ธนาคารแห่งประเทศไทย

27 ธันวาคม 2562

เรียน ผู้จัดการ

สถาบันการเงินทุกธนาคาร

ที่ ธปท.ฝตท.(01) ว.1922/2562 เรื่อง นำส่งแนวนโยบาย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security)

ปัจจุบันสถาบันการเงิน และผู้ให้บริการการชำระเงินให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่เป็นช่องทางหลัก และการใช้บริการผ่านช่องทางดังกล่าวมีปริมาณเพิ่มขึ้นอย่างรวดเร็วและขยายตัวอย่างต่อเนื่อง ขณะเดียวกันการให้บริการผ่านช่องทางดังกล่าวทำให้ต้องเผชิญกับภัยคุกคามทางไซเบอร์ (cyber threat) ที่ปัจจุบันมีความหลากหลายและซับซ้อนมากขึ้น อาจก่อให้เกิดความเสียหายต่อลูกค้าผู้ใช้บริการได้ ธนาคารแห่งประเทศไทย (ธปท.) ได้ดูแลเรื่องดังกล่าวมาอย่างต่อเนื่องโดยได้ออกแนวนโยบายว่าด้วยการเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่ (Guiding Principles for Trusted Mobile Payments) ลงวันที่ 24 มีนาคม 2560 อย่างไรก็ตาม เพื่อยกระดับความมั่นคงปลอดภัยในการให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่ ป้องกันและควบคุมความเสี่ยงจากภัยคุกคามสำคัญได้อย่างรัดกุมเพียงพอตามมาตรฐานสากลให้ประชาชนเกิดความเชื่อมั่นในการใช้บริการ ธปท. จึงได้ออกแนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ที่ให้บริการแก่ลูกค้ารายย่อย ซึ่งประกอบด้วยมาตรการ 2 ระดับ คือ (1) มาตรการขั้นต่ำที่จำเป็นต้องดำเนินการเพื่อความรัดกุมด้านความมั่นคงปลอดภัยในการให้บริการ (2) มาตรการเพิ่มเติมที่อาจพิจารณาดำเนินการเพื่อให้เกิดความรัดกุมปลอดภัยยิ่งขึ้น

ทั้งนี้ ธปท. กำหนดให้สถาบันการเงิน ที่ให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ (Mobile Banking Application) แก่ผู้ใช้บริการลูกค้ารายย่อย ดำเนินการตามแนวนโยบายนี้ และขอให้หน่วยงานบริหารความเสี่ยงหน่วยงานกำกับการปฏิบัติตามหลักเกณฑ์ และหน่วยงานตรวจสอบภายในของสถาบันการเงิน กำกับดูแลการปฏิบัติตามแนวนโยบายดังกล่าว ให้เกิดการถ่วงดุลตามหลัก three lines of defense

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายรณดล นุ่มนนท์)
รองผู้ว่าการ ด้านเสถียรภาพสถาบันการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย แนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security)

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347, 0 2283 6574
E-Mail ITSupervision@bot.or.th

หมายเหตุ [X] ธนาคารได้จัดประชุมชี้แจง ในวันที่ 16 ตุลาคม 2562 ณ ธนาคารแห่งประเทศไทย
[ ] ไม่มีการประชุมชี้แจง

แนวนโยบาย
เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงิน
บนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security)
สำหรับสถาบันการเงิน

