(ร่าง)

แนวปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

---------- 2561

บทนำ

การปรับตัวเข้าสู่ยุคดิจิทัลเป็นสิ่งที่เห็นได้ทั่วไปในช่วง 2-3 ปีที่ผ่านมา โดยเฉพาะอย่างยิ่งธุรกิจบริการที่ต่างแข่งขันกันนำเสนอบริการที่สะดวก รวดเร็วและตอบโจทย์ lifestyle ของลูกค้าให้ได้มากที่สุด สำนักงานตระหนักถึงความเปลี่ยนแปลงในเรื่องดังกล่าวและเห็นสัญญาณของการปรับตัวเข้าสู่ยุคดิจิทัลของผู้ประกอบธุรกิจในตลาดทุนโดยเฉพาะอย่างยิ่งการปรับเปลี่ยนวิธีการเปิดบัญชีและทำความรู้จักลูกค้า (Know Your Client: KYC) ด้วยวิธีอิเล็กทรอนิกส์ (e-KYC) อย่างไรก็ดี ผู้ประกอบธุรกิจหลายรายอาจมีความกังวลเนื่องจากไม่แน่ใจว่าจะสามารถปรับเปลี่ยนการทำ KYC ในรูปแบบอิเล็กทรอนิกส์ได้มากน้อยเพียงใด หรือวิธีการแบบใดจึงจะถูกต้องตามกฎเกณฑ์ของสำนักงาน ที่เป็นเช่นนี้เนื่องจากกฎเกณฑ์ของสำนักงานเกี่ยวกับการทำ KYC กำหนดไว้ในลักษณะหลักการ (principle-based) โดยผู้ประกอบธุรกิจซึ่งมีรูปแบบธุรกิจ ขนาด กลุ่มลูกค้า และจำนวนลูกค้าแตกต่างกัน สามารถพัฒนาวิธีที่เหมาะสมกับตนเองที่สุด ทั้งนี้ เพื่อให้เกิดความยืดหยุ่นในทางปฏิบัติสำหรับผู้ประกอบธุรกิจ

นอกจากนี้ ในปี 2561 นี้ ได้มีการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ขึ้น ซึ่งจะเป็นระบบที่ช่วยให้ขั้นตอนพิสูจน์ตัวตน (identity proofing) ไปจนถึงการทำ KYC ในขั้นตอนอื่น ๆ ง่ายขึ้น ซึ่งการใช้บริการระบบดังกล่าวต้องมีการกำหนดระดับความน่าเชื่อถือในการพิสูจน์และยืนยันตัวตน ผู้ประกอบธุรกิจจึงเกิดคำถามว่าต้องเลือกระดับความน่าเชื่อถือระดับใดที่สำนักงานเห็นว่าเหมาะสม เพียงพอ โดยสำนักงานได้รับคำถามในเรื่องเหล่านี้มาอย่างต่อเนื่อง

สำนักงานสนับสนุนให้เกิดการนำเทคโนโลยีเข้ามาปรับใช้ในการประกอบธุรกิจซึ่งรวมไปถึงการปรับเปลี่ยนวิธีการทำ KYC ไปในรูปแบบอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการพัฒนาวิธีการของตนเอง หรือใช้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) เนื่องจากนอกจากจะช่วยลดค่าใช้จ่ายในการทำ KYC ได้แล้ว ยังดำเนินการได้รวดเร็ว มีประสิทธิภาพ และน่าเชื่อถือ โดยวิธีการดังกล่าวยังคงต้องบรรลุหลักการที่สำนักงานกำหนด โดยมีการบริหารความเสี่ยงที่จะแตกต่างไปจากเดิมได้อย่างเหมาะสม

เพื่อลดความกังวลและสร้างความเชื่อมั่นให้กับผู้ประกอบธุรกิจในการปรับเปลี่ยนวิธีดำเนินการ สำนักงานจึงจัดทำแนวปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า (แนวปฏิบัติฯ) นี้ขึ้น เพื่อให้ผู้ประกอบธุรกิจที่ต้องการปรับเปลี่ยนวิธีการใช้เป็นแนวทางในการพัฒนารูปแบบการเปิดบัญชีและทำ e-KYC โดยมีเนื้อหาครอบคลุมถึงการทำ KYC แบบพบหน้าลูกค้า (face-to-face) แต่มีการใช้เครื่องมือหรือเทคโนโลยีเข้ามาเสริมให้การดำเนินการมีประสิทธิภาพมากขึ้น ทั้งในด้านความสะดวก รวดเร็ว น่าเชื่อถือ และการทำ KYC แบบ online ที่ไม่ได้พบหน้าลูกค้า (non face-to-face) แต่ใช้เทคโนโลยีเข้ามาช่วยให้การดำเนินการได้คุณภาพเทียบเท่าแบบพบหน้า การทำ

e-KYC จึงไม่ได้จำกัดเฉพาะเพียงการทำในรูปแบบที่ไม่ได้พบหน้า โดยหลักการที่นำเสนอในแนวปฏิบัติฯ ฉบับนี้บางส่วนอ้างอิงจากข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ข้อเสนอแนะมาตรฐานฯ) ที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) จัดทำขึ้น ซึ่งผู้ประกอบธุรกิจควรศึกษาข้อเสนอแนะมาตรฐานฯ ดังกล่าวเพิ่มเติมเพื่อให้เข้าใจถึงที่มาที่ไปของตัวอย่าง วิธีการ เทคนิคต่าง ๆ ในแต่ละเรื่องให้ชัดเจนยิ่งขึ้นก่อนการนำไปใช้เพื่อกำหนดวิธีการทำ e-KYC ของตนเอง และการกำหนดตัวอย่างวิธีการในแนวปฏิบัตินี้ สำนักงานได้ร่วมหารือกับหน่วยงานที่เกี่ยวข้อง* จัดการประชุมผู้ประกอบธุรกิจแบบ focus group รวมถึงเปิดรับฟังความคิดเห็นผ่านเว็บไซต์ของสำนักงานแล้ว

หากผู้ประกอบธุรกิจเลือกใช้วิธีการตามตัวอย่างในแนวปฏิบัติฯ นี้ ก็ถือว่าเป็นการทำ e-KYC ที่เพียงพอกับหลักการของสำนักงาน อย่างไรก็ดี วิธีการที่แสดงในแนวปฏิบัติฯ ฉบับนี้เป็นเพียงตัวอย่างวิธีการขั้นต่ำ เนื่องจากไม่มีรูปแบบ วิธีการทำ e-KYC ใดที่สามารถจัดการความเสี่ยงที่อาจจะเกิดขึ้นได้หมด สำหรับทุก business model ทุกกลุ่มลูกค้า หรือทุกสถานการณ์ ผู้ประกอบธุรกิจสามารถปรับเปลี่ยนวิธีการได้ตามที่เห็นว่าเหมาะสมกับ business model ของตนเอง หรือสอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงไปได้หากสามารถพิสูจน์ได้ว่าช่วยให้บรรลุหลักการของสำนักงานได้เช่นกัน ประกอบกับเทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็วจนทำให้ตัวอย่างวิธีการในแนวปฏิบัติ ฯ ฉบับนี้อาจล้าสมัย สำนักงานจึงอาจปรับปรุงแนวปฏิบัติฯ นี้ให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงดังกล่าวต่อไปในอนาคต

สำนักงานหวังว่าแนวปฏิบัติฯ ฉบับนี้จะช่วยให้ผู้ประกอบธุรกิจสามารถออกแบบวิธีการที่เหมาะสมได้อย่างมั่นใจ ช่วยให้ลูกค้าเข้าถึงการลงทุนได้ง่ายและช่วยยกระดับมาตรฐานการให้บริการในตลาดทุนไทยให้เกิดความสะดวกรวดเร็วควบคู่ไปกับความปลอดภัยและน่าเชื่อถือ

ฝ่ายนโยบายธุรกิจตัวกลาง
สำนักงาน ก.ล.ต.

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

สารบัญ

หน้า

1. ความหมายของ KYC และ ECOSYSTEM

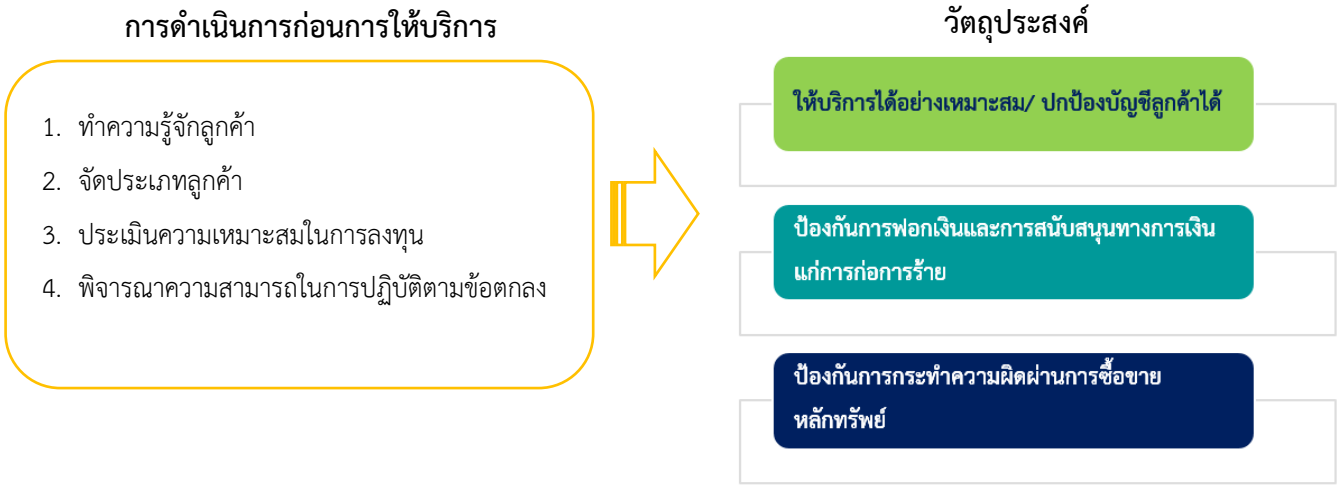
<u>การทำความรู้จักลูกค้า (Know Your Client : KYC)</u> คือ การรวบรวมและประเมินข้อมูลต่าง ๆ ของลูกค้าก่อนที่ผู้ประกอบธุรกิจจะให้บริการธุรกิจหลักทรัพย์ โดยจะต้องรวบรวมข้อมูลส่วนบุคคลเพื่อให้รู้ว่าลูกค้าเป็นใคร

นอกจากนี้ ในการทำ KYC ยังหมายความรวมถึงการทำความรู้จักลูกค้าเพื่อให้บริการเหมาะสม (Client Due Diligence : CDD) ด้วยการรวบรวมข้อมูลต่าง ๆ ของลูกค้า ได้แก่ รายได้และแหล่งที่มาของรายได้ ฐานะการเงิน ความรู้ความเข้าใจและประสบการณ์ลงทุน วัตถุประสงค์ในการลงทุน ไปจนถึงความเสี่ยงที่ยอมรับได้ เพื่อสามารถให้บริการในธุรกิจหลักทรัพย์และสัญญาซื้อขายล่วงหน้าได้ตามขอบเขตใบอนุญาตที่ผู้ประกอบธุรกิจได้รับ เช่น การประเมินความเหมาะสมใน การลงทุนการให้คำแนะนำ การให้วงเงินการให้บริการซื้อขายหลักทรัพย์ได้อย่างเหมาะสมกับลูกค้านั้น ๆ ซึ่งมักจะเรียกรวมกันว่าการทำ KYC/CDD

<u>KYC framework ของสำนักงาน</u>

สำนักงานกำหนดให้ในการให้บริการแก่ลูกค้า ผู้ประกอบธุรกิจจะต้องทำ KYC ก่อนที่จะให้บริการอย่างน้อยเพื่อวัตถุประสงค์หลัก 2 ประการ คือ การทำความรู้จักตัวตนที่แท้จริงของลูกค้า และการประเมินความเหมาะสมในการลงทุนในผลิตภัณฑ์ตลาดทุนเพื่อที่จะให้บริการที่เหมาะสมกับความเสี่ยงที่ลูกค้าจะยอมรับได้

โดยกฎเกณฑ์เกี่ยวกับการทำ KYC ของสำนักงาน ได้กำหนดไว้เป็นหลักการซึ่งสรุปได้ ดังนี้



วิวัฒนาการของ KYC

เดิมการทำ KYC ผู้ประกอบธุรกิจส่วนใหญ่จะใช้วิธีการรวบรวมข้อมูลจากลูกค้า ผ่านใบคำขอเปิดบัญชี และขอหลักฐานเป็นสำเนาบัตรประชาชน สำเนาหน้าสมุดบัญชีธนาคาร และ statement ทางการเงินย้อนหลัง นอกจากนี้ ยังให้ลูกค้าทำ suitability test โดยทุกขั้นตอนทำเป็นกระดาษ (paper work) หลังจากนั้น ผู้ประกอบธุรกิจก็จะนำเอกสารที่ได้รับมาตรวจสอบความมีตัวตนลูกค้า เช่น ดูว่าข้อมูลในใบคำขอฯ ตรงกับสำเนาบัตรประชาชน มีการโทรศัพท์ยืนยันการเปิดบัญชีกับลูกค้าหรือบุคคลอ้างอิงตามข้อมูลที่ได้รับ มีการประเมินความเหมาะสมในการลงทุน แล้วจึงจัดกลุ่มความเสี่ยง กำหนดวงเงิน และอนุมัติเปิดบัญชี รวมถึงจัดเก็บเอกสารเปิดบัญชีดังกล่าวไว้เพื่อการตรวจสอบตามความจำเป็นในภายหลัง

การพิสูจน์และยืนยันตัวตนที่ผู้ประกอบธุรกิจปฏิบัติเปรียบเทียบกับเกณฑ์ KYC

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

แต่ปัจจุบัน แม้เทคโนโลยีจะพัฒนาการอย่างก้าวกระโดด ลูกค้าปรับเปลี่ยนวิถีชีวิตเข้าสู่รูปแบบ online lifestyle กันมากขึ้น และผู้ประกอบธุรกิจก็ให้ความสนใจปรับเปลี่ยนการให้บริการต่าง ๆ เข้าสู่รูปแบบ online อย่างไรก็ดี การทำ KYC ด้วยวิธีการอิเล็กทรอนิกส์ (e-KYC) ในตลาดทุน ในช่วงเริ่มต้น มักจะเป็นการทำในขั้นตอนที่ไม่ซับซ้อน เช่น เพื่อจัดเก็บข้อมูลทางอิเล็กทรอนิกส์ หรือลดการใช้กระดาษ (paperless) แต่ก็ยังไม่สามารถอำนวยความสะดวกให้แก่ลูกค้าได้มากนัก เนื่องจากกฎหมายที่รองรับผลทางกฎหมายของการทำธุรกรรมอิเล็กทรอนิกส์ยังมีกรณีตัวอย่างเกิดขึ้นน้อย และมีความเสี่ยงในการนำเรื่องเข้าสู่การพิจารณาของศาล นอกจากนี้ หากเป็นการทำธุรกรรมผ่านช่องทาง online โดยไม่ได้พบหน้าลูกค้า กฎเกณฑ์จะให้ความสำคัญกับการทำ KYC เพื่อให้รู้จักตัวตน

