ประกาศธนาคารแห่งประเทศไทย

ที่ ๔/๒๕๖๘

เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงิน

๑. เหตุผลในการออกประกาศ

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) มีบทบาทสำคัญสำหรับการดำเนินธุรกิจของสถาบันการเงิน โดยเฉพาะการให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันของสถาบันการเงินแก่ผู้ใช้บริการที่เป็นบุคคลธรรมดาบนอุปกรณ์เคลื่อนที่ (บริการ Mobile Banking) ที่มีการใช้งานเพิ่มขึ้นอย่างรวดเร็ว และยังคงขยายตัวอย่างต่อเนื่อง ขณะเดียวกันการให้บริการ Mobile Banking ก็นำมาซึ่งความเสี่ยงจากภัยคุกคามทางไซเบอร์ (cyber threat) และภัยทุจริตทางการเงิน (fraud) ที่มีการปรับเปลี่ยนรูปแบบและใช้เทคนิควิธีการที่ซับซ้อนมากขึ้น อันอาจสร้างความเสียหายต่อผู้ใช้บริการในวงกว้าง ส่งผลกระทบต่อความน่าเชื่อถือของระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

ธนาคารแห่งประเทศไทยตระหนักถึงความสำคัญในการป้องกันภัยทุจริตดังกล่าว จึงได้ออกประกาศหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ เพื่อยกระดับการให้บริการ Mobile Banking ให้มีมาตรฐานขั้นต่ำที่จำเป็นสำหรับการให้บริการทางการเงินและการชำระเงินบนแอปพลิเคชันของสถาบันการเงินให้เป็นไปอย่างปลอดภัย เท่าทันความเสี่ยงจากภัยคุกคามทางไซเบอร์และภัยทุจริตทางการเงินที่มีการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (Unauthorized Payment Fraud)

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา ๓๙ และมาตรา ๔๑ แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

๓. แนวนโยบายที่ยกเลิก

๓.๑ แนวนโยบาย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ตามหนังสือเวียนธนาคารแห่งประเทศไทย ที่ ธปท.ฝตท.(๐๑) ว. ๑๙๒๒/๒๕๖๒ ลงวันที่ ๒๗ ธันวาคม ๒๕๖๒

๓.๒ ข้อ ๑.๒ ข้อ ๑.๔ และข้อ ๑.๖ ในเอกสารแนบ ๒ ของแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ฉบับลงวันที่ ๒๙ มีนาคม ๒๕๖๖

๔. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

๕. เนื้อหา

๕.๑ คำจำกัดความ

ในประกาศฉบับนี้

“อุปกรณ์เคลื่อนที่” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์แบบพกพาซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่น เพื่อรับหรือส่งข้อมูลทางการเงิน การชำระเงิน หรือคำสั่งการชำระเงินผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง

“สถาบันการเงิน” หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“ผู้ใช้บริการ” หมายความว่า บุคคลธรรมดาที่ใช้บริการทางการเงินและการชำระเงินผ่านบริการ Mobile Banking บนอุปกรณ์เคลื่อนที่

“บริการ Mobile Banking” หมายความว่า การให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันของสถาบันการเงินที่มีการให้บริการแก่ผู้ใช้บริการบนอุปกรณ์เคลื่อนที่ ซึ่งให้บริการถอนเงิน โอนเงิน หรือการชำระค่าสินค้าและบริการ อย่างใดอย่างหนึ่ง

“การสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (Unauthorized Payment Fraud)” หมายถึง ภัยทุจริตทางการเงินที่เกิดขึ้นจากการที่ผู้อื่นสวมรอยทำธุรกรรมแทนผู้ใช้บริการโดยทุจริต โดยที่ผู้ใช้บริการไม่ได้ให้ความยินยอม เช่น กรณีผู้ไม่ประสงค์ดีติดตั้ง malware บนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ ทำให้สามารถเข้าถึงหรือควบคุมอุปกรณ์เคลื่อนที่และแอปพลิเคชัน และสวมรอยทำธุรกรรมผ่านบัญชีของผู้ใช้บริการโดยไม่ได้รับอนุญาต