---

1. เหตุผลในการออกแนวนโยบาย

ปัจจุบันสถาบันการเงินให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่เป็นช่องทางหลัก และการใช้บริการผ่านช่องทางดังกล่าวมีปริมาณเพิ่มขึ้นอย่างรวดเร็วและขยายตัวอย่างต่อเนื่อง ขณะเดียวกัน การให้บริการผ่านช่องทางดังกล่าวทำให้ต้องเผชิญกับภัยคุกคามทางไซเบอร์ (cyber threat) ที่ปัจจุบันมีความหลากหลายและซับซ้อนมากขึ้น อาจก่อให้เกิดความเสียหายต่อลูกค้าผู้ใช้บริการได้ ธนาคารแห่งประเทศไทย (ธปท.) ได้ดูแลเรื่องดังกล่าวมาอย่างต่อเนื่องโดยได้ออกแนวนโยบายว่าด้วยการเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่ (Guiding Principles for Trusted Mobile Payments) ลงวันที่ 24 มีนาคม 2560 อย่างไรก็ตาม เพื่อยกระดับความมั่นคงปลอดภัย ในการให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่ให้มั่นใจว่าสามารถป้องกัน และควบคุมความเสี่ยงจากภัยคุกคามสำคัญได้อย่างรัดกุม เพียงพอตามมาตรฐานสากล ให้ประชาชนเกิดความเชื่อมั่นในการใช้บริการ ธปท. จึงได้ออกแนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ที่ให้บริการแก่กลุ่มลูกค้ารายย่อย ซึ่งประกอบด้วยมาตรการ 2 ระดับ คือ

1. มาตรการขั้นต่ำที่จำเป็นต้องดำเนินการเพื่อความรัดกุมด้านความมั่นคงปลอดภัยในการให้บริการ

2. มาตรการเพิ่มเติมที่อาจพิจารณาดำเนินการเพื่อให้เกิดความรัดกุมปลอดภัยยิ่งขึ้น

ทั้งนี้ แนวนโยบายฉบับนี้ครอบคลุมด้านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ ด้านอุปกรณ์เคลื่อนที่ของลูกค้า ด้านระบบเครือข่ายที่เชื่อมต่อกับผู้ใช้บริการหรือผู้ให้บริการภายนอก ด้านระบบประมวลผล และด้านการวางแอปพลิเคชันบนแพลตฟอร์มอิเล็กทรอนิกส์ (e-Marketplace) โดยอ้างอิงตามมาตรฐานการทดสอบที่เป็นสากล เช่น OWASP Mobile Top 10 เป็นต้น

2. ขอบเขตของการถือปฏิบัติ

แนวนโยบายฉบับนี้ใช้กับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินที่ให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ แก่ผู้ใช้บริการกลุ่มลูกค้ารายย่อย

3. เนื้อหา

3.1 คำจำกัดความ

“อุปกรณ์เคลื่อนที่” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่น เพื่อรับหรือส่งข้อมูลทางการเงิน การชำระเงิน หรือคำสั่งการชำระเงินผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง

“ผู้ให้บริการ” หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินที่ให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่แก่ผู้ใช้บริการกลุ่มลูกค้ารายย่อย

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการทางการเงินและการชำระเงินโดยช่องทางการให้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่กับผู้ให้บริการ

3.2 มาตรการการรักษาความมั่นคงปลอดภัย

แนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ฉบับนี้ ประกอบด้วยมาตรการ 2 ระดับ คือ 1. มาตรการขั้นต่ำ ที่จำเป็นต้องดำเนินการเพื่อความรัดกุมด้านความมั่นคงปลอดภัยในการให้บริการ และ 2. มาตรการเพิ่มเติมที่อาจพิจารณาดำเนินการเพื่อให้เกิดความรัดกุมปลอดภัยยิ่งขึ้น ดังนี้

1. มาตรการขั้นต่ำ เป็นมาตรการที่ป้องกันความเสี่ยงจากภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อผู้ใช้บริการและความเชื่อมั่นในวงกว้าง โดยผู้ให้บริการต้องดำเนินการปรับปรุงการรักษาความมั่นคงปลอดภัยของแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ให้เป็นไปตามมาตรการขั้นต่ำ ดังนี้