ลูกค้าที่มาใช้บริการและระบบงานที่เกี่ยวข้อง เพื่อสามารถให้บริการได้อย่างเหมาะสม ป้องกันการกระทำความผิดและปกป้องคุ้มครองทรัพย์สินของลูกค้าเนื่องจากหากเกิดความผิดพลาด เช่น การใช้ตัวตนปลอมหรือใช้ข้อมูลบุคคลอื่นในการเปิดบัญชี การซื้อขายแทนกัน หรือการถูกลักลอบใช้บัญชีซื้อขาย การถูกยักยอกเงินโดยเจ้าของบัญชีไม่รู้ตัวได้

อย่างไรก็ดี ด้วยสภาพแวดล้อมที่ยังคงเดินหน้าเข้าสู่ยุคดิจิทัล ลูกค้าให้ความสำคัญกับบริการที่สะดวก รวดเร็วมากขึ้นเรื่อย ๆ ในระยะ 2 ปีที่ผ่านมา การเปิดบัญชีซื้อขายหลักทรัพย์ online และการทำ e-KYC จึงถูกหยิบยกขึ้นมาหารือกันระหว่างสำนักงานและผู้ประกอบธุรกิจอย่างต่อเนื่อง โดยผู้ประกอบธุรกิจหลายรายมีแนวคิดที่ต้องการพัฒนาระบบเปิดบัญชี online และทำ e-KYC ทั้งกระบวนการแบบ paperless หรือใช้เทคโนโลยีมาช่วยในการพิสูจน์ตัวตน เพื่อแข่งขันกันตอบสนองต่อ lifestyle ของลูกค้าที่เปลี่ยนแปลงไป ซึ่งจะช่วยให้การเปิดบัญชีให้ลูกค้าสะดวก รวดเร็ว และน่าเชื่อถือ

เมื่อจะต้องปรับเปลี่ยนวิธีการทำ KYC รูปแบบเดิม เป็น e-KYC เพื่อให้บริการธุรกรรมทางการเงินการลงทุนนั้น หัวใจสำคัญที่ผู้ประกอบธุรกิจต้องมั่นใจได้ คือ จะต้องมีวิธีการที่สามารถระบุตัวตน (identify) ของบุคคลในโลก digital ได้ว่าเป็นบุคคลใดในโลก physical

การพิสูจน์ตัวตนบุคคลด้วยวิธีการอิเล็กทรอนิกส์ที่ใช้กันทั่วไป เริ่มจากผู้ให้บริการต้องตรวจสอบตัวตนทางกายภาพ (physical) ของลูกค้าก่อน (เช่น การตรวจสอบบัตรประชาชนกับบุคคลจริง) เมื่อได้ข้อมูลตัวตนของลูกค้ามาแล้ว จึงสร้างตัวตนในโลก digital ที่สามารถอ้างอิงกันและกันได้ และออกสิ่งที่ใช้ยืนยันตัวตน (credential เช่น username/password) ให้ตัวตนในโลก digital นำกลับมาใช้ยืนยันว่าตนเองเป็นบุคคลคนเดียวกันกับตัวตนในโลก physical ที่ผู้ประกอบธุรกิจได้เคยตรวจสอบตัวตนไว้

ตัวอย่างกระบวนการพิสูจน์ตัวตนแบบง่าย เช่น เมื่อลูกค้าต้องการเปิดบัญชีกับ บล. จึงส่งใบคำขอเปิดบัญชีที่กรอกข้อมูลต่าง ๆ และแนบหลักฐานคือสำเนาบัตรประชาชนให้ บล. ต่อมา บล. ตรวจสอบตัวตนลูกค้าว่าเป็นใคร โดยอ้างอิงจากในใบคำขอฯ กับข้อมูลจากบัตรประชาชน (อาจใช้วิธีการตรวจสอบเพิ่มเติมไปยังฐานข้อมูลกรมการปกครอง เพื่อให้มั่นใจมากขึ้นว่าบัตรยังสามารถใช้ได้ และไม่ถูกปลอมแปลง) เมื่อ บล. ตรวจสอบตัวตนจนมั่นใจแล้วว่าผู้มาสมัครใช้บริการกับข้อมูลที่มีในหลักฐานเป็นคนเดียวกัน จึงจะออก username/password ให้ลูกค้าใช้ในการทำธุรกรรมในโลก digital ซึ่งทำให้ บล. สามารถอ้างอิงไปยังตัวตนของลูกค้าคนนั้นได้ เมื่อลูกค้าเข้าทำธุรกรรม online ด้วย username/password ดังกล่าว บล. จึงรู้ว่าผู้ที่ใช้ username/password นี้ในโลก digital เป็นใครในโลก physical นั่นเอง

กระบวนการที่กล่าวข้างต้น ไม่ว่าจะเป็นการทำในรูปแบบเดิมคือทำบนกระดาษ หรือทำแบบ online ทั้งกระบวนการก็ต้องมีประสิทธิภาพ น่าเชื่อถือ เพื่อให้มั่นใจว่าไม่มีการปลอมแปลงตัวตนเป็นบุคคลอื่น ซึ่งก็ตามมาด้วยความยุ่งยาก เสียเวลาและค่าใช้จ่ายสูง

อย่างไรก็ดี ปัจจุบันมีแนวคิดที่ช่วยสร้างเครื่องมือที่ช่วยตอบโจทย์การสร้างตัวตนและการยืนยันตัวตนบนโลก digital ให้ง่ายขึ้นในหลายประเทศ เช่น อินเดีย สิงคโปร์ และอังกฤษ สรุปได้ดังนี้

อินเดีย: Aadhaar

ปัญหาการระบุตัวตนของประชากรอินเดีย เกิดขึ้นจากความแตกต่างด้านการเมืองและเศรษฐกิจที่ซับซ้อนของประชากรอินเดียที่มีจำนวนมากกว่าพันล้านคน เงินอุดหนุนจากรัฐสำหรับคนยากจนไม่สามารถไปถึงมือผู้ที่ควรได้รับจริง ๆ อีกทั้งการเข้าถึงบริการที่สำคัญ ๆ อย่างเช่น สถาบันการเงิน ก็เป็นไปได้ยากด้วย รัฐบาลอินเดียเล็งเห็นถึงปัญหานี้จึงจัดตั้งหน่วยงาน Unique Identification Authority of India (UIDAI)[1] 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 แต่เปลี่ยนเป็นการระบุตัวตนผ่านวิธีการทางอิเล็กทรอนิกส์แทน ซึ่งใช้เวลาไม่นาน Aadhaar สามารถใช้ประโยชน์ในการเข้าถึงบริการจากสถาบันการเงิน เช่น การเปิดบัญชีธนาคาร และการใช้ micro ATMs รวมไปถึงการขอรับสวัสดิการจากรัฐที่เมื่อระบุตัวตนประชาชนที่เข้าข่ายสมควรได้รับความช่วยเหลือได้ สวัสดิการก็ไปถึงมือได้ นอกจากนั้น Aadhaar ยังสามารถใช้ในการทำใบขับขี่ หรือลงทะเบียนโทรศัพท์มือถือ ช่วยให้ประชาชนสามารถเข้าถึงระบบสาธารณูปโภคได้ง่ายขึ้นอีกด้วย

สิงคโปร์: MyInfo

รัฐบาลสิงคโปร์เองก็มีแนวคิดในการผลักดันการพิสูจน์และยืนยันตัวตนให้เข้าสู่รูปแบบดิจิทัลเพื่อเพิ่มความสะดวกและลดความซ้ำซ้อนในการใช้บริการ โดยได้มีการพัฒนาระบบ MyInfo[2] ซึ่งเป็นระบบที่สามารถแชร์ข้อมูลประชาชนระหว่างหน่วยงานรัฐและเอกชน เช่น ธนาคาร ช่วยให้ประชาชนที่ต้องการใช้บริการต่าง ๆ ไม่ต้อง

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

[2] www.myinfo.gov.sg.

กรอกข้อมูลซ้ำ ๆ ช่วยลดความผิดพลาดในการกรอกข้อมูลลงในแบบฟอร์มด้วยตนเอง และไม่ต้องยื่นหลักฐานจริง แต่ใช้การแชร์ข้อมูลจากฐานข้อมูลกลางแทน โดยข้อมูลสำคัญ ๆ เช่น รายได้จะต้องมีการให้ความยินยอมก่อนการแชร์ข้อมูล

ข้อมูลในฐานข้อมูลของระบบ MyInfo ได้แก่ ข้อมูลส่วนบุคคลต่าง ๆ เช่น ชื่อ-นามสกุล เลขที่บัตรประจำตัวประชาชน วันเกิด ข้อมูลช่องทางติดต่อ เช่น เบอร์โทรศัพท์มือถือ อีเมล์ ที่อยู่ ข้อมูลรายได้ ข้อมูลการศึกษาและการทำงาน ข้อมูลครอบครัว ไปจนถึงการครอบครองยานพาหนะ

ปัจจุบันมีหน่วยงานภาครัฐถึง 38 หน่วยงานเชื่อมต่อระบบกับ MyInfo เช่น การสมัคร public housing flats หรือ Baby Bonus scheme นอกเหนือจากบริการภาครัฐ ยังมีธนาคารหลายแห่งที่ให้ลูกค้าใช้ข้อมูลจาก MyInfo เพื่อการเปิดบัญชีธนาคารได้โดยไม่ต้องกรอกแบบฟอร์มหรือแสดงหลักฐานอีก ช่วยให้การเปิดบัญชีธนาคารทำได้รวดเร็วยิ่งขึ้นด้วย

อังกฤษ: GOV.UK Verify

ประเทศอังกฤษเป็นอีกประเทศหนึ่งที่รัฐบาลพัฒนาระบบการพิสูจน์ตัวตนที่ช่วยลดความซ้ำซ้อนและสร้างความรวดเร็วในการใช้บริการภาครัฐในรูปแบบ online ได้ โดยรัฐบาลโดยหน่วยงาน Government Digital Service (GDS) ได้จัดทำระบบที่มีชื่อว่า GOV.UK Verify ซึ่งเริ่มใช้งานในปี 2016

กระบวนการพิสูจน์ตัวตนของระบบดังกล่าวคือ เมื่อมีผู้ต้องการใช้บริการภาครัฐทาง online บุคคลผู้นั้นต้องไปพิสูจน์ตัวตนและสร้างตัวตนดิจิทัลกับผู้ให้บริการยืนยันตัวตน หรือ Identity Providers เสียก่อน โดยเลือก Identity

Provider ที่ต้องการจาก Identity Providers จำนวน 7 รายที่ได้รับความเห็นชอบจากรัฐให้ทำหน้าที่พิสูจน์ตัวตนแล้ว โดย Identity Provider จะขอข้อมูลจากผู้ที่ต้องการใช้บริการและทำการตรวจสอบข้อมูลนั้นกับแหล่งข้อมูลที่น่าเชื่อถือ ซึ่ง Identity Provider แต่ละรายจะมีวิธีการพิสูจน์ตัวตนที่แตกต่างกันไป อย่างไรก็ดี กระบวนการพิสูจน์ตัวตนนี้จะใช้เวลาเพียง 5-15 นาทีเท่านั้น หลังจากนั้นผู้ใช้บริการก็จะสามารถใช้ตัวตนดิจิทัลนั้นเข้าใช้บริการภาครัฐที่ต้องการในครั้งต่อ ๆ ไปโดยไม่ต้องพิสูจน์ตัวตนอีก

ปัจจุบันมีบริการภาครัฐ 18 บริการที่สามารถใช้การพิสูจน์ตัวตนผ่าน GOV.UK Verify ได้ เช่น การตรวจสอบภาษีเงินได้ ตรวจสอบสวัสดิการของรัฐ หรือการดูข้อมูลใบขับขี่ เป็นต้น ซึ่งมีผู้ผ่านการพิสูจน์ตัวตนด้วยระบบนี้แล้วจำนวนกว่า 2.8 ล้านคน

การพัฒนา GOV.UK Verify ช่วยลดภาระของทั้งผู้ขอใช้บริการและหน่วยงานภาครัฐที่เดิมต้องพิสูจน์ตัวตนซ้ำ ๆ ช่วยลดระยะเวลาการเข้าใช้บริการ ช่วยให้การพิสูจน์ตัวตนมีความปลอดภัย เนื่องจากไม่มีการรวมศูนย์ข้อมูลไว้ในที่เดียว ไม่มีการแชร์ข้อมูลโดยไม่จำเป็น และได้มาตรฐานเนื่องจาก Identity Providers ต้องมีขั้นตอนการพิสูจน์ตัวตนที่ได้มาตรฐานของรัฐและมาตรฐานสากลในเรื่องความมั่นคงปลอดภัยและการคุ้มครองข้อมูลของผู้ขอใช้บริการด้วย

ระบบ Digital ID ตัวช่วยยืนยันตัวตนของไทย

สำหรับประเทศไทยเองในปี 2561 นี้ รัฐบาลได้สนับสนุนให้เกิดการพัฒนาโครงสร้างพื้นฐานของประเทศที่ใช้ในการพิสูจน์และยืนยันตัวตนผ่านระบบอิเล็กทรอนิกส์ คือ ระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล หรือระบบ Digital ID

