



เรียน ผู้จัดการ

ธนาคารพาณิชย์ทุกธนาคาร

ที่ ธพท.ฝกท.ว. ๒๐๕๓ / 2561 เรื่อง การอนุญาตให้ธนาคารพาณิชย์ให้บริการยืนยันตัวตน
ของลูกค้าหรือการให้ข้อมูล ในรูปแบบดิจิทัล

วิวัฒนาการทางด้านเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วและต่อเนื่อง ทำให้ธนาคารพาณิชย์ (ธนาคาร) มีความเชื่อมโยงกับการดำเนินธุรกิจของภาคเอกชนในลักษณะพันธมิตรทางธุรกิจเพิ่มมากขึ้น ทั้งในด้านการให้บริการทางการเงิน การให้ข้อมูลข่าวสาร รวมถึง การใช้ทรัพยากรและความเชี่ยวชาญ ทางด้านการเงินของธนาคารให้เป็นประโยชน์ต่อลูกค้า

นอกจากนี้ เพื่อเป็นการสนับสนุนโครงการการพิสูจน์และยืนยันตัวตนทางดิจิทัล (National Digital ID : NDID) ซึ่งเป็นระบบกลางในการยืนยันตัวตนทางดิจิทัลของประเทศ ธนาคารแห่งประเทศไทย (ธพท.) จึงเห็นควรขยายขอบเขตให้ธนาคารทำหน้าที่ในการยืนยันตัวตนของลูกค้าหรือให้ข้อมูล¹ ในรูปแบบดิจิทัลได้ อย่างไรก็ตาม การให้บริการดังกล่าว เป็นการให้ข้อมูลที่จำเป็นของลูกค้าต่อพันธมิตรทางธุรกิจของธนาคาร ดังนั้น ธนาคารต้องคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคลของลูกค้า การได้รับความยินยอมของลูกค้า รวมทั้งการนำเทคโนโลยีที่เหมาะสมมาใช้เพื่อให้บริการ

ธพท. พิจารณาแล้ว อนุญาตให้ธนาคารที่มีความพร้อมทั้งด้านระบบงาน บุคลากรและ การบริหารความเสี่ยงด้านต่าง ๆ (ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านปฏิบัติการ และความเสี่ยง ด้านกลยุทธ์) สามารถให้บริการดังกล่าวข้างต้นได้เป็นการทั่วไป โดยอาศัยอำนาจตามมาตรา 36 ของ พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และขอให้ธนาคารถือปฏิบัติตามเงื่อนไข ดังนี้

1. ธนาคารต้องได้รับความยินยอมจากลูกค้าผู้เป็นเจ้าของข้อมูล ตามหลักเกณฑ์การขอ ความยินยอม (Consent) ที่สอดคล้องกับกฎหมายและประกาศที่เกี่ยวข้อง ดังนี้

- 1.1 ไม่บังคับ และให้โอกาสเจ้าของข้อมูลเลือกที่จะเปิดเผยข้อมูล (Freely given)
- 1.2 ต้องระบุวัตถุประสงค์ ขอบเขตการนำข้อมูลไปใช้อย่างชัดเจน และเจาะจง (Specific)
- 1.3 แจ้งให้ทราบถึงสิทธิของลูกค้า (Informed) โดยเฉพาะสิทธิในการเข้าถึงข้อมูล (Right to access) สิทธิในการแก้ไขข้อมูล (Right to rectification) สิทธิไม่อนุญาตให้นำข้อมูลไปประมวลผล (Right to restrict data processing) สิทธิในการลบหรือยกเลิกการให้ข้อมูล (Right to be forgotten)
- 1.4 ข้อความที่ระบุในการขอความยินยอมต้องไม่คลุมเครือ (Unambiguous)

2. การนำเทคโนโลยีมาใช้เพื่อให้บริการแก่พันธมิตรทางธุรกิจของธนาคาร ขอให้ธนาคารพัฒนา หรือใช้เทคโนโลยีที่เหมาะสม เพื่อให้สามารถเชื่อมโยงกับผู้ให้บริการรายอื่นในโครงการ NDID ได้ในอนาคต และหากโครงการ NDID เริ่มโครงการ ขอให้ธนาคารพิจารณาเข้าร่วมโครงการดังกล่าวด้วย

¹ เสมือนการทำหน้าที่เป็นผู้พิสูจน์และยืนยันตัวตน (Identity Provider : IDP) หรือผู้ให้ข้อมูลที่น่าเชื่อถือ (Authoritative Source : AS) ตามโครงการ NDID

3. ธนาคารต้องไม่กำหนดเงื่อนไขใด ๆ ทั้งทางตรงและทางอ้อม ในรูปแบบของสัญญาหรือเทคโนโลยีที่ใช้ อันอาจเป็นการจำกัดสิทธิในการเลือกใช้บริการของลูกค้าและพันธมิตรทางธุรกิจของธนาคาร

4. ธนาคารต้องมีระบบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management and Cyber Security) โดยมีกระบวนการประเมินและติดตามความพร้อมใช้งานของระบบและการเชื่อมโยงที่เกี่ยวข้อง เพื่อให้มั่นใจว่าสามารถรองรับการใช้บริการผ่านช่องทางของธนาคารได้อย่างต่อเนื่อง รวมถึงจัดให้มีมาตรการป้องกันและเฝ้าระวังให้มีความมั่นคงปลอดภัย โดยควรมีการประเมินช่องโหว่และทบทวนระบบงานให้ทันสมัยอย่างเป็นประจำ และให้มีการติดตามดูแลเพื่อให้มั่นใจว่าพันธมิตรทางธุรกิจของธนาคารมีการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลของลูกค้าอย่างเหมาะสมและเป็นไปตามมาตรฐานที่ดีตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ



(นายวิโรฒ สันติประภาพ)

ผู้ว่าการ

ฝ่ายกำกับธุรกิจสถาบันการเงิน

โทรศัพท์ 0 2283 6837

โทรสาร 0 2356 7448