ด้านระบบ

(1) ไม่อนุญาตให้ใช้อุปกรณ์เคลื่อนที่ที่เปิดสิทธิ์ให้เข้าถึงระบบปฏิบัติการ (rooted/jailbroken) เข้าใช้งานแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลสำคัญของผู้ใช้บริการ และละเมิดหรือหลีกเลี่ยงมาตรการการรักษาความมั่นคงปลอดภัยที่ผู้ให้บริการกำหนดไว้

(2) ไม่อนุญาตให้อุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการล้าสมัย (obsolete Operating System : OS) มีช่องโหว่ร้ายแรงที่ประกาศจากหน่วยงานด้านความมั่นคงปลอดภัยที่เป็นสากลและกระทบการใช้งานของผู้ใช้บริการในวงกว้างเข้าใช้งานแอปพลิเคชัน ทั้งนี้ ในกรณีที่ obsolete OS มีช่องโหว่อื่นที่ไม่กระทบผู้ใช้บริการในวงกว้าง ควรมีมาตรการรองรับเพื่อลดความเสี่ยงของผู้ให้บริการและผู้ใช้บริการตามความเหมาะสม เช่น การแจ้งเตือนผู้ใช้บริการ การจำกัดวงเงินธุรกรรม และการเพิ่มมาตรการยืนยันตัวตน

(3) ขอสิทธิ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสิทธิ์ดังกล่าวอย่างเป็นประจำ เพื่อป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของผู้ใช้บริการ

(4) ป้องกัน source code ส่วนสำคัญ เช่น การโอนเงิน การพิสูจน์ตัวตน ไม่ให้รั่วไหลจากแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีทำการแก้ไข เปลี่ยนแปลง source code ดังกล่าว

(5) ป้องกันการฝังข้อมูลสำคัญ หรือ code ที่ไม่พึงประสงค์ (malicious code) บนแอปพลิเคชัน

(6) เข้ารหัสไฟล์ข้อมูล (files encryption) ที่จัดเก็บข้อมูลสำคัญบนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ เพื่อป้องกันข้อมูลสำคัญของผู้ใช้บริการรั่วไหล

(7) ไม่อนุญาตให้ผู้ใช้บริการใช้แอปพลิเคชันเวอร์ชั่นต่ำกว่าที่ผู้ให้บริการกำหนด เพื่อให้แอปพลิเคชันมีการรักษาความมั่นคงปลอดภัยเป็นไปตามมาตรฐานของผู้ให้บริการ

(8) ป้องกันการโจมตีในลักษณะ Distributed denial-of-service (DDoS Attack) ในระดับเครือข่าย (network layer) เพื่อป้องกันระบบจากการถูกโจมตีจนไม่สามารถให้บริการได้

(9) ป้องกันภัยจากการถูกดักจับหรือแก้ไขเปลี่ยนแปลงข้อมูลระหว่างการรับส่ง (Man in the Middle Attack) โดยยืนยันตัวตนด้วยเทคนิค Certificate Pinning หรือวิธีอื่นที่เทียบเท่า และการใช้ช่องทางสื่อสารที่ปลอดภัย (secure protocol) ในการรับส่งข้อมูล

(10) ป้องกันการสวมรอยการเข้าใช้งานของลูกค้า (Session Hijacking)

(11) ป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (server) โดยไม่ได้รับอนุญาต เช่น การเข้าถึงโดยอาศัยวิธี SQL Injection, Local File Inclusion หรือ Directory Traversal เพื่อลดความเสี่ยงจากข้อมูลรั่วไหลและระบบถูกโจมตี

(12) ตรวจสอบและรับมือแอปพลิเคชันปลอมบนแพลตฟอร์มอิเล็กทรอนิกส์ที่เป็นที่ยอมรับและน่าเชื่อถือ (official e-Marketplace) เช่น Google Play Store, App Store เพื่อลดความเสี่ยงจากการที่ลูกค้า download และติดตั้งแอปพลิเคชันปลอม