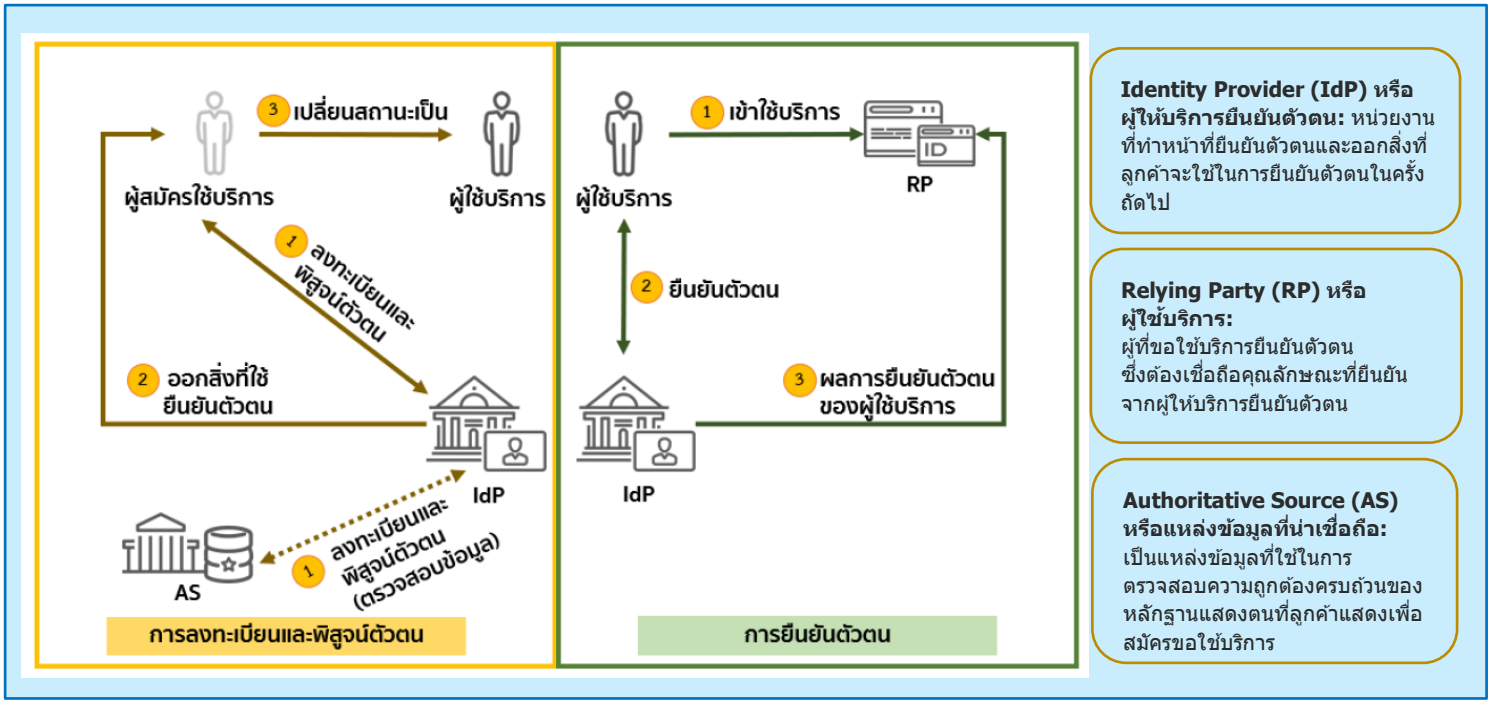
ระบบ Digital ID[3] คือโครงสร้างพื้นฐานของประเทศที่เชื่อมต่อการยืนยันตัวตนจากทุกภาคส่วนเพื่อเพิ่มความสะดวก รวดเร็วในการใช้บริการของประชาชน

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

และลดการปลอมแปลงตัวตน ช่วยให้การยืนยันตัวตนน่าเชื่อถือยิ่งขึ้น ซึ่งรัฐบาลโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและกระทรวงการคลังเป็นหน่วยงานรับผิดชอบในการพัฒนาระบบดังกล่าว

ระบบนี้จะรองรับการยืนยันตัวตนของบุคคลธรรมดาและนิติบุคคลในรูปแบบอิเล็กทรอนิกส์ในการรับบริการต่าง ๆ ของรัฐและเอกชน โดยอ้างอิงข้อมูลจากแหล่งข้อมูลที่น่าเชื่อถือ เช่น กรมการปกครอง เพื่อให้แน่ใจว่าข้อมูลที่บุคคลนั้นแสดง ถูกต้อง เชื่อถือได้ และบุคคลที่ต้องการใช้บริการเป็นบุคคลที่อ้างถึงจริง ถือเป็นโครงสร้างพื้นฐานสำคัญที่จะช่วยอำนวยความสะดวกให้การทำธุรกิจในยุคดิจิทัลและไทยแลนด์ 4.0 มีความรวดเร็ว มั่นคงปลอดภัย และมีความน่าเชื่อถือในระดับสากล เนื่องจาก สพธอ. กำหนดมาตรฐานในการยืนยันตัวตน โดยอ้างอิงมาตรฐานของต่างประเทศ คือ Digital Identity Guidelines ของ National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา ระบบนี้จะช่วยให้การทำ e-KYC ของผู้ประกอบธุรกิจจะง่ายยิ่งขึ้น โดยผู้ประกอบธุรกิจสามารถพัฒนาระบบของตนเองแล้วเชื่อมโยงข้อมูลกับระบบนี้เพื่อใช้บริการได้ โดยมีค่าใช้จ่ายตามที่กำหนด ผู้ประกอบธุรกิจสามารถศึกษาข้อมูลเกี่ยวกับระบบ Digital ID เพิ่มเติมได้ที่เว็บไซต์ http://www.digitalid.or.th/

กระบวนการลงทะเบียน การพิสูจน์และยืนยันตัวตนลูกค้าด้วยระบบ Digital ID[4]



[4] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - ภาพรวมและอภิธานศัพท์ DIGITAL IDENTITY GUIDELINE FOR THAILAND – OVERVIEW AND GLOSSARY เวอร์ชั่น 1.0 https://standard.etda.or.th/wp-content/uploads/2018/10/20171204-ER-DigitalID-Overview-V01-29F.pdf

ด้านซ้ายของรูป : แสดงกระบวนการลงทะเบียนและพิสูจน์ตัวตน ซึ่งมีขั้นตอนทั่วไป ดังนี้

(1) ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของ IdP ซึ่ง IdP จะพิสูจน์ตัวตนของผู้สมัครใช้บริการตามระดับความน่าเชื่อถือของไอเดนทิตี[5] ที่กำหนด โดยอาจตรวจสอบข้อมูลกับผู้ให้ข้อมูลที่น่าเชื่อถือ (authoritative source: AS)

(2) หากการพิสูจน์ตัวตนสำเร็จ IdP จะสร้างหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตน และสร้างสิ่งที่ใช้รับรองตัวตน ซึ่งเป็นข้อมูลเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ

(3) ผู้สมัครใช้บริการเปลี่ยนสถานะเป็น “ผู้ใช้บริการ” โดย IdP จะเก็บรักษาสิ่งที่ใช้รับรองตัวตน สถานะของสิ่งที่ใช้รับรองตัวตน และข้อมูลที่ผู้ใช้บริการใช้ลงทะเบียน ตลอดอายุการใช้งาน ของสิ่งที่ใช้รับรองตัวตน (เป็นอย่างน้อย) ส่วนผู้ใช้บริการเก็บรักษาสิ่งที่ใช้ยืนยันตัวตน

ด้านขวาของรูป : แสดงกระบวนการยืนยันตัวตนที่เกิดขึ้นเมื่อผู้ใช้บริการต้องการเข้าใช้บริการ หรือทำธุรกรรมกับ RP ซึ่งมีขั้นตอนทั่วไปดังนี้

(1) ผู้ใช้บริการขอเข้าใช้บริการหรือทำธุรกรรมออนไลน์กับ RP โดยใช้ดิจิทัลไอดีที่มีระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนตรงตามความต้องการของ RP

(2) ผู้ใช้บริการยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยพิสูจน์ให้ IdP เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีที่ IdP กำหนด

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

(4) RP ทำการเชื่อมต่อกับผู้ใช้บริการ

ขอยกตัวอย่างการกระบวนการลงทะเบียน การพิสูจน์และยืนยันตัวตนลูกค้าด้วยระบบ Digital ID ข้างต้น โดยขั้นตอนแรกลูกค้าไปเปิดบัญชีกับธนาคารพาณิชย์ (ธพ.) ซึ่ง ธพ. จะมีวิธีการในการรับลงทะเบียนและพิสูจน์ตัวตนที่มีความน่าเชื่อถือในระดับที่ ธพ. กำหนดก่อนออกบัญชีธนาคารให้ลูกค้าใช้เป็นหลักฐานสำหรับทำธุรกรรมและออก username/password ให้ลูกค้าเพื่อใช้ยืนยันตนเองเมื่อต้องการทำธุรกรรมกับ ธพ. แบบ online ด้วย

หลังจากนั้นลูกค้าต้องการเปิดบัญชีกับบริษัทหลักทรัพย์ (บล.) บล. จึงให้ลูกค้าพิสูจน์ตัวตนกับ ธพ. ที่ตนเองเคยลงทะเบียนและพิสูจน์ตัวตนมาแล้วผ่านระบบ digital ID ในขั้นตอนนี้ ธพ. จึงทำหน้าที่ IdP ส่วน บล. คือ RP ที่ขอใช้บริการ IdP ให้ช่วยพิสูจน์ตัวตนลูกค้าให้ โดย ธพ. จะให้ลูกค้าเข้าระบบ online ของ ธพ. ด้วย username/password ที่ ธพ. เคยให้ไว้เพื่อยืนยันว่าบุคคลนี้คือคนเดียวกับที่เคยมาลงทะเบียนและพิสูจน์ตัวตนกับ ธพ. มาแล้ว หากกระบวนการทั้งหมดสำเร็จ ธพ. จึงแจ้ง บล. ว่าลูกค้าคนนี้เป็นบุคคลที่กล่าวอ้างจริง เมื่อ บล.

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

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 ซึ่งมีความน่าเชื่อถือเป็นที่ยอมรับในระดับสากล นอกจากนั้น ยังมีอีกหลายประเทศที่กำหนดแนวปฏิบัติในเรื่องการพิสูจน์ตัวตน 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 ในที่นี้จึงขอเล่ามาตรฐานของสหรัฐอเมริกาโดยสรุป ดังนี้

<u>National Institute of Standards and Technology (NIST)</u>

NIST หรือสถาบันมาตรฐานเทคโนโลยีสารสนเทศแห่งชาติของสหรัฐอเมริกา จัดทำ Digital Identity Guidelines[6] ที่กำหนด

(1) ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level : IAL)

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

(2) ระดับความน่าเชื่อถือในการยืนยันตัวตนเมื่อเข้าใช้ระบบ (Authentication Assurance Level : AAL)

(3) การยืนยันตัวตนลูกค้าแทนกันในกลุ่ม (Federation Assertion)

โดยแต่ละเรื่องจะกำหนดระดับความน่าเชื่อถือใน 3 ระดับ คือ ระดับ 1 คือน่าเชื่อถือต่ำที่สุด ระดับ 2 คือ น่าเชื่อถือปานกลาง และระดับ 3 คือน่าเชื่อถือสูงที่สุด ซึ่งแนวปฏิบัติฯ นี้จะอ้างอิงเฉพาะเรื่อง IAL และ AAL

(1) ระดับความน่าเชื่อถือของไอเดนทิตี[7] (IAL) คือ การพิสูจน์ตัวตนลูกค้าว่าลูกค้าเป็นบุคคลที่กล่าวอ้างและเป็นเจ้าของหลักฐานที่นำมาแสดง ซึ่งระดับความน่าเชื่อถือจะเกิดจาก (1) วิธีการตรวจสอบข้อมูล (2) คุณภาพของหลักฐาน (3) จำนวนหลักฐานที่ลูกค้านำมาแสดง และ (4) การพบหน้าลูกค้าเพื่อดูพฤติกรรม โดยสรุปดังนี้

IAL	ข้อกำหนด
IAL 1	ไม่มีการตรวจสอบหลักฐาน เชื่อในสิ่งที่บุคคลนั้นกล่าวอ้าง เช่น การสร้างบัญชีบน Facebook หรือ Google ที่ให้ผู้สมัครแจ้งข้อมูลของตน
IAL 2	จะมีการตรวจสอบข้อมูลและขอหลักฐานกับแหล่งข้อมูลที่น่าเชื่อถือเพิ่มเติมเพื่อยืนยันสิ่งที่ลูกค้าอ้าง เช่น การเปิดบัญชีซื้อขายหลักทรัพย์ที่ต้องขอดูบัตรประชาชน เพื่ออ้างอิงตัวตนลูกค้า
IAL 3	คือระดับที่มีความน่าเชื่อถือมากที่สุด จะเพิ่มความเข้มงวดให้กับข้อกำหนดที่ระดับ 2 ด้วยการพิจารณาหลักฐานแสดงตนที่น่าเชื่อถืออย่างน้อย 2 ชิ้น และการเก็บข้อมูลชีวมาตร (biometric) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่น การหลอกลวง การลงทะเบียนซ้ำ ทั้งนี้ การพิสูจน์ตัวตนที่ IAL ระดับ 3 สามารถทำได้เฉพาะแบบพบหน้า หรือหากทำผ่านช่องทางอิเล็กทรอนิกส์ จะต้องมีความน่าเชื่อถือและความมั่นคงปลอดภัยเทียบเท่ากับแบบพบหน้า โดยคุณลักษณะที่ใช้ลงทะเบียนต้องผ่านการตรวจสอบจากผู้ให้บริการยืนยันตัวตน (IdP)

ผู้ประกอบธุรกิจจะเลือกใช้ความน่าเชื่อถือในการพิสูจน์ตัวตนในระดับใดนั้น ขึ้นอยู่กับการพิจารณาความเสี่ยงในด้านต่าง ๆ จากการทำธุรกรรม (ดูตัวอย่างกระบวนการพิจารณาความเสี่ยงเพื่อการเลือกระดับความน่าเชื่อถือที่เหมาะสมได้จาก Appendix 1)

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

(2) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL)

เมื่อลูกค้าต้องการเข้าใช้งานระบบ จะต้องมีการยืนยันตัวตนด้วยวิธีการที่น่าเชื่อถือก่อน จึงจะสามารถใช้ระบบได้ โดยความน่าเชื่อถือจะเกิดจากจำนวนและคุณภาพของปัจจัยที่นำมาใช้ยืนยันตัวตน ซึ่งประกอบด้วยปัจจัย 3 ประเภท คือ something you have เช่น OTP หรือมือถือที่ได้ลงทะเบียนไว้ something you know เช่น username/password หรือ pin code และ something you are คือข้อมูลชีวมาตร (biometric) เช่น ใบหน้า ลายนิ้วมือ ม่านตา เสียง

หลักการในการใช้ปัจจัยยืนยันตัวตนคือ เลือกใช้ปัจจัยยืนยันตัวตนให้เหมาะสมกับความเสี่ยงของธุรกรรมนั้น ๆ ยิ่งใช้ปัจจัยหลายอย่าง หลายประเภท เป็นปัจจัยที่มีคุณภาพสูง ถูก hack ถูกขโมยได้ยาก ก็ยิ่งน่าเชื่อถือ

ตัวอย่างเช่น ในการยืนยันตัวตนเพื่อเข้า application ของธนาคาร อาจใช้เพียงปัจจัยการยืนยันตัวตนเพียงปัจจัยเดียว (AAL 1) เช่น username/password เพื่อดูข้อมูลทั่วไป แต่หากต้องการทำรายการเบิก ถอนเงิน จะใช้การใช้การยืนยันตัวตนด้วย 2 ปัจจัยที่ต่างกัน (AAL 2) เช่น username/password เพื่อเข้าใช้บัญชีธนาคาร online และใช้ OTP ที่ได้รับจากธนาคารเพื่อจะทำธุรกรรม ส่วน AAL 3 คือใช้วิธีการยืนยันตัวตนแบบใช้ 2 ปัจจัยที่ต่างกัน และมีปัจจัยหนึ่งเป็นกุญแจเข้ารหัส (cryptographic key) เช่น USB Token ซึ่งบรรจุ Private key ที่สามารถใช้งานได้เมื่อใส่รหัสผ่านถูกต้อง เช่น การใช้ username/password ประกอบกับตัวเลข 6 หลักที่ได้จากอุปกรณ์แบบ hardware เพื่อเข้าระบบในการทำงานที่มี security สูง