๕.๒ หลักการ

สถาบันการเงินที่ให้บริการ Mobile Banking บนอุปกรณ์เคลื่อนที่มีหน้าที่ต้องติดตาม ดูแลและปรับปรุงระบบงานและบริการ Mobile Banking ให้มีความมั่นคงปลอดภัยตามมาตรฐานสากล เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริตรูปแบบใหม่ที่มีเทคนิคซับซ้อนขึ้น ครอบคลุมทั้งในส่วนของระบบการให้บริการของสถาบันการเงิน และความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ

๕.๓ หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่

หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ ประกอบด้วยมาตรการ ๒ ส่วน ได้แก่ (๑) การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (Unauthorized Payment Fraud) และ (๒) การรักษาความมั่นคงปลอดภัยของบริการ Mobile Banking ดังนี้

๕.๓.๑ การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ

สถาบันการเงินต้องมีการป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ โดยอย่างน้อยต้องดำเนินการ ดังต่อไปนี้

(๑) งดเว้นการแนบลิงก์ผ่านช่องทางข้อความสั้น (SMS) และช่องทางอีเมล แต่สำหรับกรณีช่องทางสื่อสังคมออนไลน์ (social media) ให้สถาบันการเงินงดแนบลิงก์เฉพาะที่มีการขอข้อมูลในการยืนยันตัวตน หรือข้อมูลส่วนบุคคล เช่น ชื่อผู้ใช้งาน รหัสผ่าน รหัสใช้ครั้งเดียว (one time password - OTP) รหัส PIN หมายเลขบัตรประชาชนชน วันเดือนปีเกิด เพื่อป้องกันการสวมรอยเป็นสถาบันการเงิน การขอให้เปิดเผยข้อมูลสำคัญ (social engineering) หรือการถูกติดตั้ง mobile malware

อย่างไรก็ดี สถาบันการเงินสามารถแนบลิงก์ผ่านทั้ง ๓ ช่องทางดังกล่าวได้ หากผู้ใช้บริการดำเนินการร้องขอเอง โดยสถาบันการเงินสามารถแนบลิงก์ได้เป็นรายครั้ง พร้อมทั้งต้องมีการสื่อสารย้ำให้ผู้ใช้บริการทราบว่าการส่งลิงก์ดังกล่าวเป็นกรณีเฉพาะตามคำร้องขอของผู้ใช้บริการเป็นรายครั้งเท่านั้น

(๒) มีกระบวนการติดตามและรับมืออย่างทันการณ์ต่อแอปพลิเคชันที่ปลอมแปลงหรือแอบอ้างเป็นแอปพลิเคชันของสถาบันการเงินที่ให้บริการ Mobile Banking ในแพลตฟอร์มที่เป็นทางการของผู้ให้บริการดาวน์โหลดแอปพลิเคชัน (official app store) เช่น Google Play Store Apple App Store รวมทั้งมีกระบวนการรับมือและตอบสนองอย่างเหมาะสมและทันการณ์สำหรับแอปพลิเคชันปลอมแปลงที่อยู่นอกแพลตฟอร์มดังกล่าว เพื่อลดความเสี่ยงที่ผู้ใช้บริการจะหลงเชื่อและเปิดเผยข้อมูลสำคัญ ถูกติดตั้ง malware หรือถูกติดตั้งแอปพลิเคชันปลอม

(๓) จำกัดการใช้บริการ Mobile Banking ของผู้ใช้บริการไว้เพียง ๑ บัญชีผู้ใช้งานต่อ ๑ บริการ Mobile Banking ของแต่ละสถาบันการเงิน และจำกัดการใช้บริการดังกล่าวโดยให้ใช้งานบน ๑ อุปกรณ์เคลื่อนที่ของผู้ใช้บริการเท่านั้น

(๔) ต้องจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้บริการเพิ่มเติมในขั้นตอนการทำธุรกรรมผ่านบริการ Mobile Banking บนอุปกรณ์เคลื่อนที่ โดยใช้เทคโนโลยีเปรียบเทียบใบหน้า (face comparison) ร่วมกับการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) ที่สามารถป้องกันการใช้รูปภาพ วิดีโอ หรือการปลอมแปลงชีวมิติในรูปแบบต่าง ๆ ได้ เช่น การใช้เทคโนโลยี liveness detection เพื่อให้มั่นใจว่าผู้ใช้บริการเป็นผู้ทำธุรกรรมด้วยตนเอง ซึ่งต้องจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้บริการเพิ่มเติมดังกล่าวอย่างน้อยในกรณี ดังต่อไปนี้