ด้านการดูแลลูกค้าผู้ใช้บริการ

(1) ผู้ให้บริการต้องจัดให้มีการเสริมสร้างความรู้ความเข้าใจการใช้บริการเทคโนโลยีทางการเงินให้แก่ประชาชน ทั้งความรู้เกี่ยวกับภัยคุกคามใหม่ ๆ และวิธีการปฏิบัติตนให้ปลอดภัยในการใช้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ในเชิงรุกและต่อเนื่อง

(2) จัดให้มีแนวปฏิบัติการให้บริการลูกค้าในการใช้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่แก่พนักงานของสถาบันการเงิน และดูแลให้พนักงาน

ถือปฏิบัติอย่างรัดกุมเข้มงวด และระมัดระวังไม่ดำเนินการในลักษณะที่ก่อให้เกิดความเสี่ยง เช่น กรณีพนักงานสาขาติดตั้งแอปพลิเคชันให้ลูกค้า ควรดำเนินการเท่าที่จำเป็น ไม่เข้าถึงข้อมูลสำคัญของลูกค้า และไม่ใส่รหัสผ่านแทนลูกค้า เป็นต้น ซึ่งอาจนำไปสู่การก่อทุจริตได้

2. มาตรการเพิ่มเติม เพื่อให้การให้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่มีการรักษาความมั่นคงปลอดภัยเข้มแข็งมากยิ่งขึ้น ผู้ให้บริการควรพิจารณาดำเนินการเพิ่มเติม ดังนี้

(1) ตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชัน เมื่อผู้ใช้บริการเข้าใช้งานในทันที (Anti-Tampering) เพื่อป้องกันไม่ให้ข้อมูลผู้ใช้บริการรั่วไหลหรือเกิดความเสียหาย จากแอปพลิเคชันที่มีการดัดแปลงแก้ไขโดยฝัง malicious code ไว้

(2) กำหนดให้ตั้งค่า PIN หรือ รหัสผ่านที่ซับซ้อน (PIN / password complexity) ในการเข้าใช้งานแอปพลิเคชันเพื่อให้ยากต่อการคาดเดา

(3) แสดงผลข้อมูลผู้ใช้บริการบนแอปพลิเคชันอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของลูกค้า (sensitive data masking) การปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application Blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้บริการจะรั่วไหล

(4) ป้องกันภัยคุกคามในระดับแอปพลิเคชัน (application layer) เช่น การเข้ารหัสข้อมูลสำคัญระหว่างรับ/ส่ง การป้องกัน DDoS Attack เพื่อยกระดับการป้องกันข้อมูลรั่วไหลระหว่างรับ/ส่ง หรือป้องกันระบบถูกโจมตีจนไม่สามารถให้บริการได้

(5) ตรวจสอบและรับมือแอปพลิเคชันปลอมบน website อื่น นอกเหนือจากแพลตฟอร์มอิเล็กทรอนิกส์ที่เป็นที่ยอมรับและน่าเชื่อถือ (official e-Marketplace) เช่น บน darkweb เป็นต้น

4. วันที่ประกาศให้ทราบ

แนวนโยบายฉบับนี้ให้ใช้บังคับตั้งแต่วันที่ 1 พฤษภาคม 2563 เป็นต้นไป

คำถาม – คำตอบแนบท้ายแนวนโยบาย

เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงิน บนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security)

