ประกาศธนาคารแห่งประเทศไทย

ที่ ๔๗/๒๕๖๙

เรื่อง หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการ
เครื่อง White-label Smart Machine

๑. เหตุผลในการออกประกาศ

ปัจจุบันภัยคุกคามทางไซเบอร์มีรูปแบบหลากหลาย ซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ซึ่งบริการเครื่อง White-label Smart Machine เป็นหนึ่งในช่องทางการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์แก่ประชาชนที่อาจมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ได้ หากผู้ประกอบธุรกิจการให้บริการเครื่อง White-label Smart Machine ไม่มีการรักษาความปลอดภัยของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine ตลอดทั้งกระบวนการอย่างรัดกุมเพียงพอ อาจทำให้ระบบการให้บริการมีช่องโหว่ต่อการถูกโจมตีทางไซเบอร์และส่งผลเสียหายต่อการใช้บริการและการทำธุรกรรมทางการเงินของประชาชน รวมถึงอาจส่งผลกระทบต่อชื่อเสียงและความเชื่อมั่นของระบบการชำระเงินของประเทศได้

ธนาคารแห่งประเทศไทยจึงออกหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการเครื่อง White-label Smart Machine เพื่อให้ผู้ประกอบธุรกิจที่ให้บริการเครื่อง White-label Smart Machine ถือปฏิบัติเพิ่มเติมนอกเหนือจากการปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา ๒๔ แห่งพระราชบัญญัติระบบการชำระเงิน พ.ศ. ๒๕๖๐ ธนาคารแห่งประเทศไทยกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการเครื่อง White-label Smart Machine ตามความในประกาศฉบับนี้

๓. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ประกอบธุรกิจการให้บริการเครื่อง White-label Smart Machine ตามกฎหมายว่าด้วยระบบการชำระเงิน

๔. เนื้อหา

๔.๑ คำจำกัดความ

ในประกาศฉบับนี้

“ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจที่ได้รับอนุญาตให้ประกอบธุรกิจการให้บริการเครื่อง White-label Smart Machine ตามกฎหมายว่าด้วยระบบการชำระเงิน

“เครื่อง White-label Smart Machine” หมายความว่า เครื่องอิเล็กทรอนิกส์ที่ใช้สำหรับฝากเงิน ถอนเงิน หรือถามยอดเงินคงเหลือ กับธนาคารพาณิชย์หรือสถาบันการเงินเฉพาะกิจ ซึ่งมีการเชื่อมต่อกับระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ (Inter-institution Fund Transfer System) ไม่ว่าโดยทางตรงหรือทางอ้อม ทั้งนี้ ไม่รวมถึงเครื่องอิเล็กทรอนิกส์ที่ให้บริการภายใต้ชื่อ เครื่องหมาย หรือสัญลักษณ์ของธนาคารพาณิชย์หรือสถาบันการเงินเฉพาะกิจ

“เครื่องอิเล็กทรอนิกส์” หมายความว่า ตู้หรือเครื่องสำหรับฝากเงิน ถอนเงิน หรือถามยอดเงินคงเหลือ ที่ผู้ใช้บริการสามารถดำเนินการได้ด้วยตนเองโดยอัตโนมัติ เช่น เครื่องถอนเงินสดอัตโนมัติ (Automatic Teller Machine: ATM) เครื่องฝากเงินสดอัตโนมัติ (Cash Deposit Machine: CDM) เครื่องฝากและถอนเงินสดอัตโนมัติ (Cash Recycling Machine: CRM)

“ระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ” (Inter-institution Fund Transfer System) หมายความว่า ระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบตามประกาศกระทรวงการคลังว่าด้วยการกำหนดระบบการชำระเงินภายใต้การกำกับ

“เทคโนโลยีสารสนเทศ” (Information Technology: IT) หมายความว่า เทคโนโลยีสารสนเทศที่นำมาใช้ในการให้บริการหรือดำเนินธุรกิจ ซึ่งครอบคลุมถึง ข้อมูล ระบบปฏิบัติการ (operating system) ระบบงาน (application system) ระบบฐานข้อมูล (database system) อุปกรณ์คอมพิวเตอร์ (computer hardware) และระบบเครือข่ายสื่อสาร (communication) เป็นต้น

“ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (Information Technology Risk: IT risk) หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของผู้ประกอบธุรกิจ รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threats)

“ระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine” หมายความว่า ระบบและองค์ประกอบด้านเทคโนโลยีสารสนเทศทั้งหมดที่ใช้ประกอบรวมกันสำหรับการให้บริการเครื่อง White-label Smart Machine เช่น ระบบเครือข่ายสื่อสาร อุปกรณ์รักษาความมั่นคงปลอดภัยเครื่องอิเล็กทรอนิกส์ อุปกรณ์เครือข่ายสื่อสาร ระบบประมวลผลกลาง และซอฟต์แวร์ที่เกี่ยวข้อง

“ธปท.” หมายความว่า ธนาคารแห่งประเทศไทยตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