(๔.๑) การทำธุรกรรมโอนเงินในแต่ละครั้งมีมูลค่าตั้งแต่ ๕๐,๐๐๐ บาทขึ้นไป หรือ

(๔.๒) การทำธุรกรรมโอนเงินมูลค่ารวมกัน ครบทุก ๒๐๐,๐๐๐ บาทในรอบระยะเวลา ๑ วัน หรือ

(๔.๓) การปรับเพิ่มวงเงินการทำธุรกรรมโอนเงินต่อวัน ให้สามารถโอนได้ตั้งแต่ ๕๐,๐๐๐ บาทขึ้นไป

ทั้งนี้ กรณีที่ผู้ใช้บริการมีข้อจำกัดในการใช้เทคโนโลยีเปรียบเทียบใบหน้า (face comparison) เช่น เป็นคนพิการทางสายตา สถาบันการเงินอาจพิจารณางดเว้นการยืนยันตัวตนเพิ่มเติมตามที่กำหนดข้างต้นได้ โดยต้องมีแนวทางลดความเสี่ยงทดแทน หรือกรณีการทำธุรกรรมที่มีความเสี่ยงต่ำ เช่น การทำธุรกรรมโอนเงินระหว่างบัญชีตนเอง การทำธุรกรรมโอนเงินประจำอัตโนมัติ (automatic recurring transfer) ที่ได้ยืนยันตัวตนไปแล้วในครั้งแรก สถาบันการเงินอาจพิจารณางดเว้นการยืนยันตัวตนเพิ่มเติมตามที่กำหนดข้างต้นได้

(๕) กำหนดเพดานวงเงินสูงสุดต่อวันสำหรับธุรกรรมถอนเงินหรือโอนเงินผ่านบริการ Mobile Banking ให้เหมาะสมกับระดับความเสี่ยงของกลุ่มผู้ใช้บริการ เพื่อลดความเสียหายเมื่อผู้ใช้บริการตกเป็นเหยื่อ หรือถูกใช้เป็นเครื่องมือในการทุจริต เช่น กรณีกลุ่มผู้ใช้บริการที่อายุต่ำกว่า ๑๕ ปี ให้กำหนดวงเงินสูงสุดของการทำธุรกรรมถอนหรือโอนเงินรวมกันไม่เกิน ๕๐,๐๐๐ บาทต่อวัน เป็นต้น

ทั้งนี้ สถาบันการเงินสามารถใช้แนวทางหรือข้อกำหนดที่ได้จัดทำร่วมกัน (industry standard) มาใช้ประกอบการจัดระดับความเสี่ยง หรือกำหนดเพดานวงเงินสูงสุดของกลุ่มผู้ใช้บริการได้ และในกรณีที่ผู้ใช้บริการขอยกเว้นการกำหนดวงเงินตามกลุ่มความเสี่ยงที่กำหนดไว้ สถาบันการเงินต้องมีกระบวนการพิจารณาการขอยกเว้นที่ชัดเจนและรัดกุมด้วย

๕.๓.๒ การรักษาความมั่นคงปลอดภัยของบริการ Mobile Banking

สถาบันการเงินต้องกำหนดให้มีการรักษาความมั่นคงปลอดภัยแอปพลิเคชันที่ให้บริการ Mobile Banking ภายใต้กรอบหลักการที่สำคัญ คือ (๑) การรักษาความมั่นคงปลอดภัยของข้อมูล (๒) การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน และ (๓) การรักษาความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่ เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์และภัยทุจริตทางการเงินที่ส่งผลกระทบต่อผู้ใช้บริการและความเชื่อมั่นต่อระบบสถาบันการเงิน ดังนี้

(๑) การรักษาความมั่นคงปลอดภัยของข้อมูล

สถาบันการเงินต้องรักษาความลับและความปลอดภัยของข้อมูลสำคัญของผู้ใช้บริการอย่างรัดกุม เพื่อป้องกันข้อมูลสำคัญของผู้ใช้บริการรั่วไหล หรือถูกเปลี่ยนแปลงแก้ไขทั้งขณะจัดเก็บ แสดงผล และรับ - ส่งข้อมูลระหว่างอุปกรณ์เคลื่อนที่ของผู้ใช้บริการและระบบงานของสถาบันการเงิน โดยต้องดำเนินการอย่างน้อย ดังนี้