(ดูรายละเอียดกฎเกณฑ์และมาตรฐานต่างประเทศเพิ่มเติมได้จาก Appendix 2)

กล่าวโดยสรุป คือ กฎเกณฑ์และมาตรฐานในต่างประเทศให้ความสำคัญกับการปรับเปลี่ยนวิธีการให้บริการจาก offline เป็นแบบ online ว่าจะต้องมีคุณภาพที่เทียบเท่ากัน มีรูปแบบ วิธีการที่น่าเชื่อถือ ปลอดภัยตามความเหมาะสม โดยแนะนำให้เริ่มจากการประเมินความเสี่ยงหากเกิดความผิดพลาดในการให้บริการแบบ online ว่าจะเกิดผลกระทบอย่างไรได้บ้าง รุนแรงเพียงใด แล้วจึงเลือกวิธีการ เทคนิคที่สามารถบรรเทาหรือกำจัดความเสี่ยงในแต่ละเรื่องมาใช้กับบริการของตนเอง เพื่อให้เกิดความน่าเชื่อถือในการยืนยันตัวตนในระดับที่เหมาะสม

มาตรฐานการพิสูจน์และยืนยันตัวตนของไทย

สพธอ. ได้มีการจัดทำข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสาหรับประเทศไทย (ภาพรวมและอภิธานศัพท์ การลงทะเบียน

และพิสูจน์ตัวตน และการยืนยันตัวตน[8] (“ข้อเสนอแนะมาตรฐานฯ”) ขึ้น เพื่อเป็นแนวทางให้หน่วยงานต่าง ๆ ที่ต้องการพัฒนาระบบพิสูจน์และยืนยันตัวตนแบบ online ใช้อ้างอิงได้ รวมถึงเป็นมาตรฐานสำหรับการพิสูจน์และยืนยันตัวตนผ่านระบบ Digital ID โดยข้อเสนอแนะนี้ใช้หลักการที่สอดคล้องกับมาตรฐานของ NIST ในเรื่อง IAL และ AAL และมีการปรับเปลี่ยนให้เข้ากับบริบทของประเทศไทย โดยสรุป IAL และ AAL ของไทยได้ดังนี้ **(โปรดอ่านข้อเสนอแนะมาตรฐานฯ ฉบับเต็มของ สพธอ. ประกอบการนำไปปรับใช้ในการกำหนดวิธีการทำ e-KYC)**

IAL แบ่งเป็น 3 ระดับ ได้แก่

IAL	ข้อกำหนด
ระดับ 1	
1.1	ไม่มีการตรวจสอบข้อมูล/หลักฐานของลูกค้า ให้ลูกค้ายืนยันตนเอง
1.2	ขอสำเนาหลักฐานจากลูกค้า แต่ไม่มีการตรวจสอบจากแหล่งที่มาข้อมูลหลักฐาน หรือ trusted source
1.3	ผู้ประกอบธุรกิจได้จับต้องหลักฐานตัวจริงของลูกค้า แต่ไม่มีการจากแหล่งที่มาข้อมูลหลักฐาน หรือ trusted source
ระดับ 2	
2.1	ตรวจสอบความแท้จริงของหลักฐาน เช่น ใช้ card reader อ่านบัตรประชาชน และใช้เจ้าหน้าที่เปรียบเทียบภาพในบัตรประชาชนกับตัวลูกค้า กรณีไม่ได้พบหน้าลูกค้า เช่น การเปิดบัญชีผ่าน Kiosk หรือเครื่องมือของลูกค้า เช่น smartphone ต้องถ่ายภาพใบหน้าลูกค้าเพื่อเปรียบเทียบกับแหล่งข้อมูลที่น่าเชื่อถือโดยเจ้าหน้าที่ และจัดเก็บเพื่อป้องกันการปฏิเสธธุรกรรมหรือการพิสูจน์ตัวตนในครั้งต่อไป
2.2	2.1 + (1) ตรวจสอบหลักฐานกับผู้ออกหรือแหล่งข้อมูลที่น่าเชื่อถือ (online)

[8] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ DIGITAL IDENTITY GUIDELINE FOR THAILAND – OVERVIEW AND GLOSSARY เวอร์ชั่น 1.0 https://standard.etda.or.th/wp-content/uploads/2018/10/20171204-ER-DigitalID-Overview-V01-29F.pdf
ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน DIGITAL IDENTITY GUIDELINE FOR THAILAND –ENROLMENT AND IDENTITY PROOFING เวอร์ชั่น 1.0 https://standard.etda.or.th/wp-content/uploads/2018/10/20171204-ER-DigitalID-EnrolmentIdentityProofing-V01-16F.pdf
ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน DIGITAL IDENTITY GUIDELINE FOR THAILAND –Authentication เวอร์ชั่น 1.0 https://standard.etda.or.th/wp-content/uploads/2018/10/20171204-ER-DigitalID-Authentication-V01-20F.pdf

IAL	ข้อกำหนด
	(2) ถ่ายภาพใบหน้าลูกค้าเพื่อเปรียบเทียบกับแหล่งข้อมูลที่น่าเชื่อถือโดยเจ้าหน้าที่และจัดเก็บเพื่อป้องกันการปฏิเสธธุรกรรมหรือการพิสูจน์ตัวตนในครั้งต่อไป
2.3	2.2 + เก็บภาพใบหน้าลูกค้าแบบ Biometric เพื่อเปรียบเทียบกับภาพจากแหล่งข้อมูลที่น่าเชื่อถือด้วยเทคโนโลยี เช่น Facial recognition และจัดเก็บเพื่อป้องกันการปฏิเสธธุรกรรมหรือการพิสูจน์ตัวตนในครั้งต่อไป (แทนการถ่ายภาพลูกค้าและให้เจ้าหน้าที่เปรียบเทียบตาม IAL 2.2)
ระดับ 3	
3	2.3 + หลักฐานยืนยันตัวตนที่น่าเชื่อถือ 2 ชิ้น เช่น บัตรประชาชน และ Passport

AAL แบ่งเป็น 3 ระดับ ได้แก่

AAL	ข้อกำหนด
ระดับ 1	
1	● ใช้ปัจจัยยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย (Single-factor authentication) ● มีการป้องกันการโจมตีช่องทางรับส่งข้อมูลระหว่างลูกค้ากับผู้ประกอบธุรกิจจากผู้ไม่ประสงค์ดีได้ (man-in-the-middle)
ระดับ 2	
2.1	● *ใช้ปัจจัยยืนยันตัวตนแบบ Multi-factor authentication (หลายปัจจัย)* ● มีการป้องกันการโจมตีช่องทางรับส่งข้อมูลระหว่างลูกค้ากับผู้ประกอบธุรกิจจากผู้ไม่ประสงค์ดีได้ (man-in-the-middle) และการโจมตีแบบส่งข้อมูลปัจจัยยืนยันตัวตนซ้ำ (reply attack)
2.2	● *ใช้ Biometric ร่วมกับปัจจัยยืนยันตัวตนแบบ Multi-factor authentication* ● มีการป้องกันการโจมตีช่องทางรับส่งข้อมูลระหว่างลูกค้ากับผู้ประกอบธุรกิจจากผู้ไม่ประสงค์ดีได้ (man-in-the-middle) และการโจมตีแบบส่งข้อมูลปัจจัยยืนยันตัวตนซ้ำ (reply attack)

AAL	ข้อกำหนด
ระดับ 3	
3	• *ใช้ปัจจัยยืนยันตัวตนแบบ Multi-factor authentication โดยปัจจัยหนึ่งต้องเป็นอุปกรณ์ (Device)* • มีการป้องกันการโจมตีช่องทางรับส่งข้อมูลระหว่างลูกค้ากับผู้ประกอบธุรกิจจากผู้ไม่ประสงค์ดีได้ (man-in-the-middle) การโจมตีแบบส่งข้อมูลปัจจัยยืนยันตัวตนซ้ำ (reply attack) และการปลอมตัวเป็น IdP ที่ออกสิ่งที่ใช้ยืนยันตัวตนได้ (IdP impersonation attack)

2. แนวปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้าในตลาดทุน

2.1 การพิสูจน์ตัวตน (IDENTITY PROOFING)

เพื่อเป็นการยกระดับการพิสูจน์ตัวตนลูกค้าให้มีคุณภาพทัดเทียมกันทั้งในภาคตลาดทุน ตลาดการเงิน และสอดคล้องกับมาตรฐานสากล สำนักงานจึงร่วมกับหน่วยงานต่าง ๆ ที่เกี่ยวข้อง เช่น สมาคมบริษัทหลักทรัพย์ไทย และสมาคมบริษัทจัดการลงทุน**กำหนดมาตรฐานขั้นต่ำในการพิสูจน์ตัวตน (Identity proofing) สำหรับขั้นตอนการเปิดบัญชี** โดยพิจารณาจาก**ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) ในข้อเสนอแนะมาตรฐานฯ** ที่ได้กล่าวถึงในบทที่แล้ว (หัวข้อมาตรฐานการพิสูจน์และยืนยันตัวตนของไทย) ซึ่ง IAL ที่กำหนดคือ **IAL ระดับ 2.1 ขึ้นไป และให้มีวิธีตรวจสอบหลักฐานทาง online**

หากผู้ประกอบธุรกิจต้องการจะใช้การพิสูจน์ตัวตนผ่านระบบ digital ID ก็สามารถใช้ IdP ที่มี IAL **ระดับ 2.1 บวก** โดย**<u>สิ่งที่ต้องทำเพิ่มเติมจากระดับ 2.1</u>** คือ ผู้ประกอบธุรกิจจะต้องดำเนินการตรวจสอบหลักฐานทาง online กับแหล่งข้อมูลที่น่าเชื่อถือด้วย หรือหากผู้ประกอบธุรกิจเลือกใช้ IdP ระดับ 2.2 ขึ้นไป ตามข้อเสนอแนะมาตรฐาน ฯ ผู้ประกอบธุรกิจไม่ต้องตรวจสอบหลักฐานทาง online เพิ่มเติม

การกำหนดมาตรฐานขั้นต่ำในการพิสูจน์ตัวตนข้างต้นนั้น เพื่อให้ขั้นตอนการรวบรวมและตรวจสอบข้อมูล หลักฐานลูกค้า (identification และ verification) มีคุณภาพเพียงพอที่จะให้มั่นใจว่า

1) ลูกค้ามีตัวตนจริง มีเพียงคนเดียว
2) หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง และ
3) ลูกค้าเป็นเจ้าของหลักฐานที่นำมาแสดง

การพิสูจน์ตัวตนลูกค้าด้วย IAL 2.1 ขึ้นไป และให้มีวิธีตรวจสอบหลักฐานทาง online นั้น แบ่งขั้นตอนการดำเนินการได้ 4 ขั้นตอน ดังนี้

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

ในการทำ e-KYC นั้น การรวบรวมข้อมูลและหลักฐานของลูกค้าอาจแตกต่างไปจากวิธีการเดิม คือ มีการใช้เทคโนโลยีเข้ามาช่วยในการรวบรวมและตรวจสอบข้อมูล เช่น การให้ลูกค้ากรอกข้อมูลพร้อมแนบไฟล์หลักฐานผ่านระบบอิเล็กทรอนิกส์ มีการใช้ลายมือชื่ออิเล็กทรอนิกส์แทนการลงนามด้วยปากกา โดยไม่ต้องส่งเป็นกระดาษเช่นเดิม (paperless) หรือการตรวจสอบหลักฐานด้วยอุปกรณ์อิเล็กทรอนิกส์ (การ dip chip) หรือตรวจสอบ online กับแหล่งข้อมูลที่น่าเชื่อถือหรือผู้ออกหลักฐาน

แม้จะมีการใช้วิธีการที่แตกต่างไปจากเดิม แต่เพื่อให้ผู้ประกอบธุรกิจยังคงมั่นใจว่ารู้จักตัวตนของลูกค้าได้ เช่นเดียวกับวิธีการเดิม ข้อมูล หลักฐานที่ผู้ประกอบธุรกิจจะรวบรวมจากลูกค้า ทั้งเอกสารที่แปลงเป็นไฟล์อิเล็กทรอนิกส์ ภาพถ่ายหลักฐาน หรือภาพถ่ายบุคคล จะต้องมีความละเอียด ความชัดเจนเพียงพอที่จะนำไปใช้งานต่อได้[9] นอกจากนี้ การตรวจสอบหลักฐานต่าง ๆ ยังต้องมีคุณภาพเทียบเท่าแบบเดิม (หรือมากกว่า ในกรณีที่ผู้ประกอบธุรกิจไม่ได้พบหน้า หรือพูดคุยกับลูกค้าในช่วงเวลาที่ให้บริการ)

การเชื่อมโยงข้อมูลกับหน่วยงานที่น่าเชื่อถือ

นอกจากการขอข้อมูล หลักฐานจากลูกค้าแล้ว หากเทคโนโลยีและกฎหมายเอื้ออำนวย ผู้ประกอบธุรกิจอาจใช้วิธีการเชื่อมโยงข้อมูลกับหน่วยงานต่าง ๆ ที่น่าเชื่อถือซึ่งมีข้อมูลของลูกค้าอยู่แล้ว เมื่อมีลูกค้ามาเปิดบัญชี สามารถใช้วิธีการดึงข้อมูลลูกค้าจากฐานข้อมูลเหล่านั้นมากรอกลงแบบคำขอเปิดบัญชีอัตโนมัติแทนการให้ลูกค้ากรอกข้อมูลเอง ทั้งนี้ จะต้องได้รับความยินยอมจากลูกค้าก่อน *หรือหากลูกค้าต้องการปรับปรุงข้อมูลที่ได้จากฐานข้อมูลที่น่าเชื่อถือ ก็จะต้องมีหลักฐานประกอบการเปลี่ยนแปลงข้อมูลนั้น* วิธีนี้นอกจากข้อมูลที่ได้รับจะมีความน่าเชื่อถือมากขึ้นแล้ว ยังเพิ่มความสะดวกให้ลูกค้าได้ แต่ผู้ประกอบธุรกิจต้องมั่นใจว่าแหล่งข้อมูลนั้นน่าเชื่อถือ มีข้อมูลที่ถูกต้องและเป็นปัจจุบัน

การพิสูจน์ตัวตนของลูกค้าด้วยหลักฐานที่หลากหลาย

การเพิ่มความหลากหลายของหลักฐาน จะช่วยให้ผู้ประกอบธุรกิจสามารถพิจารณาความสอดคล้องของข้อมูลลูกค้าจากหลักฐานเหล่านั้น (cross verification) เพื่อให้มั่นใจว่าลูกค้ามีตัวตนจริง ตัวอย่างหลักฐานที่ผู้ประกอบธุรกิจอาจกำหนดให้ลูกค้าส่งให้ เช่น

1) หลักฐานประเภท long-term คือ สิ่งที่อยู่กับลูกค้าเป็นระยะเวลายาวนาน เช่น บัตรประชาชน passport

