิจารณาความเสี่ยงเพื่อการเลือกระดับความน่าเชื่อถือที่เหมาะสม

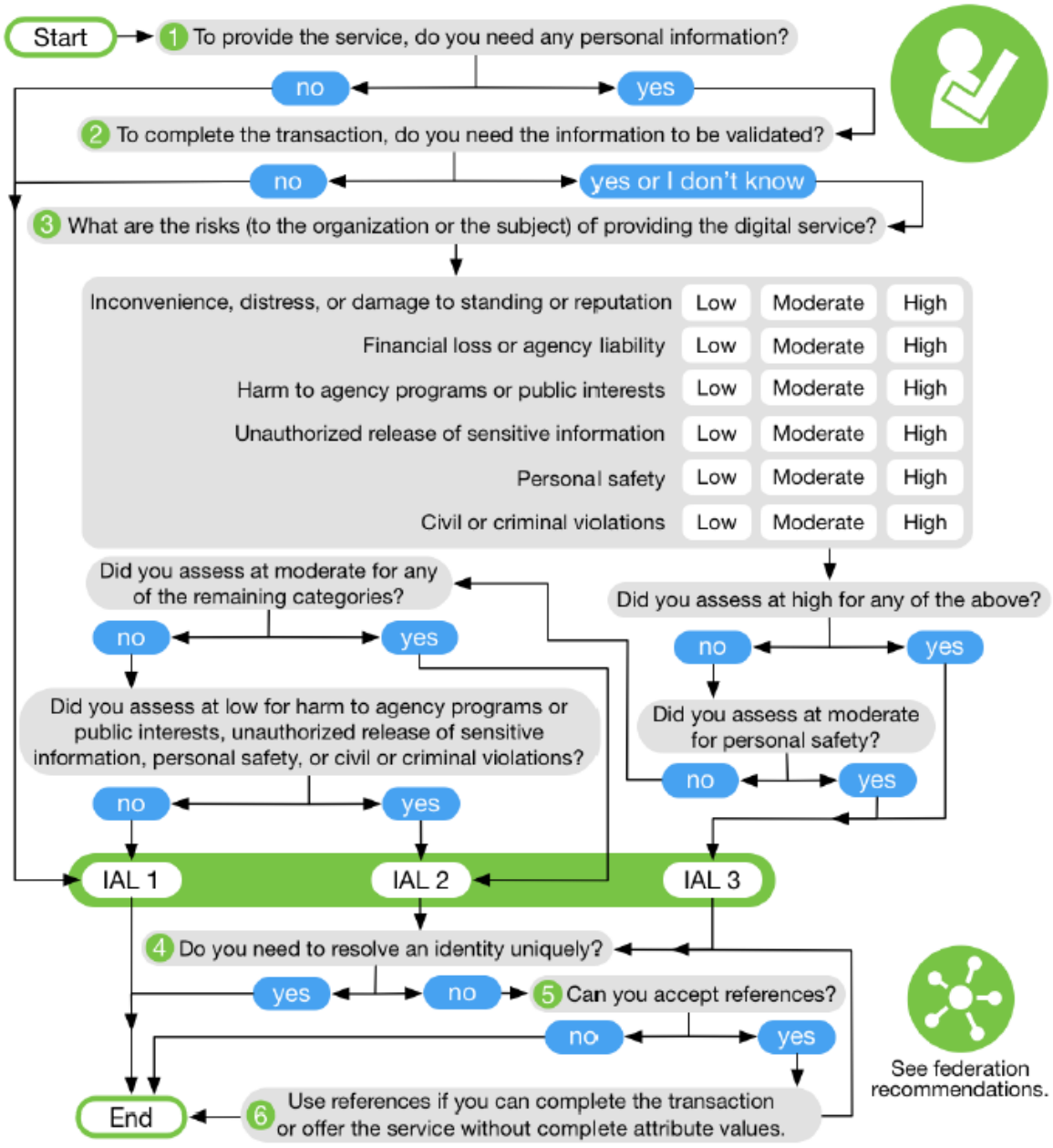


Figure 6-1 Selecting IAL

ภาคผนวก 3: รายละเอียดกฎเกณฑ์และมาตรฐานต่างประเทศ

1) กฎเกณฑ์ต่างประเทศ

- **International Organization of Securities Commission Organization** หรือ **IOSCO** เป็นเสมือน ก.ล.ต. โลก และ **Banking for International Settlements (BIS) หรือ ธนาคารเพื่อการชำระหนี้ระหว่างประเทศ**ได้พูดเกี่ยวกับการเปิดบัญชีผ่านระบบอิเล็กทรอนิกส์ว่าผู้ประกอบธุรกิจต้องมีกระบวนการที่เทียบเท่าหรือมากกว่าวิธีการแบบเดิม และพูดถึงการทำ Digital onboarding และความเสี่ยงจากการใช้ online platform[16] ไว้ว่า การให้บริการแบบ online นั้น ผู้ประกอบธุรกิจจะต้องกำหนดนโยบาย และกระบวนการบริหารความเสี่ยงที่เทียบเท่าหรือมากกว่าวิธีการแบบเดิม เพราะการเปิดบัญชี online นั้น มีความเสี่ยงที่ลูกค้าจะกรอกข้อมูลเท็จเพื่อปิดบังตัวตน สร้าง profile ที่ดูดีเพื่อให้เปิดบัญชีได้ หรือไม่ก็ตั้งใจจะกระทำผิดอยู่แล้วจึงเลือกเปิดบัญชีด้วยวิธีนี้ แทนที่จะต้องเจอหน้าบริษัท เพราะบริษัทจะขอดูหลักฐานที่มีรูปถ่าย ออกโดยหน่วยงานรัฐ ดังนั้น บริษัทจึงควรมีกระบวนการป้องกันการให้ข้อมูลเท็จหรือขโมยข้อมูลมาเปิดบัญชี

  นอกจากนั้น บริษัทยังมีความเสี่ยงที่จะไม่รู้จักลูกค้าอย่างแท้จริง ให้บริการไม่เหมาะสม เพราะไม่ได้พบหน้าพูดคุยกับลูกค้า ลูกค้าจึงลงทุนไม่เหมาะสมกับตนเอง เนื่องจากตามปกติแล้วในการให้คำแนะนำการลงทุนแก่ลูกค้า บริษัทต้องสร้าง profile ลูกค้าขึ้นมาก่อนด้วยการถามคำถามต่าง ๆ เพื่อให้เข้าใจสถานการณ์ของลูกค้า แต่การเปิดบัญชีแบบ online นั้น จะใช้คำถามมาตรฐานกับลูกค้าทุกคนทำแบบอัตโนมัติ บริษัทจึงมีความเสี่ยงที่จะไม่รู้สถานการณ์ของลูกค้าได้ถ่องแท้นั่นเอง