(๑.๑) หลีกเลี่ยงการจัดเก็บข้อมูลสำคัญไว้ในอุปกรณ์เคลื่อนที่ เช่น ข้อมูลที่ใช้ยืนยันตัวตน ข้อมูลส่วนบุคคล โดยหากจำเป็นต้องจัดเก็บข้อมูลดังกล่าว ต้องมีกระบวนการรักษาความปลอดภัยที่รัดกุม โดยอย่างน้อยสถาบันการเงินต้องเข้ารหัสข้อมูล (data encryption) ด้วยวิธีการที่ปลอดภัยตามมาตรฐานสากล และทำลายข้อมูลเมื่อสิ้นสุดการใช้งานข้อมูล

(๑.๒) แอปพลิเคชันของสถาบันการเงินต้องแสดงผลข้อมูลสำคัญ (sensitive information) ของผู้ใช้บริการเท่าที่จำเป็นและเป็นไปอย่างรัดกุม โดยอย่างน้อยต้องปิดบังการแสดงข้อมูลรหัสผ่าน และปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (application blurring)

(๑.๓) ใช้ช่องทางสื่อสารที่ปลอดภัย (secure protocol) และยืนยันตัวตนด้วยเทคนิค certificate pinning หรือวิธีอื่นที่เทียบเท่า รวมทั้งต้องดำเนินการเข้ารหัสข้อมูลสำคัญในระดับแอปพลิเคชัน (application layer) ในการรับ - ส่งข้อมูล เพื่อป้องกันการถูกดักจับหรือแก้ไขเปลี่ยนแปลงข้อมูลระหว่างการรับส่ง (man in the middle attack)

(๒) การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน

สถาบันการเงินต้องติดตามดูแลและปรับปรุงแอปพลิเคชันให้มีความมั่นคงปลอดภัยตามมาตรฐานสากลและเท่าทันภัยคุกคามรูปแบบใหม่อยู่เสมอ โดยต้องดำเนินการอย่างน้อย ดังนี้

(๒.๑) แอปพลิเคชันของสถาบันการเงินต้องขอสิทธิเข้าถึงทรัพยากรหรือบริการบนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ (application permission) เท่าที่จำเป็น และมีการทบทวนการขอสิทธิดังกล่าวทุกครั้งที่มีการเปลี่ยนแปลงแอปพลิเคชันอย่างมีนัยสำคัญ เพื่อป้องกันการละเมิดสิทธิความเป็นส่วนตัวของผู้ใช้บริการ รวมถึงเป็นช่องโหว่ที่อาจถูกใช้โดยผู้อื่นที่กระทำการโดยทุจริต

(๒.๒) ไม่ให้บริการบนแอปพลิเคชันเวอร์ชันเก่าที่อาจมีช่องโหว่และอาจทำให้เกิดความเสี่ยงในการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ

(๒.๓) ตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชันทุกครั้งในทันทีที่ผู้ใช้บริการเข้าใช้งาน (anti-tampering) และไม่อนุญาตให้ผู้ใช้บริการใช้งานแอปพลิเคชันที่ถูกเปลี่ยนแปลงแก้ไข เพื่อป้องกันไม่ให้ข้อมูลผู้ใช้บริการรั่วไหลหรือเกิดความเสียหายจากแอปพลิเคชันที่มีการดัดแปลงแก้ไข เช่น การฝัง malicious code

(๒.๔) จัดการการเชื่อมต่อระหว่างคอมพิวเตอร์ (session) ให้ปลอดภัยเพื่อป้องกันการสวมรอยเข้าใช้งานโดยไม่ได้รับอนุญาต (session hijacking)

(๒.๕) ป้องกัน source code ของแอปพลิเคชันไม่ให้อยู่ในรูปแบบที่อ่านเข้าใจโดยง่าย เช่น การทำ source code obfuscation เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงและทำการเปลี่ยนแปลงแก้ไข source code ได้

(๓) การรักษาความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่

สถาบันการเงินต้องให้บริการ Mobile Banking ในสภาพแวดล้อมของอุปกรณ์เคลื่อนที่ที่ปลอดภัย เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีกระทำการทุจริตโดยอาศัยช่องโหว่ของระบบปฏิบัติการเข้าถึง Mobile Banking และบัญชีของผู้ใช้บริการ โดยต้องดำเนินการอย่างน้อยดังนี้

