สรุปผลการรับฟังความคิดเห็นผู้เกี่ยวข้องต่อร่างประกาศธนาคารแห่งประเทศไทย
เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่

ธนาคารแห่งประเทศไทย (ธปท.) ได้จัดให้มีการรับฟังความคิดเห็นของผู้เกี่ยวข้องเพื่อประกอบการพิจารณาร่างประกาศธนาคารแห่งประเทศไทย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ โดยสรุปผลการรับฟังความคิดเห็นได้ ดังนี้

1. วิธีการ จำนวนครั้ง และระยะเวลาในการรับฟังความคิดเห็น

1.1 การรับฟังความคิดเห็นผ่านทางเว็บไซต์ระบบกลางทางกฎหมาย (www.law.go.th) จำนวน 1 ครั้ง ตั้งแต่วันที่ 2 ธันวาคม 2567 - 31 ธันวาคม 2567

1.2 การรับฟังความคิดเห็นผ่านทางเว็บไซต์ธนาคารแห่งประเทศไทย (www.bot.or.th) จำนวน 1 ครั้ง ตั้งแต่วันที่ 2 ธันวาคม 2567 - 31 ธันวาคม 2567

ทั้งนี้ ข้อมูลประกอบการรับฟังความคิดเห็นและรายละเอียดของประเด็นที่นำไปรับฟังความคิดเห็นของผู้เกี่ยวข้อง ปรากฏตามเอกสารแนบ

2. ผู้เกี่ยวข้องในการรับฟังความคิดเห็น

สถาบันการเงิน สถาบันการเงินเฉพาะกิจ ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับและสมาคมที่เกี่ยวข้อง

3. ผลการพิจารณา

ในการรับฟังความคิดเห็น ผู้ที่แสดงความคิดเห็นได้ร่วมแสดงความคิดเห็นต่อร่างประกาศธนาคารแห่งประเทศไทย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ ซึ่งธนาคารแห่งประเทศไทยได้พิจารณาความเห็นของผู้เกี่ยวข้องต่าง ๆ และได้นำมาประกอบการพิจารณาจัดทำหลักเกณฑ์ดังกล่าว โดยสามารถสรุปความคิดเห็นในแต่ละประเด็นได้ ดังนี้

ประเด็นที่มีการแสดงความคิดเห็น	ผู้ที่แสดงความคิดเห็น	ความคิดเห็น	ผลการพิจารณา
ข้อ 4. ขอบเขตการบังคับใช้	- สถาบันการเงิน - ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ - สมาคมที่เกี่ยวข้อง	เสนอให้ระบุนิยามของ “บริการ Mobile Banking” และ “ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ” ที่เข้าข่ายต้องดำเนินการตามประกาศให้ชัดเจน ว่าครอบคลุม ผู้ให้บริการและแอปพลิเคชันที่ใช้ทำธุรกรรมประเภทใดบ้าง	**ธปท. ปรับนิยามในหลักเกณฑ์ให้ชัดเจน**
ข้อ 7.1.1	- สถาบันการเงิน - สมาคมที่เกี่ยวข้อง	เสนอให้ระบุนิยาม “ลิงก์” ให้ชัดเจน เช่น กรณี QR code หรือข้อความโฆษณาที่มี URL ถือเป็นลิงก์ตามนิยาม ธปท. หรือไม่	**ธปท. ขยายความเพิ่มเติมใน “คำถาม – คำตอบแนบท้ายประกาศ”**
ข้อ 7.1.2	- สถาบันการเงิน - ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ - สมาคมที่เกี่ยวข้อง - องค์กรนิติบุคคล	เสนอให้กำหนดแนวทาง “กระบวนการรับมือแอปพลิเคชันปลอมอย่างทันการณ์” ให้ชัดเจน รวมทั้ง พิจารณาวิธีการดำเนินการติดตามแอปพลิเคชันปลอมกับช่องทางเว็บไซต์และสื่อสังคมออนไลน์ เนื่องจากอาจมีข้อจำกัดในการติดตามในทางปฏิบัติ	**ธปท. ปรับหลักเกณฑ์ให้ชัดเจน และขยายความเพิ่มเติมใน “คำถาม – คำตอบแนบท้ายประกาศ”**
ข้อ 7.1.4	- สถาบันการเงิน	เสนอให้ระบุประเภทธุรกรรมโอนเงินที่เข้าข่ายต้องยืนยันตัวตนผู้ใช้บริการด้วยเทคโนโลยีเปรียบเทียบใบหน้าให้ชัดเจน	**ธปท. ขยายความเพิ่มเติมใน “คำถาม – คำตอบแนบท้ายประกาศ”**
	- สถาบันการเงิน - ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ	เสนอให้ยืดหยุ่นการใช้เทคโนโลยีเปรียบเทียบใบหน้า เช่น - สามารถพิจารณาวิธีการยืนยันตัวตนด้วยเทคโนโลยีอื่นนอกเหนือจากเทคโนโลยีเปรียบเทียบใบหน้า	**ธปท. พิจารณาแล้วยังคงหลักการเดิม** โดยมาตรการที่กำหนดให้ใช้เทคโนโลยีเปรียบเทียบใบหน้าเป็นมาตรการช่วยลดความเสียหายแก่ผู้ใช้บริการที่อาจตกเป็น