2) หลักฐานประเภท routine คือ สิ่งที่ลูกค้าได้รับอย่างสม่ำเสมอ เช่น บิลค่าสาธารณูปโภค ใบแจ้งยอดบัตรเครดิต ช่วยให้เห็นความมีตัวตนจริงของลูกค้า

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

[9] รายละเอียดตาม Appendix 3 ตัวอย่างมาตรฐานขั้นต่ำทางเทคนิค เรื่อง มาตรฐานขั้นต่ำสำหรับความละเอียด (Resolution) ของภาพหลักฐานที่ลูกค้าส่งให้ผู้ประกอบธุรกิจผ่านระบบอิเล็กทรอนิกส์ และมาตรฐานขั้นต่ำของภาพถ่ายและวิดีโอสำหรับบันทึกการทำธุรกรรม

วิธีการแบบ paperless กับผลทางกฎหมาย

การปรับเปลี่ยนวิธีการรวบรวมข้อมูลและหลักฐานด้วยวิธีการแบบ paperless นี้ ผู้ประกอบธุรกิจอาจกังวลว่าจะผิดกฎหมาย/กฎเกณฑ์หรือไม่ ในเรื่องนี้มีตัวช่วยสนับสนุนเรื่องการมีผลทางกฎหมายของข้อมูลหลักฐาน และลายมือชื่ออิเล็กทรอนิกส์ ได้แก่ **พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544**[10] อย่างไรก็ดี ผู้ประกอบธุรกิจควรมั่นใจว่าได้กำหนดรูปแบบ วิธีการให้เป็นไปตามที่กฎหมายกำหนดในรายละเอียดด้วย เช่น การกำหนดวิธีการสร้างลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ เพื่อให้มั่นใจว่าข้อมูลและหลักฐานรวมถึงลายมือชื่อในรูปแบบอิเล็กทรอนิกส์นั้น นอกจากจะสร้างความสะดวก รวดเร็ว มีคุณภาพเทียบเท่าวิธีการแบบเดิมแล้ว ยังมีผลทางกฎหมายด้วย

2. <u>การตรวจสอบหลักฐาน (Verification)</u>

e-KYC แม้จะช่วยสร้างความสะดวก รวดเร็ว แต่ปฏิเสธไม่ได้ว่าอาจมีความเสี่ยงที่ลูกค้าจะให้ข้อมูลหรือหลักฐานเท็จได้ไม่ต่างจากการทำ KYC รูปแบบเดิม ผู้ประกอบธุรกิจจึงต้องกำหนดวิธีการตรวจสอบข้อมูลกับหลักฐานและตัวลูกค้าได้อย่างมีประสิทธิภาพ แนวปฏิบัติฯ ฉบับนี้ขอยกตัวอย่างตัวอย่างวิธีการที่เห็นว่าช่วยลดความเสี่ยงได้

การพิสูจน์ตัวตนลูกค้าโดยทั่วไป ผู้ประกอบธุรกิจจะใช้การตรวจสอบ (verify/validate) ข้อมูลลูกค้าด้วยการตรวจสอบหลักฐานอ้างอิงข้อมูลที่ลูกค้าแจ้งมา ซึ่งเดิมการตรวจสอบหลักฐาน ผู้ประกอบธุรกิจอาจจะตรวจสอบหลักฐานตัวจริง เช่น เมื่อพบลูกค้าต่อหน้า จะขอบัตรประชาชนจากลูกค้ามาทำสำเนา ซึ่งจะเป็นโอกาสให้ผู้ประกอบธุรกิจสามารถสังเกตดูบัตรประชาชนได้ว่ามีจุดใดที่ปลอมแปลงมาหรือไม่ ปัจจุบันกรณีลูกค้ามาเปิดบัญชีแบบพบหน้า ผู้ประกอบธุรกิจอาจนำเทคโนโลยีเข้ามาช่วยในการตรวจสอบหลักฐาน เช่น นำบัตรประชาชนมาเสียบกับเครื่องอ่านบัตร (dip chip) เพื่อตรวจสอบข้อมูลในชิพในบัตรว่าตรงกับข้อมูลหน้าบัตรและข้อมูลที่ลูกค้ากรอกในใบคำขอเปิดบัญชี รวมถึงเทียบใบหน้าลูกค้าทั้งบนหน้าบัตร ในชิพและใบหน้าจริงของลูกค้าว่าตรงกันหรือไม่ ซึ่งเจ้าหน้าที่ที่ทำหน้าที่ตรวจสอบในขั้นตอนนี้ควรมีความชำนาญและมีความระมัดระวังเพื่อให้มั่นใจว่าการตรวจสอบมีคุณภาพ

อย่างไรก็ดี หากเป็นการทำ KYC แบบ online ผู้ประกอบธุรกิจไม่ได้เจอตัวลูกค้า ไม่ได้จับต้องหลักฐานตัวจริง จึงมีความเป็นไปได้ที่ลูกค้าจะปลอมหลักฐานส่งให้ผู้ประกอบธุรกิจด้วยหลายสาเหตุ หรือนำหลักฐานของคนอื่นมาใช้ ดังนั้น ผู้ประกอบธุรกิจจึงควร<u>ใช้วิธีการที่น่าเชื่อถือในการตรวจสอบข้อมูลและหลักฐานของลูกค้าด้วยการตรวจสอบหลักฐานกับผู้ออกหลักฐาน (issuing source) หรือแหล่งข้อมูลที่น่าเชื่อถือ (authoritative source)</u> เช่น ตรวจสอบ (validate) บัตรประชาชน online กับฐานข้อมูลของกรมการปกครอง[11]

[10] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551

[11] การตรวจสอบบัตรประชาชน online กับกรมการปกครองเป็นการกรอกข้อมูลที่อยู่บนบัตรประชาชน 5 อย่างได้แก่ ชื่อ นามสกุล วันเดือนปีเกิด เลขที่บัตรประชาชน และ laser code หลังบัตร บนระบบ web-service ของกรมการปกครอง โดยระบบจะแจ้งสถานะบัตร เช่น ใช้งานได้ปกติ หรือถูกขโมยหรือถูกออกบัตรใหม่ เป็นต้น แต่ไม่เห็นรูปถ่ายลูกค้าในฐานข้อมูล

เพื่อให้รู้ว่าบัตรประชาชนที่นำมาเปิดบัญชีนั้นมีสถานะปกติ ไม่ได้มีการแจ้งหาย ยกเลิก หรือทำบัตรใหม่มาทดแทนแล้ว และข้อมูลบนบัตรตรงกับฐานข้อมูลของกรมการปกครอง อย่างไรก็ดี วิธีการนี้ยังมีความเสี่ยงที่บุคคลที่นำบัตรประชาชนดังกล่าวมาเปิดบัญชี ไม่ใช่เจ้าของบัตร เนื่องจากไม่สามารถเห็นรูปถ่ายที่อยู่ในฐานข้อมูลได้ จึงยังมีความเสี่ยงว่าลูกค้าอาจใช้บัตรประชาชนของคนอื่นมาเปิดบัญชี ผู้ประกอบธุรกิจจึงต้องมีการตรวจสอบความสอดคล้องของตัวลูกค้ากับหลักฐาน เพื่อให้รู้ว่าลูกค้าเป็นเจ้าของหลักฐานนั้น โดยจะกล่าวต่อไปในข้อ 3 การตรวจสอบตัวบุคคล

หลักฐานที่น่าเชื่อถืออีกประเภทหนึ่งที่สามารถใช้ในการยืนยันตัวตนได้คือ *passport ซึ่งมีการเก็บข้อมูลในชิพตามมาตรฐาน International Civil Aviation Organization (ICAO)* ที่สามารถใช้เทคโนโลยี NFC หรือ Near Field Communication ผ่าน smart phone เพื่ออ่านข้อมูลในชิพใน passport ซึ่งจะเห็นได้ทั้งข้อมูลและรูปถ่ายลูกค้า มีความน่าเชื่อถือสูง เนื่องจากเป็นข้อมูลซึ่งอยู่ในชิพที่ปลอมแปลงได้ยาก และข้อดีของการใช้ passport อีกประการหนึ่งคือ รูปถ่ายลูกค้าที่อยู่ในชิพมีความละเอียดสูง สามารถใช้ประโยชน์หากต้องการเทียบใบหน้าลูกค้ากับรูปถ่ายด้วยเทคโนโลยี facial recognition

3. การตรวจสอบตัวบุคคล

ในการพิสูจน์ว่าลูกค้าเป็นเจ้าของหลักฐานที่นำมาเปิดบัญชีนั้น ผู้ประกอบธุรกิจควรมีวิธีการตรวจสอบความสอดคล้องของตัวลูกค้ากับหลักฐานที่ลูกค้าแสดงเพื่อลดความเสี่ยงที่ลูกค้าจะใช้หลักฐานของผู้อื่นมาเปิดบัญชี เช่น เทียบใบหน้าลูกค้ากับรูปถ่ายจากแหล่งข้อมูลที่น่าเชื่อถือหรือรูปถ่ายบนหลักฐาน

ยกตัวอย่างกรณีการเปิดบัญชีแบบ online ไม่ได้พบตัวจริงลูกค้า ผู้ประกอบธุรกิจจึงให้ลูกค้าถ่ายภาพตนเอง หรือ VDO clip และถ่ายภาพบัตรประชาชนด้วยความละเอียดของภาพที่เพียงพอ แล้วผู้ประกอบธุรกิจจัดให้มีเจ้าหน้าที่พิจารณาว่าลูกค้ามีใบหน้าตรงกันกับภาพบนหลักฐาน (physical comparison) ซึ่งควรใช้เจ้าหน้าที่มีความชำนาญ ได้รับการอบรมในเรื่องที่เกี่ยวข้องอย่างเพียงพอ หรือหากต้องการเพิ่มความมั่นใจยิ่งขึ้น อาจนำเทคโนโลยีการเปรียบเทียบใบหน้า (facial recognition) เข้ามาปรับใช้ และควรกำหนดระดับความผิดพลาดในการเปรียบเทียบ (false match rate : FMR) ในระดับต่ำ

อย่างไรก็ดี การเทียบภาพถ่ายลูกค้ากับภาพถ่ายบนบัตรประชาชนยังมีความเสี่ยงที่ผู้ประกอบธุรกิจควรคำนึงถึงคือ การปลอมรูปบนหน้าบัตรประชาชนเพื่อให้สอดคล้องกับผู้ที่นำบัตรมาเปิดบัญชี ซึ่งผู้ประกอบธุรกิจอาจกำหนดวิธีการบริหารความเสี่ยงเพิ่มเติม เช่น การขอหลักฐานที่น่าเชื่อถือมาตรวจสอบอีก 1 ชิ้น หรือจำกัดความเสี่ยงด้วยการจำกัดประเภทบัญชีและวงเงินที่ไม่สูงนัก และมีการติดตามการซื้อขายอย่างต่อเนื่องพร้อมทั้งรีบทบทวนข้อมูลลูกค้าทันทีหากพบความผิดปกติ เช่น การโอนเงินเข้าบัญชีจำนวนมากหรือมีการซื้อขายเกินวงเงิน

นอกจากนั้น ผู้ประกอบธุรกิจอาจพัฒนาการเปรียบเทียบข้อมูลอื่นเท่าที่เทคโนโลยีหรือฐานข้อมูลที่ใช้เปรียบเทียบจะเอื้ออำนวย เช่น การเปรียบเทียบลายนิ้วมือของลูกค้ากับลายนิ้วมือที่อยู่ในหลักฐาน ซึ่งจะช่วยเพิ่มความน่าเชื่อถือได้อีกระดับ ทั้งยังช่วยแก้ปัญหาที่การเทียบใบหน้ากับรูปถ่ายไม่สามารถทำได้ คือ การแยกแยะคู่แฝดที่อาจนำบัตรประชาชนของอีกคนมาใช้ เป็นต้น

VDO conference

อีกวิธีการหนึ่งที่อาจช่วยให้ผู้ประกอบธุรกิจตรวจสอบตัวบุคคลได้ คือการพิจารณาความสอดคล้องของตัวลูกค้ากับหลักฐาน ด้วยการทำ VDO conference เพื่อพูดคุยกับลูกค้า ซึ่งนอกจากจะแสดงได้ว่า ได้คุยกับคนจริง ๆ เห็นหน้าตาแล้ว อาจให้ลูกค้าแสดงหลักฐานตัวจริง เช่น แสดงบัตรประชาชนทั้งด้านหน้า-หลัง ผ่านหน้ากล้องให้เจ้าหน้าที่ได้สังเกตรายละเอียดต่าง ๆ ว่าบัตรเป็นของจริง มีข้อมูลตรงกับภาพหลักฐานที่ส่งให้เพิ่มความมั่นใจว่าหลักฐานเป็นของจริง และการได้พูดคุยยังช่วยให้เจ้าหน้าที่สามารถสังเกตลักษณะ ท่าทาง พฤติกรรมลูกค้าว่ามีความผิดปกติหรือไม่ การพูดคุยตอบคำถามสอดคล้องกับความรู้ ประสบการณ์ลงทุนที่แจ้งไว้เพื่อให้บริการได้อย่างเหมาะสม

อย่างไรก็ดี เทคโนโลยีที่ก้าวหน้า ทำให้การปลอมแปลงตัวตนบน VDO conference มีความเป็นไปได้มากขึ้น ผู้ประกอบธุรกิจที่เลือกใช้วิธีการนี้ จึงควรระวังการปลอมแปลงตัวตน และปรับปรุงรูปแบบ วิธีการ รวมถึงเทคนิคต่าง ๆ ที่จะช่วยป้องกันการปลอมแปลงตัวตนผ่าน VDO conference อย่างต่อเนื่อง เพื่อให้การใช้เครื่องมือดังกล่าวเกิดประโยชน์สูงสุด ช่วยให้รู้จักลูกค้าได้อย่างแท้จริง คุ้มค่ากับค่าใช้จ่ายด้านระบบที่จะใช้ดำเนินการและการจัดเก็บไฟล์เพื่อเป็นหลักฐานอ้างอิงในอนาคต ผู้ประกอบธุรกิจสามารถใช้เทคนิคต่อไปนี้ในการเพิ่มคุณภาพการทำ 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

ผู้ประกอบธุรกิจสามารถศึกษามาตรฐานขั้นต่ำด้านเทคนิคในเรื่องคุณภาพของภาพถ่ายลูกค้าและการทำ VDO conference ได้ที่ Appendix 3 ตัวอย่างมาตรฐานขั้นต่ำด้านเทคนิคในเรื่องคุณภาพของภาพถ่ายลูกค้าและการทำ VDO conference เพื่อให้การบริหารความเสี่ยงเพิ่มเติมด้วยวิธีการดังกล่าวมีคุณภาพเพียงพอที่จะนำมาประกอบการทำความรู้จักลูกค้าได้อย่างแท้จริง

อย่างไรก็ดี หากผู้ประกอบธุรกิจพิจารณาว่าลูกค้าจัดอยู่ในกลุ่มเสี่ยงสูงหรือวงเงินสูง ก็ควรพิจารณานัดพบกับลูกค้าเพื่อพูดคุย และขอดูหลักฐานตัวจริง เพื่อให้เป็นไปตามกรอบการบริหารความเสี่ยงที่เหมาะสม