- **Banking for International Settlements (BIS)** หรือ ธนาคารเพื่อการชำระหนี้ระหว่างประเทศได้พูดใน General guidelines to account opening[17] ว่าหากกฎหมายอนุญาตให้เปิดบัญชีแบบไม่พบเห็นลูกค้าต่อหน้าได้ กระบวนการ Identify และ Verify ควรมีประสิทธิภาพเทียบเท่าการเปิดบัญชีแบบพบเห็นลูกค้าต่อหน้า โดยธนาคารต้องรู้ว่าลูกค้ามีตัวตนและรู้ว่าบุคคลที่มาทำธุรกรรมกับธนาคารคือลูกค้า

[16] IOSCO Research Report on Financial Technologies (Fintech) (Feb 2017)

[17] Guidelines - Sound management of risks related to money laundering and financing of terrorism (Feb 2016)

2) มาตรฐาน NIST

- **National Institute of Standards and Technology (NIST)** หรือ สถาบันมาตรฐานเทคโนโลยีสารสนเทศแห่งชาติของสหรัฐ ที่เป็นหน่วยงานที่พัฒนามาตรฐานด้านเทคโนโลยีต่าง ๆ ซึ่งได้ออก Digital Identity Guidelines เพื่อให้หน่วยงานรัฐใช้ในการบริหารความเสี่ยง และการพัฒนาระบบ digital service ทั้งการทำ identity proofing และการ authenticate บุคคลที่จะเข้าใช้ระบบของหน่วยงาน กระบวนการของ NIST จะเริ่มจากการประเมินความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นหากเกิดความผิดพลาดในการยืนยันตัวตน เช่น ความเสียหายด้านชื่อเสียง ความเสียหายทางการเงิน ไปจนถึงความสูญเสียหรืออันตรายต่อชีวิต แล้วจึงประเมินว่าจะเลือกใช้วิธีการที่มีระดับความน่าเชื่อถือ (Identity Assurance Level) ในระดับใด

ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL)

Identity Assurance Level
IAL1: At IAL1, attributes, if any, are self-asserted or should be treated as self-asserted.
IAL2: At IAL2, either remote or in-person identity proofing is required. IAL2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in SP 800-63A.
IAL3: At IAL3, in-person identity proofing is required. Identifying attributes must be verified by an authorized CSP representative through examination of physical documentation as described in SP 800-63A.