		- สามารถเพิ่มวงเงินที่ต้องสแกนใบหน้าได้เกินกว่า 50,000 บาทต่อครั้ง และ 200,000 บาทต่อวัน สำหรับกลุ่มผู้ใช้บริการบางประเภท เช่น ลูกค้ากลุ่มบุคคลธรรมดาเพื่อการค้า - เพิ่มแนวทางในการดำเนินการสำหรับกลุ่มผู้ใช้บริการที่มีข้อจำกัดในการใช้เทคโนโลยีเปรียบเทียบใบหน้า เช่น คนพิการทางสายตา	เหยื่อได้ อย่างไรก็ดี ธปท. มีการปรับให้สถาบันการเงินสามารถพิจารณาแนวทางลดความเสี่ยงอื่นทดแทนได้ในกรณีที่ผู้ใช้บริการมีข้อจำกัดในการใช้เทคโนโลยีดังกล่าว
ข้อ 7.1.5	- สถาบันการเงิน - ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ - สมาคมที่เกี่ยวข้อง	เสนอให้ยกเลิกการกำหนดเพดานวงเงิน และปรับเป็นมาตรการตามระดับความเสี่ยงของกลุ่มผู้ใช้บริการแทน เช่น ตรวจสอบความผิดปกติจากธุรกรรม หรือแจ้งเตือนหรือให้ความรู้ตามระดับความเสี่ยงของกลุ่ม	**<u>ธปท. พิจารณาแล้วยังคงแนวทางเดิม</u>** การกำหนดเพดานวงเงินสูงสุดต่อวันที่เหมาะสมตามระดับความเสี่ยงของผู้ใช้บริการเป็นมาตรการควบคุมที่ช่วยลดความเสียหายของลูกค้าได้
ข้อ 7.2.1	- สถาบันการเงิน - ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ	เสนอให้ระบุให้ชัดเจนว่าข้อมูลลักษณะใดที่ถือเป็น "ข้อมูลสำคัญของผู้ใช้บริการ"	**<u>ธปท. ปรับถ้อยคำในหลักเกณฑ์ให้ชัดเจน</u>**
ข้อ 7.2.2 (2), 7.2.3 (2)	- สถาบันการเงิน	เสนอให้เพิ่มกรอบระยะเวลาให้ผู้ให้บริการดำเนินการปรับปรุงระบบให้แล้วเสร็จกรณี ตรวจพบช่องโหว่ หรือเทคนิค root/jailbreak ใหม่	**<u>ธปท. พิจารณาแล้วยังคงแนวทางเดิม</u>** ผู้ให้บริการมีหน้าที่ต้องติดตามและปรับปรุงการรักษาความมั่นคงปลอดภัยของการให้บริการ Mobile Banking ให้เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริตรูปแบบใหม่อย่างต่อเนื่อง โดยกรณีที่พบช่องโหว่ใหม่ ผู้ให้บริการต้องเร่งดำเนินการให้มีแนวทาง