4. การตรวจสอบช่องทางติดต่อ

ผู้ประกอบธุรกิจควรมีการตรวจสอบช่องทางการติดต่อของลูกค้าที่ได้ให้ไว้ในขั้นตอนการเปิดบัญชีว่าสามารถติดต่อลูกค้าได้จริง ลูกค้าคือเจ้าของช่องทางที่ใช้ในการติดต่อจริง รวมถึงมั่นใจว่าผู้ประกอบธุรกิจจะสามารถติดต่อหรือส่งข้อมูลข่าวสารสำคัญไปยังลูกค้าผ่านช่องทางดังกล่าวได้จริง ตัวอย่างวิธีการตรวจสอบ เช่น

- การส่ง OTP ไปยังหมายเลขโทรศัพท์มือถือให้ลูกค้ากรอกเข้าระบบของผู้ประกอบธุรกิจ
- การส่งข้อความไปยังอีเมล์ที่ลูกค้าแจ้งไว้ พร้อมแนบ link ให้ลูกค้าคลิกยืนยันกลับมายังผู้ประกอบธุรกิจ

ตัวอย่างวิธีการทำ identity proofing ที่กล่าวมาข้างต้นนี้ เป็นตัวอย่างวิธีการที่สำนักงานเห็นว่ามีความเหมาะสมที่จะช่วยให้การพิสูจน์ตัวตนลูกค้าบรรลุหลักการตามประกาศของสำนักงานได้ ผู้ประกอบธุรกิจสามารถศึกษาตัวอย่างวิธีการทำ Identity proofing เพิ่มเติมได้ที่ Appendix 4 ตัวอย่างวิธีการทำ Identity proofing ที่ได้ระดับ IAL 2.1 บวกตรวจสอบหลักฐานกับผู้ออกหรือแหล่งข้อมูลที่น่าเชื่อถือ (online)

อย่างไรก็ดี เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงที่รวดเร็ว ซึ่งความเสี่ยงต่าง ๆ ก็เปลี่ยนแปลงไปตามเทคโนโลยีเช่นกัน จึงมีความเป็นไปได้ว่าในอนาคต ตัวอย่างวิธีการในการทำ Identity proofing นี้อาจล้าสมัยหรือไม่ได้ประสิทธิภาพ สำนักงานจึงขอให้ผู้ประกอบธุรกิจมีการทบทวนวิธีการของตนเองให้เหมาะสมตามสถานการณ์ที่เปลี่ยนแปลงไป เพื่อให้วิธีการที่เลือกใช้บรรลุหลักการของสำนักงานได้อย่างต่อเนื่อง

2.2 การยืนยันตัวตน (AUTHENTICATION)

<u>การกำหนดมาตรฐานขั้นต่ำในการยืนยันตัวตนสำหรับตลาดทุน</u>

การยืนยันตัวตนในธุรกรรมของตลาดทุนนั้น เป็นอีกเรื่องสำคัญที่สำนักงานกำหนดแนวทางไว้ โดยแบ่งตามวัตถุประสงค์ 2 เรื่อง ได้แก่

1. การยืนยันตัวตนในระบบ Digital ID: เมื่อผู้ขอใช้บริการ ต้องการเปิดบัญชีกับผู้ประกอบธุรกิจ เช่น บล. โดย บล. ใช้การพิสูจน์ตัวตนผ่านระบบ Digital ID ซึ่งในกระบวนการดังกล่าวจะมีขั้นตอนให้ผู้ขอใช้บริการเข้าไปยืนยันตัวตน (Authenticate) กับ IdP ที่ตนเองเคยพิสูจน์ตัวตนไว้ตามระดับความน่าเชื่อถือ (AAL) ที่ บล. กำหนด ซึ่งเมื่อผู้ขอใช้บริการยืนยันตัวตนสำเร็จ IdP จึงส่งคำยืนยันไปให้ บล. ว่า ผู้ขอใช้บริการคนนี้คือคนที่เคยมาพิสูจน์ตัวตนกับ IdP แล้ว

การกำหนดระดับความน่าเชื่อถือในการยืนยันตัวตนเมื่อมีการใช้บริการพิสูจน์ตัวตนผ่านระบบ Digital ID นั้น **สำนักงานและหน่วยงานที่เกี่ยวข้องได้ร่วมกันกำหนดความน่าเชื่อถือที่ระดับ 2.1 คือมีการใช้ปัจจัยยืนยันตัวตนมากกว่า 1 ปัจจัย**

2. การยืนยันตัวตนเพื่อเข้าทำธุรกรรมในระบบ online: เมื่อผู้ขอใช้บริการเปิดบัญชีกับ บล. แล้ว และต้องการเข้าระบบเพื่อทำธุรกรรมต่าง ๆ ก็ต้องมีขั้นตอนการยืนยันตัวตนเพื่อให้มั่นใจได้ว่า ลูกค้าเป็นผู้เข้ามาใช้งานระบบด้วยตนเองเพื่อให้ บล. บรรลุวัตถุประสงค์ตามหลักเกณฑ์ของสำนักงานในเรื่องการให้บริการลูกค้าอย่างเหมาะสม ซึ่งระดับความน่าเชื่อถือในการยืนยันตัวตนในขั้นตอนนี้ สำนักงานกำหนดหลักการให้ผู้ประกอบธุรกิจต้องมีกระบวนการในการยืนยันตัวตนของลูกค้า (authentication) ที่เหมาะสมและน่าเชื่อถือ เพื่อให้มั่นใจว่าการลงทุนหรือการทำธุรกรรมในผลิตภัณฑ์ตลาดทุนได้กระทำโดยลูกค้าหรือผู้ได้รับมอบอำนาจจากลูกค้าที่ผู้ประกอบธุรกิจติดต่อและให้บริการ[12] อย่างไรก็ดี สำนักงานไม่ได้กำหนดวิธีการทำ authentication ที่เป็นการเฉพาะตายตัว แต่เสนอแนะให้ผู้ประกอบธุรกิจกำหนดวิธีการที่น่าเชื่อถือ โดยพิจารณาถึงจุดสมดุลระหว่างความสะดวกรวดเร็วในการเข้าใช้บริการของลูกค้ากับผลกระทบที่อาจเกิดขึ้นหากเกิดความผิดพลาดในการยืนยันตัวตน แล้วจึงพิจารณาเลือกวิธีการที่เหมาะสมกับความเสี่ยงของธุรกรรม และต้องมั่นใจว่า มีการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นได้อย่างเหมาะสม ยกตัวอย่างเช่น หากเป็นการเข้าระบบเพื่อดูข้อมูลบัญชีเพียงอย่างเดียวอาจเข้าระบบด้วยปัจจัยเพียงอย่างเดียว เช่น การใช้ username/ password แต่หากเป็นธุรกรรมที่มีความ

[12] ร่างประกาศ สธ. .../ 2561 ผู้ประกอบธุรกิจต้องมีระบบงานที่ทำให้มั่นใจได้ว่าการกำหนดขั้นตอนและวิธีการในรายละเอียดของกระบวนการติดต่อและให้บริการแก่ลูกค้าได้มีการคำนึงถึงเรื่องต่อไปนี้ รวมทั้งสอดคล้องและเหมาะสมกับผลิตภัณฑ์ในตลาดทุนหรือบริการแต่ละประเภท และมีกระบวนการในการยืนยันตัวตนของลูกค้า (authentication) ที่เหมาะสมและน่าเชื่อถือ เพื่อให้มั่นใจว่าการลงทุนหรือการทำธุรกรรมในผลิตภัณฑ์ในตลาดทุนได้กระทำโดยลูกค้าหรือผู้ได้รับมอบอำนาจจากลูกค้าที่ผู้ประกอบธุรกิจติดต่อและให้บริการ

เสี่ยงสูงขึ้น เช่น ขยายวงเงิน หรือเปลี่ยนแปลงข้อมูลในบัญชีได้ด้วย ควรใช้ปัจจัยยืนยันตัวตนที่แตกต่างกัน 2 อย่าง ประกอบกัน (two-factor authentication) เช่น การใช้ username/password (something you know) ประกอบกับ OTP (something you have)

หรือกรณีที่เป็นธุรกรรมที่ต้องการความรวดเร็วในการดำเนินการ เช่น การส่งคำสั่งซื้อขาย หากผู้ประกอบธุรกิจเลือกใช้ปัจจัยยืนยันตัวตนที่ต้องการความสะดวกรวดเร็ว เช่น username/password (something you know) ประกอบกับ pin code (something you know) จะต้องคำนึงถึงการบริหารความเสี่ยงที่อาจเกิดขึ้นให้เหมาะสม

<u>ข้อเสนอแนะเกี่ยวกับการกำหนดวิธีการยืนยันตัวตน</u>

ปัจจัยในการยืนยันตัวตน : การใช้บริการแบบ online นั้น เมื่อลูกค้าต้องการจะเข้าระบบ ผู้ประกอบธุรกิจจะต้องมีการกำหนดขั้นตอน authentication ก่อนการใช้บริการระบบ โดยใช้สิ่งที่เรียกว่าปัจจัยยืนยันตัวตน

การยืนยันตัวตนในโลก online นั้น ตามปกติมักใช้ปัจจัย 3 ประเภทในการยืนยันตัวตน ได้แก่

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

ปัจจัยเหล่านี้ ลูกค้าอาจได้รับจากผู้ประกอบธุรกิจ เช่น username/password หรือลงทะเบียนไว้กับผู้ประกอบธุรกิจ เช่น บันทึกลายนิ้วมือไว้ตั้งแต่ขั้นตอนการลงทะเบียนและพิสูจน์ตัวตน เพื่อให้ลูกค้านำกลับมาใช้ในการยืนยันตัวตนเพื่อเข้าใช้ระบบในภายหลัง ซึ่งการกำหนดให้ลูกค้าใช้ปัจจัยยืนยันตัวตนเพื่อเข้าใช้ระบบผู้ประกอบธุรกิจอาจกำหนดวิธีการที่มีความน่าเชื่อถือ เช่น

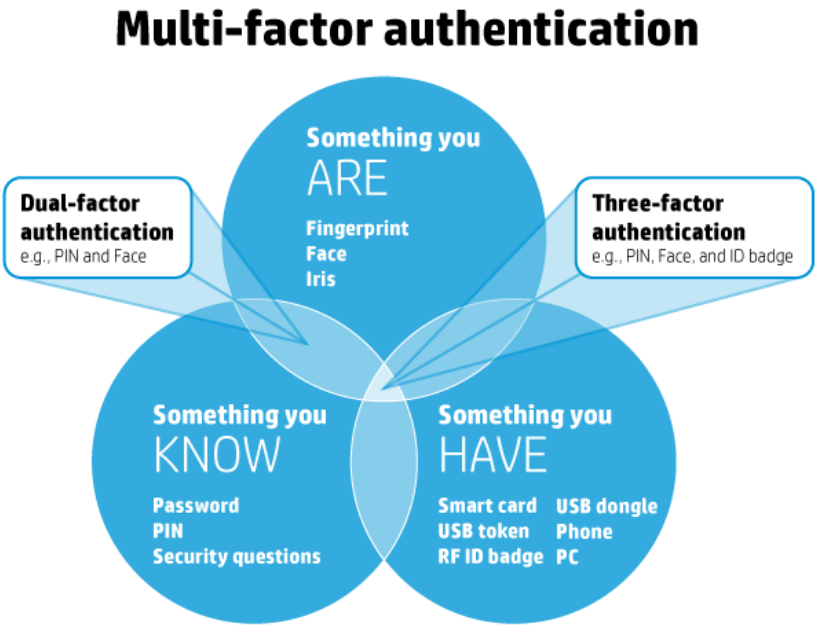
1. <u>กำหนดจำนวนปัจจัยในการยืนยันตัวตนเพื่อเข้าระบบให้เหมาะสมกับความเสี่ยงของธุรกรรม</u>

ปัจจัยในการยืนยันตัวตนแต่ละประเภทมีหลายชนิด ผู้ประกอบธุรกิจสามารถเลือกผสมผสานปัจจัยมากกว่า 1 ชนิดเพื่อช่วยเพิ่มความน่าเชื่อถือในการยืนยันตัวตน

ทั้งนี้ การจะเลือกใช้ปัจจัยประเภทหรือชนิดใดมาประกอบกันนั้น ผู้ประกอบธุรกิจอาจพิจารณาว่าปัจจัยทั้ง 2 อย่างนั้น เมื่อใช้ร่วมกันแล้วจะช่วยให้การยืนยันตัวตนมีความน่าเชื่อถือเพิ่มขึ้น จากตัวอย่างข้างต้น คือการใช้ username/password (something you have) ประกอบกับ OTP (something you know) 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

ประเภทของปัจจัยยืนยันตัวตน	ตัวอย่างชนิดของปัจจัยยืนยันตัวตน		
something you have	mobile phone	smart card	USB token
something you know	password	pin code	security question
something you are	finger print	face	iris



Source: https://store.hp.com/us/en/cv/taw-article?ai=16&ap=5&au=3-ways-to-create-more-secure-passwords&am=Nov&ay=2015#true

2. <u>กำหนดคุณภาพของปัจจัยให้เหมาะสม</u>[13]

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 หรือ ยอมรับการยืนยันตัวตนจาก 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
  - ควรมีการเก็บตัวอย่าง biometric ที่มีคุณภาพ
  - เทคโนโลยีที่ใช้เปรียบเทียบควรมีความผิดพลาด (False Match Rate: FMR) ไม่เกิน 1 ใน 1,000
  - ควรจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดได้ไม่เกิน 5 ครั้ง

[13] อ้างอิงจากข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการลงทะเบียนและพิสูจน์ตัวตนและการยืนยันตัวตน – การยืนยันตัวตน https://standard.etda.or.th/wp-content/uploads/2018/10/20171204-ER-DigitalID-Authentication-V01-20F.pdf

3. <u>การใช้ช่องทางรับส่งปัจจัยยืนยันตัวตนที่มีความมั่นคงปลอดภัยสูง</u>

การยืนยันตัวตนผ่านระบบอิเล็กทรอนิกส์นั้น มีความเสี่ยงที่ผู้ไม่ประสงค์ดีจะกระทำการด้วยวิธีการต่าง ๆ ที่จะทำให้เกิดความผิดพลาดในการยืนยันตัวตน เนื่องมาจากกระบวนการให้บริการลูกค้าผ่านระบบอิเล็กทรอนิกส์นั้น ต้องมีการรับ-ส่งข้อมูลระหว่างกันผ่านระบบอิเล็กทรอนิกส์ซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่ประสงค์ดีจะใช้วิธีการต่าง ๆ ที่จะทำให้เกิดความผิดพลาดในการยืนยันตัวตน เช่น เข้ามาแก้ไขข้อมูล หรือแอบดักขโมยข้อมูล 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)[14] ซึ่งจัดทำโดย สพธอ.