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: AAL)

Authenticator Assurance Level
AAL1: AAL1 provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol.
AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.
AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a "hard" cryptographic authenticator that provides verifier impersonation resistance.

ภาคผนวก 4: ตัวอย่างมาตรฐานขั้นต่ำด้านเทคนิคในเรื่องคุณภาพของภาพหลักฐาน ภาพถ่ายลูกค้าและการทำ VDO conference

ข้อกำหนดด้านเทคนิค

1. มาตรฐานขั้นต่ำสำหรับความละเอียด (Resolution) ของภาพหลักฐานที่ลูกค้าส่งให้ผู้ประกอบธุรกิจผ่านระบบอิเล็กทรอนิกส์[18]

- ภาพลายเส้น หรือภาพขาวดำ อย่างน้อย 150 จุดต่อนิ้ว (dot per inch หรือ dpi)
- ภาพสี อย่างน้อย 300 จุดต่อนิ้ว

2. มาตรฐานขั้นต่ำของภาพถ่ายและวิดีโอสำหรับบันทึกการทำธุรกรรม[19]

มาตรฐานขั้นต่ำของภาพถ่าย

1) ความละเอียดของภาพไม่น้อยกว่า 1280 x 720 pixels หรือ 1080 x 1080 pixels
2) การบีบอัดข้อมูลภาพถ่ายควรใช้การบีบอัดข้อมูลแบบไม่สูญเสีย (lossless data compression) หรือในกรณีที่ใช้การบีบอัดข้อมูลแบบสูญเสียบางส่วน (lossy data compression) ต้องตรวจสอบให้มั่นใจได้ว่าคุณภาพของภาพอยู่ในระดับที่เพียงพอต่อการใช้งาน
3) ภาพของลูกค้าควรมีคุณลักษณะ ดังนี้
    - ภาพเป็นชนิดภาพสี
    - ลูกค้าต้องแสดงใบหน้าทั้งหมด ในลักษณะปกติ (ไม่ยิ้ม และปากปิด) ใบหน้าตรง และมองตรงมายังกล้อง
    - ภาพต้องคมชัด และอยู่ในโฟกัส
    - ภาพต้องแสดงส่วนของศีรษะทั้งหมดของลูกค้าโดยปราศจากสิ่งปกคลุม ยกเว้นกรณีสวมเครื่องแต่งกายของศาสนาหรือวัสดุทางการแพทย์ ทั้งนี้ ภาพต้องแสดงใบหน้าทั้งหมดของลูกค้าอย่างชัดเจน
    - ภาพต้องแสดงดวงตาของลูกค้าอย่างชัดเจน และไม่มีสีแดง (red-eye)

---

[18] อ้างอิงจากข้อกำหนดแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553 ฉบับที่ 1 ว่าด้วยข้อกำหนดวิธีปฏิบัติในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

[19] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร (ขมธอ. 17-2561) โดย สพธอ.

- ลูกค้าสามารถใส่แว่นสายตาขณะถ่ายภาพ หากภาพที่ถ่ายออกมาแสดงให้เห็นดวงตาอย่างชัดเจน โดยไม่มีเงาหรือแสงสะท้อนจากแว่น
- ลูกค้าไม่สามารถใส่แว่นตากันแดด หรือแว่นเคลือบสีขณะถ่ายภาพ
- ความยาวของใบหน้า (จากศีรษะถึงคาง) ประมาณร้อยละ 60-80 ของความสูงของภาพ

<u>มาตรฐานขั้นต่ำของวิดีโอ</u>

1) ความละเอียดของภาพไม่น้อยกว่า 1280 x 720 pixels
2) มี frame rate ไม่น้อยกว่า 10 ภาพต่อวินาที
3) ระบบบันทึกภาพมีการเทียบเวลาอัตโนมัติกับระบบเทียบเวลามาตรฐาน (NTP Server)
4) จุดติดตั้งกล้องต้องอยู่ในตำแหน่งที่สามารถมองเห็นภาพใบหน้าของลูกค้าอย่างชัดเจน
5) การบีบอัดข้อมูลวิดีโอควรใช้การบีบอัดข้อมูลแบบไม่สูญเสีย (lossless data compression) หรือในกรณีที่ใช้การบีบอัดข้อมูลแบบสูญเสียบางส่วน (lossy compression) ต้องตรวจสอบให้มั่นใจ ได้ว่าคุณภาพของวิดีโออยู่ในระดับที่เพียงพอต่อการใช้งาน