			ป้องกัน เพื่อปิดช่องโหว่ภายในกรอบเวลาที่เหมาะสม
ข้อ 7.2.3 (1)	- สถาบันการเงิน - สมาคมที่เกี่ยวข้อง	เสนอให้หน่วยงานกลางที่น่าเชื่อถือ เช่น TB-CERT ประกาศเวอร์ชันระบบปฏิบัติการที่ปลอดภัย เพื่อให้ผู้ให้บริการยึดปฏิบัติเป็นมาตรฐานเดียวกัน	**<u>ธปท. ปรับหลักเกณฑ์ให้ชัดเจน</u>**
ข้อ 7.2.3 (3)	- สถาบันการเงิน	เสนอให้ปรับข้อความเป็น ไม่อนุญาตให้ใช้ Mobile Banking ขณะที่มีแอปพลิเคชันอื่นที่มีพฤติกรรมที่มีความเสี่ยงต่อความปลอดภัยของ Mobile Banking กำลังทำงานอยู่	**<u>ธปท. ปรับถ้อยคำในหลักเกณฑ์ให้ชัดเจน</u>**
ข้อ 8. การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์	องค์กรนิติบุคคล	เสนอให้ยกเลิกการขอผ่อนผันการปฏิบัติตามหลักเกณฑ์	**<u>ธปท. พิจารณาแล้วยังคงแนวทางเดิม</u>** กระบวนการขอผ่อนผันเป็นกลไกที่มีความจำเป็นในการกำกับดูแลผู้ให้บริการและลดผลกระทบต่อผู้ใช้บริการในวงกว้าง โดย ธปท. มีกรอบในการพิจารณาซึ่งคำนึงถึงเหตุผลความจำเป็นและข้อเท็จจริงที่เกี่ยวข้อง เช่น ความปลอดภัย ผลกระทบต่อผู้ใช้งาน
ข้อ 9. บทเฉพาะกาล	- สถาบันการเงิน - สมาคมที่เกี่ยวข้อง - องค์กรนิติบุคคล	เสนอให้มีการกำหนดกรอบเวลาดำเนินการปรับปรุงระบบให้เป็นไปตามประกาศอย่างเหมาะสม โดยเสนอให้กำหนดระยะเวลาตั้งแต่ 2-6 เดือน	**<u>ธปท. พิจารณาแล้วยังคงแนวทางเดิม</u>** โดยให้กรอบเวลาดำเนินการปรับปรุงระบบภายใน 30 วัน เนื่องจาก ภัยทุจริตเป็นปัญหาสำคัญเร่งด่วน อย่างไรก็ตาม กรณี มาตรการหลีกเลี่ยงการให้บริการ Mobile Banking บนอุปกรณ์ที่ใช้ระบบปฏิบัติการที่มีความเสี่ยงกำหนดให้ดำเนินการภายใน 60 วัน ทั้งนี้

			เพื่อให้สถาบันการเงินมีระยะเวลาในการสื่อสารและแจ้งเตือนไปยังลูกค้า เนื่องจากเป็นมาตรการที่ส่งผลกระทบต่อลูกค้าโดยตรง
อื่น ๆ	องค์กรนิติบุคคล	เสนอให้เพิ่มข้อความใน SMS OTP แจ้งเตือนไม่ให้แชร์รหัส OTP ให้บุคคลอื่น	**<u>ธปท. จะนำความเห็นไปพิจารณาประกอบการกำหนดมาตรการที่เกี่ยวข้องในการป้องกันภัยทุจริตต่อไป</u>**
	องค์กรนิติบุคคล	เสนอให้เพิ่มข้อ 7.1.6 เมื่อผู้ใช้บริการเปลี่ยนอุปกรณ์ใหม่ หรือดาวน์โหลดแอปพลิเคชันใหม่ ควรมีวิธีการชะลอการใช้งาน เช่น การยืนยันตัวตนผ่านเคาเตอร์ หรือเว้นระยะในการใช้บริการอย่างน้อย 12 ชั่วโมง เป็นต้น	
	องค์กรนิติบุคคล	เสนอให้เพิ่มมาตรการหน่วงการโอนเงินจำนวน 10,000 บาทขึ้นไปเป็นเวลาอย่างน้อย 24 ชั่วโมง และแจ้งเตือนโดยทันทีที่มีการโอนเงินเกิน 10,000 บาท หรือเมื่อเกิดธุรกรรมทางการเงินที่มีความเสี่ยงสูง	
	องค์กรนิติบุคคล	เสนอให้เพิ่มมาตรการเยียวยาความเสียหายให้แก่ผู้ใช้บริการ ในกรณีที่ผู้ให้บริการไม่สามารถปฏิบัติตามประกาศของ ธปท. หรือบกพร่องในหน้าที่	