๔.๒ หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine

ผู้ประกอบธุรกิจต้องปฏิบัติตามประกาศ ธปท. ว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงินและต้องปฏิบัติตามหลักเกณฑ์ในประกาศฉบับนี้เพิ่มเติมด้วย โดยต้องจัดให้มีนโยบาย มาตรฐาน หรือระเบียบวิธีปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine และต้องมีการกำกับดูแลให้มีการปฏิบัติที่เป็นไปตามนโยบาย มาตรฐาน หรือระเบียบวิธีปฏิบัติดังกล่าว โดยอย่างน้อยต้องครอบคลุม ดังนี้

(๑) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (network security)

จัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine และข้อมูลที่รับส่งผ่านระบบดังกล่าว เพื่อป้องกันการบุกรุกหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น และสามารถรองรับการให้บริการได้อย่างต่อเนื่อง โดยอย่างน้อยต้องดำเนินการ ดังนี้

(๑.๑) ออกแบบระบบเครือข่ายสื่อสารของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine ให้มีความมั่นคงปลอดภัย ซึ่งรวมถึงการแบ่งแยกระบบเครือข่ายสื่อสารของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine ออกจากระบบเครือข่ายสื่อสารอื่น

(๑.๒) จัดให้มีอุปกรณ์รักษาความมั่นคงปลอดภัย เช่น firewall, intrusion detection system, intrusion prevention system

(๑.๓) การเชื่อมต่อมายังระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine ต้องกระทำผ่านช่องทางและวิธีการที่มีความปลอดภัย และสามารถป้องกันภัยคุกคามทางไซเบอร์ เช่น IP spoofing, man-in-the-middle attack

(๒) การควบคุมการเข้าถึง (access control)

จัดให้มีการควบคุมการเข้าถึงระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine อย่างรัดกุม เช่น BIOS ของเครื่อง White-label Smart Machine ระบบปฏิบัติการ (operating system) ระบบงาน (application) ตลอดจนอุปกรณ์เครือข่ายสื่อสาร และอุปกรณ์รักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงระบบ เครื่องมือ อุปกรณ์ หรือข้อมูลโดยมิชอบ โดยอย่างน้อยต้องดำเนินการ ดังนี้

(๒.๑) บริหารจัดการสิทธิการเข้าถึงและตรวจสอบการยืนยันตัวตนตามสิทธิที่กำหนดไว้ โดยให้สอดคล้องกับหลักการให้สิทธิตามความจำเป็น (least privilege) รวมทั้งมีการทบทวนและปรับปรุงสิทธิอย่างสม่ำเสมอ และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๒.๒) จัดให้มีกระบวนการควบคุม จัดเก็บ และเบิกใช้งานรหัสผ่านสำหรับการเข้าถึงอย่างรัดกุม

(๒.๓) จัดให้มีการระบุตัวตนและพิสูจน์ตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับการเข้าถึงด้วยบัญชีผู้ใช้งานที่มีสิทธิสูง (privilege user) หรือการเข้าถึงจากเครือข่ายระยะไกล (remote access) ทั้งนี้ กรณีที่ไม่สามารถจัดให้มีการดำเนินการดังกล่าวได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีการขออนุมัติยกเว้นกับผู้ที่มีอำนาจของผู้ประกอบธุรกิจ รวมทั้งต้องดำเนินการประเมินความเสี่ยง และจัดให้มีการควบคุมความเสี่ยงอย่างเพียงพอและเหมาะสม

(๓) การบริหารจัดการการตั้งค่าระบบ (system configuration management)

จัดให้มีการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) ของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine

อย่างชัดเจนเป็นลายลักษณ์อักษร และตั้งค่าการรักษาความมั่นคงปลอดภัยของระบบดังกล่าวให้สอดคล้องกับมาตรฐานที่กำหนด (security hardening) เพื่อให้มั่นใจว่าระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine มีการรักษาความมั่นคงปลอดภัยตามมาตรฐานที่กำหนด เช่น การตั้งค่าการอัปเดต BIOS ของเครื่อง White-label Smart Machine ให้มีความปลอดภัย การตั้งค่าให้มีการป้องกันการบูต (boot) ของระบบปฏิบัติการจากอุปกรณ์ที่ไม่ได้รับอนุญาต การปิดการใช้งาน (disable) หรือลบโปรแกรมหรือบริการที่ไม่ได้ใช้งาน การตั้งค่าให้มีการคัดกรองการติดต่อสื่อสารและการเชื่อมต่อที่ไม่ได้รับอนุญาต และการตั้งค่าให้มีการป้องกันการขโมยข้อมูลสำคัญจากหน่วยความจำ

(๔) การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสอดคล้องตามระดับชั้นความลับของข้อมูล ครอบคลุมข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data-in-transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data-at-rest) โดยอย่างน้อยต้องมีการเข้ารหัสฮาร์ดดิสก์ (hard disk) ของเครื่อง White-label Smart Machine และเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลที่ใช้ในการยืนยันตัวตนผู้ใช้บริการ ด้วยมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป รวมทั้งมีกระบวนการบริหารจัดการกุญแจเข้ารหัสข้อมูลอย่างรัดกุม เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูลสำคัญ

(๕) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring)

จัดให้มีการตรวจจับและแจ้งเตือนอย่างทันการณ์ เมื่อระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine มีความผิดปกติ เช่น การรีบูตในลักษณะที่ไม่ได้วางแผนไว้ล่วงหน้า (unplanned reboot) การถูกติดตั้งโปรแกรมแปลกปลอม และการถูกโจมตีทางเครือข่ายสื่อสาร (network attack) เพื่อให้สามารถรับมือเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ได้อย่างทันการณ์

(๖) การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration testing)

จัดให้มีการประเมินช่องโหว่ (vulnerability assessment) ของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งจัดให้มีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระอย่างน้อยครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (internet facing) อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อลดความเสี่ยงที่ช่องโหว่ของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine อาจเป็นช่องทางของการถูกโจมตีทางไซเบอร์ นอกจากนี้ ต้องจัดให้มีกระบวนการบริหารจัดการเพื่อแก้ไขช่องโหว่ที่พบอย่างเหมาะสมตามระดับความเสี่ยง เช่น การติดตั้งชุดซอฟต์แวร์สำหรับแก้ไขช่องโหว่ (patch) ที่เป็นปัจจุบัน การปรับการตั้งค่าระบบให้ปลอดภัยมากยิ่งขึ้น การปรับปรุงระบบปฏิบัติการให้ทันสมัย

(๗) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

จัดเก็บและสอบทานข้อมูลบันทึกเหตุการณ์ของระบบที่รองรับการให้บริการเครื่อง White-label Smart Machine เช่น บันทึกการเข้าถึงระบบ (access log) และบันทึกการดำเนินงาน (activity log) รวมทั้งเก็บข้อมูลดังกล่าวอย่างปลอดภัย เพื่อให้มีข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอสามารถใช้ติดตามและตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูล รวมทั้งสามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์

(๘) การรักษาความมั่นคงปลอดภัยของเครื่อง White-label Smart Machine

จัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่อง White-label Smart Machine รวมถึงอุปกรณ์เครือข่ายสื่อสาร เช่น router โดยอย่างน้อยต้องดำเนินการ ดังนี้

(๘.๑) ป้องกันการเข้าถึงเครื่อง White-label Smart Machine และอุปกรณ์เครือข่ายสื่อสาร ด้วยวิธีการที่เหมาะสม เพื่อป้องกันการเข้าถึงโดยมิชอบ เช่น การปิดการใช้งานพอร์ต (port) สำหรับการเชื่อมต่ออุปกรณ์ที่ไม่ได้ใช้งาน การควบคุมการใช้งานในระดับพอร์ต (port security) และการยืนยันความถูกต้องในการเชื่อมต่อระหว่างส่วนที่เป็นเครื่องจ่ายและเก็บเงินสดกับเครื่อง White-label Smart Machine (pairing authentication) เพื่อป้องกันการจ่ายเงินสดโดยไม่ได้รับอนุญาต

(๘.๒) ควบคุมการติดตั้งโปรแกรมที่เครื่อง White-label Smart Machine ด้วยวิธีการที่เหมาะสม เพื่อป้องกันความเสี่ยงจากการถูกติดตั้งโปรแกรมที่ไม่พึงประสงค์ (malware) เช่น การติดตั้งโปรแกรมป้องกันไวรัส (anti-virus) และ malware (anti-malware) การติดตั้งโปรแกรมควบคุมให้มีเฉพาะโปรแกรมที่ได้รับอนุญาตเท่านั้นที่สามารถทำงานบนเครื่อง White-label Smart Machine (whitelisting) รวมทั้งปรับปรุงประสิทธิภาพของการป้องกัน malware ให้เป็นปัจจุบัน

(๘.๓) มีระบบแจ้งเตือนผู้ประกอบธุรกิจเมื่อเครื่อง White-label Smart Machine หรืออุปกรณ์เครือข่ายสื่อสาร ถูกเข้าถึงทางกายภาพโดยมิชอบ (physical attack) เช่น เครื่อง White-label Smart Machine ถูกเปิด ถูกงัดแงะ หรือถูกติดตั้งอุปกรณ์แปลกปลอม หรืออุปกรณ์เครือข่ายสื่อสารถูกเชื่อมต่อด้วยอุปกรณ์ที่ไม่ได้รับอนุญาต

๔.๓ การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

กรณีที่ผู้ประกอบธุรกิจมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ได้ ให้ยื่นขออนุญาตผ่อนผันเป็นรายกรณีต่อ ธปท. พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนการดำเนินการ เพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธปท. จะพิจารณาให้แล้วเสร็จภายใน ๓๐ วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารประกอบการพิจารณาถูกต้องครบถ้วน โดย ธปท. อาจพิจารณาอนุญาตหรือไม่ก็ได้ หรือกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

๕. วันเริ่มต้นบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๙

วิทัย รัตนากร

ผู้ว่าการ

ธนาคารแห่งประเทศไทย