(๓.๑) ไม่อนุญาตให้แอปพลิเคชันของสถาบันการเงินใช้งานบนอุปกรณ์เคลื่อนที่ที่ตรวจพบว่ามีการเปิดสิทธิให้เข้าถึงระบบปฏิบัติการ (rooted/jailbroken)

(๓.๒) ไม่อนุญาตให้แอปพลิเคชันของสถาบันการเงินทำงานบนอุปกรณ์เคลื่อนที่ในขณะที่มีแอปพลิเคชันอื่นกำลังทำงานและมีพฤติกรรมการทำงานที่เสี่ยงจะก่อให้เกิดการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ เช่น แอปพลิเคชันที่ขอสิทธิช่วยเหลือคนพิการ (accessibility services) โดยไม่จำเป็น แอปพลิเคชันที่สามารถควบคุมอุปกรณ์เคลื่อนที่จากระยะไกลได้ (remote control) แอปพลิเคชันที่มีการปิดบังหรือขโมยข้อมูลที่แสดงบนหน้าจอของผู้ใช้งาน เพื่อลดความเสี่ยงที่แอปพลิเคชันของสถาบันการเงินจะถูกควบคุมหรือเข้าถึงโดย malware ที่มีการติดตั้งบนอุปกรณ์เคลื่อนที่

(๓.๓) หลีกเลี่ยงการให้บริการ Mobile Banking ของสถาบันการเงินบนอุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการที่หน่วยงานด้านความมั่นคงปลอดภัยที่เป็นที่ยอมรับ เช่น Thailand Banking Sector Computer Emergency Response Team (TB-CERT) กำหนดว่ามีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ หรือการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ

กรณีสถาบันการเงินมีการให้บริการบนอุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ หรือการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ สถาบันการเงินต้องจัดให้มีแนวทางการควบคุมความเสี่ยงเพิ่มเติม โดยการแจ้งเตือนถึงความเสี่ยงจากกรณีดังกล่าว รวมทั้งจำกัดวงเงินการทำธุรกรรมของกลุ่มผู้ใช้บริการดังกล่าวให้ทำธุรกรรมโอนเงินได้ไม่เกินวันละ ๕,๐๐๐ บาท

ทั้งนี้ สถาบันการเงินต้องติดตามและปรับปรุงการรักษาความมั่นคงปลอดภัยของการให้บริการ Mobile Banking ให้เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริตรูปแบบใหม่เป็นไปตามมาตรฐานสากลอย่างต่อเนื่อง โดยกรณีที่พบช่องโหว่ใหม่ สถาบันการเงินต้องเร่งดำเนินการให้มีแนวทางป้องกัน เพื่อปิดช่องโหว่ภายในกรอบเวลาที่เหมาะสม หรือดำเนินการให้แล้วเสร็จภายในระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด

๕.๔ การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

กรณีที่สถาบันการเงินมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ได้ ให้ยื่นขอผ่อนผันเป็นรายกรณีต่อธนาคารแห่งประเทศไทยพร้อมแสดงเหตุผลความจำเป็นและแผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน ๓๐ วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดยธนาคารแห่งประเทศไทยอาจกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

๖. บทเฉพาะกาล

กรณีที่สถาบันการเงินมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้อยู่ก่อนที่ประกาศฉบับนี้ใช้บังคับ และประสงค์จะขอผ่อนผันการปฏิบัติ

ตามหลักเกณฑ์ดังกล่าว ให้สถาบันการเงินยื่นคำขอผ่อนผันตามหลักเกณฑ์ข้อ ๕.๔ ภายใน ๗ วัน นับแต่วันที่ประกาศฉบับนี้มีผลใช้บังคับ โดยให้ถือว่าการปฏิบัติในระหว่างระยะเวลาการขอผ่อนผันและการพิจารณาผ่อนผันของ ธปท. ดังกล่าวไม่เป็นการฝ่าฝืนหลักเกณฑ์ของประกาศนี้

๗. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่กรณีตามข้อ ๕.๓.๒ (๓.๓) ให้ใช้บังคับเมื่อพ้นกำหนดหกสิบวันนับแต่วันถัดจากประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๑ มกราคม พ.ศ. ๒๕๖๘
เศรษฐพุฒิ สุทธิวาทนฤพุฒิ
ผู้ว่าการ
ธนาคารแห่งประเทศไทย