[14] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน DIGITAL IDENTITY GUIDELINE FOR THAILAND AUTHENTICATION เวอร์ชั่น 1.0 https://standard.etda.or.th/wp-content/uploads/2018/10/20171204-ER-DigitalID-Authentication-V01-20F.pdf

2.3 การทำความรู้จักลูกค้าเพื่อให้บริการเหมาะสม (CLIENT DUE DILIGENCE : CDD)

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

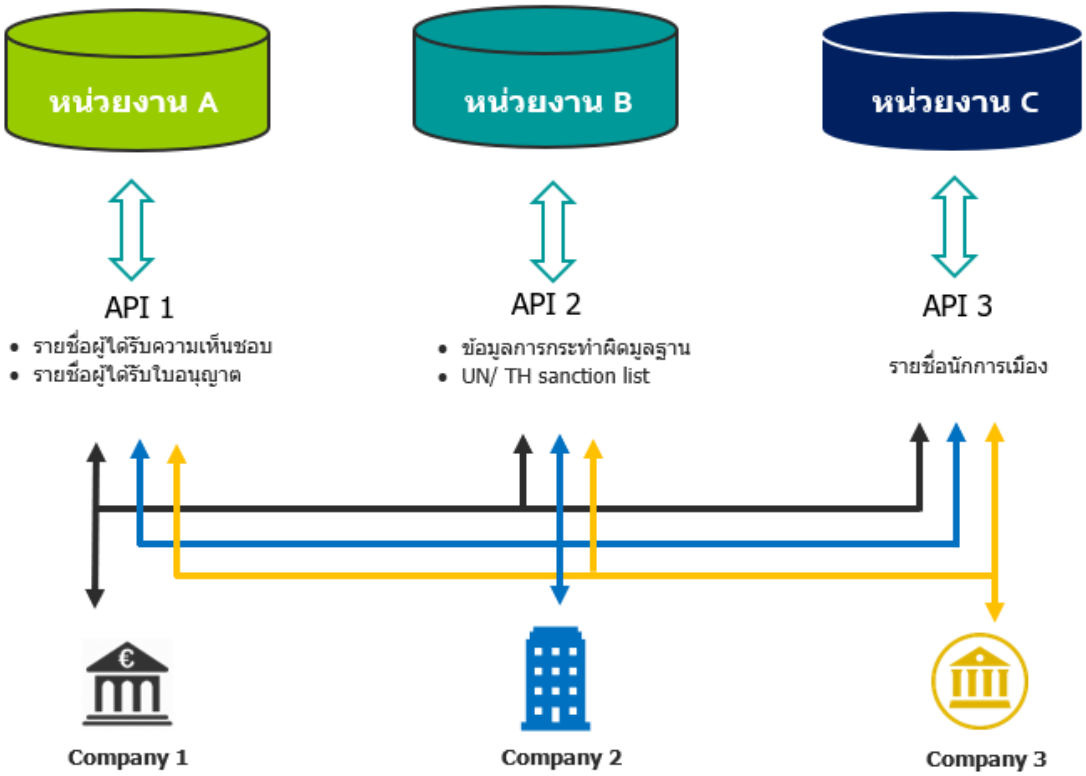
หรือในอนาคตหากมีฐานข้อมูลกลางของหน่วยงานรัฐหรือระบบที่เอกชนพัฒนาขึ้น หรือหน่วยงานกลางที่อาจมีการจัดตั้งขึ้นโดยเฉพาะเพื่อรวบรวมหรือเป็นศูนย์กลางในการเชื่อมโยงข้อมูลดังกล่าว เช่น ระบบ Digital ID ที่หน่วยงานรัฐและเอกชนซึ่งมีข้อมูลที่น่าเชื่อถือจะพิจารณาเข้ามาร่วมเป็นสมาชิกในฐานะ Authoritative Source หรือ AS โดยหากผู้ประกอบธุรกิจที่เป็นสมาชิกในระบบ Digital ID แล้วต้องการข้อมูลของลูกค้าเพื่อใช้ในการพิจารณาประกอบการเปิดบัญชีและทำ KYC ก็สามารถ request ผ่านระบบ Digital ID ไปยัง AS ที่มีข้อมูลที่ต้องการเพื่อให้ส่งข้อมูลหรือยืนยันข้อมูลของลูกค้าได้ การตรวจสอบข้อมูลลูกค้าจึงทำได้ได้อย่างสะดวก 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 (ตามประกาศ ทธ. 35/2556)

- ความสามารถและแหล่งที่มารายได้
- ฐานะการเงิน
- ประสบการณ์
- ความรู้
- วัตถุประสงค์ในการลงทุน
- ความเสี่ยงที่รับได้

ตัวอย่างการเชื่อมโยงข้อมูลด้วย API



2.4 การทบทวนข้อมูลลูกค้าและการทำความรู้จักลูกค้าเชิงลึก (ONGOING/ ENHANCED KYC)

การทำ Ongoing และ Enhanced KYC นั้น ผู้ประกอบธุรกิจสามารถใช้เทคโนโลยีเข้ามาช่วยลดภาระในการดำเนินการได้ เช่น การใช้โปรแกรมอัตโนมัติต่าง ๆ ที่ช่วยให้การทำงานง่ายขึ้น อาทิ การแจ้งเตือนอัตโนมัติเมื่อลูกค้าครบกำหนดต้องทบทวนข้อมูล KYC หรือโปรแกรมวิเคราะห์ข้อมูลความเสี่ยงลูกค้า เป็นต้น เครื่องมือทางอิเล็กทรอนิกส์เหล่านี้จะช่วยลดภาระของผู้ประกอบธุรกิจ ลดความเสี่ยงที่จะทำผิดกฎหมาย/กฎเกณฑ์ ใช้เวลาทำงานน้อยลง มีความถูกต้องมากขึ้น โปรแกรมเหล่านี้มีบริษัทผู้พัฒนาขึ้นมาให้บริการมากมาย ซึ่งการจะเลือกใช้โปรแกรมใดนั้น ผู้ประกอบธุรกิจต้องพิจารณาถึงความน่าเชื่อถือ หรือผู้ประกอบธุรกิจสามารถพัฒนาได้เอง ซึ่งถือได้ว่าเป็นการใช้ Regulatory Technology หรือ RegTech เข้ามาช่วยในการดำเนินงานนั่นเอง

สำนักงานสนับสนุนให้ผู้ประกอบธุรกิจใช้เทคโนโลยีเข้ามาช่วยในการทบทวนข้อมูลลูกค้าและการทำความรู้จักลูกค้าเชิงลึก เนื่องจากช่วยสร้างประสิทธิภาพ ความถูกต้อง และรวดเร็วในการดำเนินงาน ช่วยลดโอกาสที่จะเกิดการกระทำผิดในตลาดทุนได้ เนื่องจากลูกค้าที่เปิดบัญชีแบบ online และทำ e-KYC เป็นลูกค้ากลุ่มที่ผู้ประกอบธุรกิจอาจไม่ได้พบหน้า พบตัวจริงเลย ผู้ประกอบธุรกิจจึงควรให้ความสำคัญกับลูกค้ากลุ่มนี้สูงขึ้น เช่น กำหนดนโยบายให้มีการติดตามธุรกรรมใกล้ชิด พิจารณา trade volume กับวงเงินที่ได้รับว่าสอดคล้องกันหรือไม่ มีการกำหนดเงื่อนไข enhanced KYC เข้มขึ้นเมื่อพบธุรกรรมผิดปกติ เช่น ซื้อขายเกินวงเงิน ไม่เหมาะสมสอดคล้องกับ profile เป็นต้น นโยบายเหล่านี้ จะช่วยป้องกันทั้งตัวผู้ประกอบธุรกิจเองจากความเสี่ยงที่ลูกค้าจะใช้บัญชีเป็นช่องทางกระทำผิด และช่วยให้ผู้ประกอบธุรกิจตรวจจับพฤติกรรมผิดปกติที่เกิดจากการถูก hack เข้ามาทำธุรกรรมที่เจ้าของบัญชีไม่ได้เป็นผู้ดำเนินการได้อีกด้วย

3. ระบบงานที่เกี่ยวข้องกับการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า

3.1 IT System

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 อาจจะเป็นช่องโหว่ ที่ก่อให้เกิดความเสียหายชื่อเสียง และความเชื่อมั่นได้อย่างมากเช่นเดียวกัน การบริหารความเสี่ยงในเรื่องที่เกี่ยวข้องอย่างเหมาะสมตลอดทั้งกระบวนการที่จะดำเนินการ จึงเป็นเรื่องที่ผู้ประกอบธุรกิจควรคำนึงถึงอยู่เสมอ

ทั้งนี้ ในช่วงต้นของแนวปฏิบัติฯ 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 สำนักงานมีการกำหนดแนวทางการดำเนินการไว้ในประกาศเรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ[15] ที่ผู้ประกอบธุรกิจสามารถนำมาปรับใช้เพิ่มเติมในการกำหนดในเรื่องอื่น ๆ ที่เกี่ยวข้อง เช่น การกำหนดให้มีการควบคุมการเข้าถึง

[15] ประกาศ นป. 3/2559 เรื่อง การจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 12 กันยายน 2559

ข้อมูลและระบบสารสนเทศ การควบคุมการเข้ารหัสข้อมูล การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (outsource) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เป็นต้น

3.2 RECORD KEEPING

การคุ้มครองข้อมูลของลูกค้า

การรวบรวมข้อมูลลูกค้าเพื่อประกอบการทำ KYC นี้ ผู้ประกอบธุรกิจต้องคำนึงถึงการคุ้มครองข้อมูลของลูกค้า โดยต้องมีการจัดเก็บข้อมูลอย่างเหมาะสม ป้องกันการเข้าถึงข้อมูลอย่างไม่ถูกต้อง หรือขัดกับกฎหมายตามเกณฑ์ที่สำนักงานกำหนด

กฎเกณฑ์ของสำนักงาน[16] กำหนดให้ผู้ประกอบธุรกิจจัดเก็บข้อมูลที่เกี่ยวข้องในการให้บริการลูกค้าไว้ในรูปแบบที่เหมาะสม เช่น มีระบบจัดเก็บข้อมูลลูกค้าที่รัดกุม เป็นระเบียบ มีความปลอดภัยในการจัดเก็บ สามารถป้องกันการแก้ไข หรือถูกทำลาย หรือมีการเข้ารหัสข้อมูล (data encryption) เพื่อป้องกันความปลอดภัยให้กับข้อมูล กำหนดสิทธิในการเข้าถึงข้อมูลเพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าดูข้อมูล และมีการสำรองข้อมูลเพื่อป้องกันการสูญหาย เป็นต้น โดยเฉพาะอย่างยิ่งหากมีการเก็บข้อมูล sensitive ของลูกค้า เช่น ข้อมูลส่วนบุคคล ข้อมูลภาพถ่ายหรือ biometric ของลูกค้า ต้องใช้ระบบที่มีความปลอดภัยสูงในการจัดเก็บข้อมูลเหล่านี้เพราะหากรั่วไหลไปสู่บุคคลอื่นจะสร้างความเสียหายต่อเจ้าของข้อมูลได้มาก นอกจากนั้น ผู้ประกอบธุรกิจต้องเก็บรักษาข้อมูลตามระยะเวลาที่สำนักงานประกาศกำหนด เพื่อสามารถใช้อ้างอิงหรือเพื่อการตรวจสอบได้ในอนาคต

ผู้ประกอบธุรกิจยังต้องศึกษาและปฏิบัติตามกฎหมายอื่นที่เกี่ยวข้อง เช่น ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย[17] ที่กำหนดเรื่องการขอข้อมูลจากลูกค้า เช่น ให้ขอเท่าที่จำเป็น ต้องแจ้งวัตถุประสงค์และขอบเขตในการใช้ข้อมูลเหล่านั้นให้ลูกค้าทราบอย่างชัดเจนและเฉพาะเจาะจง และลูกค้าต้องเต็มใจที่จะให้ความยินยอม (consent) ให้ใช้ข้อมูลตามวัตถุประสงค์ที่แจ้ง รวมถึงข้อความที่ระบุในการขอความยินยอมต้องชัดเจน ไม่คลุมเครือ เป็นต้น นอกจากนั้น ผู้ประกอบธุรกิจต้องแจ้งให้ลูกค้าทราบถึงสิทธิของลูกค้า เช่น สิทธิในการเข้าถึงข้อมูล สิทธิในการแก้ไขข้อมูล สิทธิในการลบหรือยกเลิกการให้ข้อมูล เป็นต้น

นอกจากกฎหมายของไทยที่ผู้ประกอบธุรกิจต้องปฏิบัติตามแล้ว ผู้ประกอบธุรกิจควรพิจารณาระมัดระวังการดำเนินการกับข้อมูลส่วนบุคคลของลูกค้าที่ได้รับการคุ้มครองโดยกฎหมายอื่น เช่น General Data Protection Regulation[18] หรือ GDPR ซึ่งผู้ประกอบธุรกิจที่มีสถานประกอบการอยู่ภายในสหภาพยุโรป หรือมีการประมวลผลข้อมูลที่เกี่ยวข้องกับการเสนอสินค้าหรือบริการให้แก่บุคคลผู้พำนักในสหภาพยุโรป หรือมีการประมวลผลข้อมูลซึ่งเกี่ยวข้องกับการเฝ้าสังเกตพฤติกรรมที่เกิดขึ้นในสหภาพยุโรปและรวมถึงประเทศที่มีผลผูกพันทางกฎหมายกับประเทศสหภาพยุโรป ต้องระมัดระวังการดำเนินการเกี่ยวกับข้อมูลลูกค้า โดยต้องดำเนินการให้เป็นไปตาม GDPR ด้วยข้อมูล หลักฐานต่าง ๆ ที่จะเกิดขึ้นในกระบวนการ e-KYC นั้น แม้จะอยู่ในรูปแบบที่

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

[17] ปัจจุบันยังเป็นร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

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

แตกต่างจากการทำ KYC ในรูปแบบเดิมที่เป็นกระดาษ ใช้วิธีการจัดเก็บข้อมูล หลักฐานต่าง ๆ ที่แตกต่างกัน แต่ยังคงใช้หลักการเดียวกัน

ผู้ประกอบธุรกิจควรศึกษารายละเอียดในกฎหมาย/กฎเกณฑ์ต่าง ๆ ให้ชัดเจนเพื่อให้การดำเนินการเก็บรักษาข้อมูลมีประสิทธิภาพเหมาะสมและหลีกเลี่ยงโทษที่อาจเกิดขึ้นจากความผิดพลาดได้

APPENDIX

Appendix 1: ตัวอย่างกระบวนการพิจารณาความเสี่ยงเพื่อการเลือกระดับความน่าเชื่อถือที่เหมาะสม

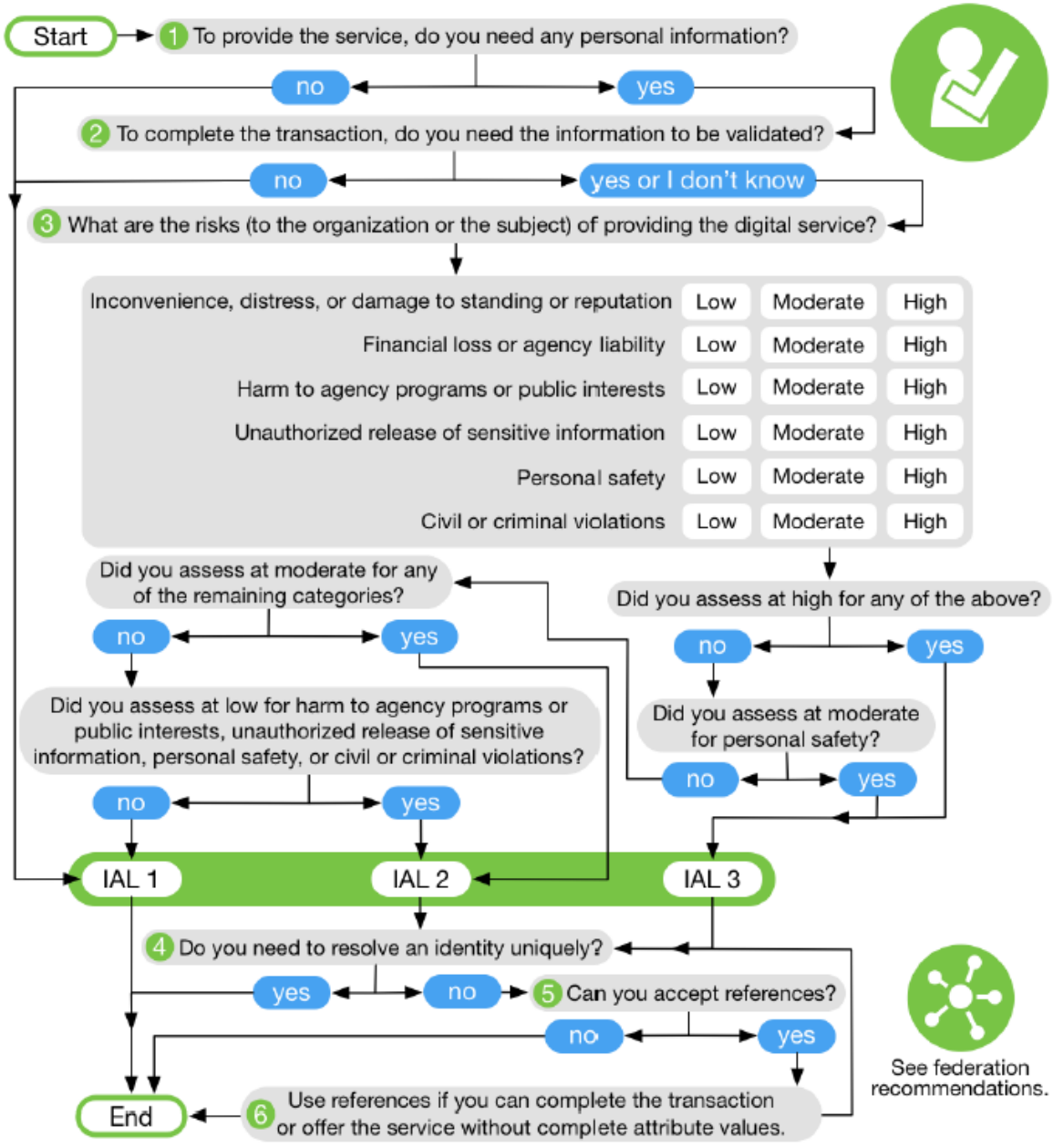


Figure 6-1 Selecting IAL

Appendix 2: 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[19] ไว้ว่า การให้บริการแบบ online นั้น ผู้ประกอบธุรกิจจะต้องกำหนดนโยบาย และกระบวนการบริหารความเสี่ยงที่เทียบเท่าหรือมากกว่าวิธีการแบบเดิม เพราะการเปิดบัญชี online นั้น มีความเสี่ยงที่ลูกค้าจะกรอกข้อมูลเท็จเพื่อปิดบังตัวตน สร้าง profile ที่ดูดีเพื่อให้เปิดบัญชีได้ หรือไม่ก็ตั้งใจจะกระทำผิดอยู่แล้วจึงเลือกเปิดบัญชีด้วยวิธีนี้ แทนที่จะต้องเจอหน้าบริษัท เพราะบริษัทจะขอดูหลักฐานที่มีรูปถ่าย ออกโดยหน่วยงานรัฐ ดังนั้น บริษัทจึงควรมีกระบวนการป้องกันการให้ข้อมูลเท็จหรือขโมยข้อมูลมาเปิดบัญชี

  นอกจากนั้น บริษัทยังมีความเสี่ยงที่จะไม่รู้จักลูกค้าอย่างแท้จริง ให้บริการไม่เหมาะสม เพราะไม่ได้พบหน้าพูดคุยกับลูกค้า ลูกค้าจึงลงทุนไม่เหมาะสมกับตนเอง เนื่องจากตามปกติแล้ว ในการให้คำแนะนำการลงทุนแก่ลูกค้า บริษัทต้องสร้าง profile ลูกค้าขึ้นมาก่อน ด้วยการถามคำถามต่าง ๆ เพื่อให้เข้าใจสถานการณ์ของลูกค้า แต่การเปิดบัญชีแบบ online นั้น จะเป็นการใช้คำถามมาตรฐานกับลูกค้าทุกคน ทำแบบอัตโนมัติ บริษัทจึงมีความเสี่ยงที่จะไม่รู้สถานการณ์ของลูกค้าได้ถ่องแท้นั่นเอง

- **Banking for International Settlements (BIS)** หรือ ธนาคารเพื่อการชำระหนี้ระหว่างประเทศได้พูดใน General guidelines to account opening[20] ว่าหากกฎหมายอนุญาตให้เปิดบัญชีแบบไม่พบหน้าได้ กระบวนการ Identify และ Verify ควรมีประสิทธิภาพเทียบเท่าการเปิดบัญชีแบบพบหน้า โดยธนาคารต้องรู้ว่าลูกค้ามีตัวตนและรู้ว่าบุคคลที่มาทำธุรกรรมกับธนาคารคือลูกค้า

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

[20] 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

ระดับความน่าเชื่อถือในการยืนยันตัวตน (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.

ระดับความน่าเชื่อถือในการยันยันตัวตนเมื่อเข้าระบบ (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.

Appendix 3: ตัวอย่างมาตรฐานขั้นต่ำด้านเทคนิคในเรื่องคุณภาพของภาพถ่ายลูกค้าและการทำ VDO conference

ข้อกำหนดด้านเทคนิค

1. มาตรฐานขั้นต่ำสำหรับความละเอียด (Resolution) ของภาพหลักฐานที่ลูกค้าส่งให้ผู้ประกอบธุรกิจผ่านระบบอิเล็กทรอนิกส์[21]

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

2. มาตรฐานขั้นต่ำของภาพถ่ายและวิดีโอสำหรับบันทึกการทำธุรกรรม[22]

มาตรฐานขั้นต่ำของภาพถ่าย

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

---

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

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

- 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

Appendix 4: ตัวอย่างวิธีการทำ Identity proofing ที่ได้ระดับ IAL 2.1 + ตรวจสอบหลักฐานกับผู้ออกหรือแหล่งข้อมูลที่น่าเชื่อถือ (online)

เปิดบัญชีแบบพบหน้า

	1 ข้อมูล	2 หลักฐาน
วัตถุประสงค์	**เพื่อรู้ว่าลูกค้าเป็นใคร**	**เพื่อยืนยันข้อมูลที่ลูกค้าแจ้ง + ดูว่าตัวลูกค้าสอดคล้องกับข้อมูล/ หลักฐาน**
1. การแสดงตน	1. ชื่อ-นามสกุล 2. วัน/เดือน/ปี เกิด 3. เลขบัตรประชาชน 4. ที่อยู่ 5. โทรศัพท์/ อีเมล์ที่ติดต่อได้ 6. ข้อมูลอื่น ๆ เท่าที่จำเป็น	1. บัตรประชาชน หรือ passport ตัวจริง 2. ภาพถ่ายลูกค้า (optional)
2. การตรวจสอบ		1. บล. เสียบบัตรประชาชนกับ card reader หรือ ใช้ NFC อ่าน passport 2. บล. ตรวจสอบข้อมูลบัตรประชาชน online กับกรมการปกครอง 3. บล. เทียบใบหน้าลูกค้ากับข้อมูลหลักฐานและในชิพในบัตรประชาชนหรือ passport 4. บล. ส่ง OTP ไปยังเบอร์โทรศัพท์มือถือลูกค้า
3. Outcomes	รู้ข้อมูลลูกค้า (แต่ยังไม่รู้ว่าเป็นข้อมูลจริงหรือไม่)	1. ลูกค้ามีตัวตนจริง มีเพียงคนเดียว 2. หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง 3. ลูกค้าเป็นเจ้าของหลักฐานที่นำมาแสดง

เปิดบัญชี online (บัตรประชาชน + เงื่อนไขเพิ่มเติม)

	1 ข้อมูล	2 หลักฐาน	3 การบริหารความเสี่ยง
วัตถุประสงค์	**เพื่อรู้ว่าลูกค้าเป็นใคร**	**เพื่อยืนยันข้อมูลที่ลูกค้าแจ้ง+ ดูว่าตัวลูกค้าสอดคล้องกับข้อมูล/หลักฐาน**	
1. การแสดงตน	1. ชื่อ-นามสกุล 2. วัน/เดือน/ปี เกิด 3. เลขบัตรประชาชน 4. ที่อยู่ 5. โทรศัพท์/ อีเมล์ที่ติดต่อได้ 6. ข้อมูลอื่น ๆ เท่าที่จำเป็น	1. รูปถ่ายบัตรประชาชน 2. รูปถ่ายลูกค้า (หลักฐานทุกประเภทชัดเจนเท่าตัวจริง ทั้งหน้า-หลัง)	กำหนดเงื่อนไข เช่น • เปิดบัญชีได้เฉพาะลูกค้าประเภทบัญชี cash balance วงเงินไม่เกิน 5 แสนบาท • หากต้องการเพิ่มวงเงินหรือเพิ่มประเภทบัญชีต้องผ่าน Enhanced KYC ก่อน
2. การตรวจสอบ		**1. บล. ตรวจสอบข้อมูลบัตรประชาชน online กับกรมการปกครอง** 2. บล. เทียบใบหน้าลูกค้ากับรูปถ่ายบนบัตรประชาชน 3. บล. ส่ง OTP ไปยังเบอร์โทรศัพท์มือถือลูกค้า	
3. outcomes	รู้ข้อมูลลูกค้า (แต่ยังไม่รู้ว่าเป็นข้อมูลจริงหรือไม่)	1. ลูกค้ามีตัวตนจริง มีเพียงคนเดียว 2. หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง **3. มีความเสี่ยงที่ลูกค้าจะไม่ได้เป็นเจ้าของหลักฐานที่นำมาแสดง เช่น ปลอมรูปบนหน้าบัตร**	

เปิดบัญชี online (บัตรประชาชน + VDO Conference)

	1 ข้อมูล	2 หลักฐาน	3 การบริหารความเสี่ยง
วัตถุประสงค์	เพื่อรู้ว่าลูกค้าเป็นใคร	เพื่อยืนยันข้อมูลที่ลูกค้าแจ้ง+ ดูว่าตัวลูกค้าสอดคล้องกับข้อมูล/หลักฐาน	บริหารความเสี่ยงที่ลูกค้าจะไม่ใช่เจ้าของหลักฐาน
1. การแสดงตน	1. ชื่อ-นามสกุล 2. วัน/เดือน/ปี เกิด 3. เลขบัตรประชาชน 4. ที่อยู่ 5. โทรศัพท์/ อีเมล์ที่ติดต่อได้ 6. ข้อมูลอื่น ๆ เท่าที่จำเป็น	1. รูปถ่ายบัตรประชาชน 2. รูปถ่ายลูกค้า (หลักฐานทุกประเภทชัดเจนเท่าตัวจริง ทั้งหน้า-หลัง)	**ทำ VDO conference พูดคุยกับลูกค้าเพื่อเพิ่มความมั่นใจในการยืนยันข้อมูลกับหลักฐานและเห็นพฤติกรรมลูกค้า** (ภาพและเสียงชัดเจน)
2. การตรวจสอบ		1. บล. ตรวจสอบข้อมูลบัตรประชาชน online กับกรมการปกครอง 2. บล. เทียบใบหน้าลูกค้ากับรูปถ่ายบนบัตรประชาชน	ให้ลูกค้าแสดงหลักฐานจริงผ่านกล้อง + ให้เจ้าหน้าที่สังเกตพฤติกรรมลูกค้าและรายละเอียดบนบัตรเช่น ลายน้ำ
3. Outcomes	รู้ข้อมูลลูกค้า (แต่ยังไม่รู้ว่าเป็นข้อมูลจริงหรือไม่)	1. ลูกค้ามีตัวตนจริง มีเพียงคนเดียว 2. หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง 3. **มีความเสี่ยงที่ลูกค้าจะไม่ได้เป็นเจ้าของหลักฐานที่นำมาแสดง เช่น ปลอมรูปบนหน้าบัตร**	1. **เพิ่มความมั่นใจว่าลูกค้าเป็นเจ้าของหลักฐาน** 2. **เห็นพฤติกรรมลูกค้าว่าลูกค้ามีลักษณะสอดคล้องกับข้อมูลที่แจ้ง**

เปิดบัญชี online (Passport)

	1 ข้อมูล	2 หลักฐาน
วัตถุประสงค์	เพื่อรู้ว่าลูกค้าเป็นใคร	เพื่อยืนยันข้อมูลที่ลูกค้าแจ้ง+ ดูว่าตัวลูกค้าสอดคล้องกับข้อมูล/หลักฐาน
1. การแสดงตน	1. ชื่อ-นามสกุล 2. วัน/เดือน/ปี เกิด 3. เลขบัตรประชาชน 4. ที่อยู่ 5. โทรศัพท์/ อีเมล์ที่ติดต่อได้ 6. ข้อมูลอื่น ๆ เท่าที่จำเป็น	1. รูปถ่าย passport 2. รูปถ่ายลูกค้า (หลักฐานทุกประเภทชัดเจนเท่าตัวจริง ทั้งหน้า-หลัง)
2. การตรวจสอบ		1. ลูกค้าใช้ NFC อ่านข้อมูลในชิพใน passport 2. **บล. เทียบข้อมูลและใบหน้าลูกค้ากับข้อมูลและรูปถ่ายในชิพใน Passport** 3. บล. ส่ง OTP ไปยังเบอร์โทรศัพท์มือถือ
3. Outcomes	รู้ข้อมูลลูกค้า (แต่ยังไม่รู้ว่าเป็นข้อมูลจริงหรือไม่)	1. ลูกค้ามีตัวตนจริง มีเพียงคนเดียว 2. หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง 3. ลูกค้าเป็นเจ้าของหลักฐานที่นำมาแสดง