ลำดับ	คำถาม	คำตอบ
1	ธปท. จะมีการกำหนดหรือไม่ว่า จะต้องดำเนินการภายในระยะเวลาเท่าไหร่ หลังจากที่ผู้ให้บริการประกาศรายชื่อ obsolete OS	สถาบันการเงินต้องปรับปรุงระบบและเตรียมการสื่อสารแก่ลูกค้า สำหรับกรณีผู้พัฒนาระบบปฏิบัติการประกาศ obsolete OS และพบช่องโหว่ร้ายแรง ธปท. เห็นว่าควรดำเนินการภายในระยะเวลา 3 เดือน ส่วนกรณีผู้พัฒนาระบบปฏิบัติการประกาศ obsolete OS แต่ยังไม่พบช่องโหว่ร้ายแรง ควรดำเนินการ ภายในระยะเวลา 6 เดือน
2	ธปท. จะมีประกาศไหมว่า OS รุ่นไหนจะไม่ให้เข้าใช้งาน จะได้ปฏิบัติได้ตรงกันทุกสถาบันการเงิน	สถาบันการเงินควรมีกระบวนการติดตามการประกาศ obsolete OS และช่องโหว่ร้ายแรงจากผู้พัฒนาระบบปฏิบัติการอย่างสม่ำเสมอ รวมทั้งควรกำหนดเป็นนโยบาย มาตรฐานหรือแนวปฏิบัติว่าระบบปฏิบัติการใดที่สถาบันการเงินไม่สามารถยอมรับความเสี่ยงได้ ทั้งนี้ สถาบันการเงินอาจหารือร่วมกับสมาชิกในกลุ่ม TB-CERT เพื่อกำหนดมาตรฐานร่วมกัน
3	ปัจจุบันสถาบันการเงินพบปัญหาเครื่องมือถือใหม่ที่มาจากบางแหล่งผลิต แต่ระบบมองว่าเป็นการ rooted เป็นไปได้หรือไม่ ให้มีการรับรองจาก กสทช. ก่อน	ธปท. อยู่ระหว่างการหารือร่วมกับ กสทช. ถึงการยกระดับความปลอดภัยของเครื่องมือถือที่นำเข้ามาใช้งานในประเทศไทย
4.	ธปท. มีรายชื่อ list โปรแกรม bypass การทำ rooted/jailbreak และการทำ Certificate Pinning ไหม ที่จะต้องสามารถป้องกันได้เป็นขั้นต่ำ	โปรแกรม bypass ขั้นต่ำจะเป็นโปรแกรมลักษณะ off-the-self คือสามารถดาวน์โหลดมาใช้งานได้ทันที โดยไม่ต้องใช้ความรู้เชิงลึก เช่น โปรแกรม RootCloak, Magisk, tsProtector สำหรับการ rooted/jailbreak และโปรแกรม SSLUnpinning, SSL Kill Switch สำหรับ Certificate Pinning เป็นต้น อย่างไรก็ดี โปรแกรมข้างต้น เป็นเพียงโปรแกรมตัวอย่างในระดับพื้นฐาน สถาบันการเงินควรพิจารณาโปรแกรมหรือเทคนิคในการ bypass อื่นเพิ่มเติมด้วย

5.	ธปท. จะมีข้อความการสื่อสารต่อผู้ใช้บริการในภาพรวมเดียวกัน เพื่อให้เกิดความชัดเจนและสื่อสารไปในทิศทางเดียวกันไหม ทั้งกรณี Rooted/Jailbroken และ Obsolete OS	สถาบันการเงินสามารถตกลงร่วมกันเพื่อกำหนดข้อความการสื่อสารให้กับประชาชนผู้ใช้บริการเพื่อให้เกิดความชัดเจนและสื่อสารไปในทิศทางเดียวกัน โดยเมื่อตกลงร่วมกันแล้ว สถาบันการเงินอาจนำข้อความที่ตกลงร่วมกันหารือกับ ธปท. ได้
6.	การป้องกัน Anti-tampering ของ 3rd party เป็นการลงทุนที่ค่อนข้างสูงของสถาบันการเงิน เป็นไปได้หรือไม่ที่จะกำหนดวิธีการที่เทียบเคียงให้ทางสถาบันการเงินปฏิบัติตาม	สถาบันการเงินสามารถใช้เทคนิคอื่นในการตรวจสอบได้ เช่น ตรวจสอบจากค่า Hashing หรือ ตรวจสอบจาก Certificate โดยเทคนิคดังกล่าวต้องสามารถป้องกันแอปพลิเคชันที่มีการดัดแปลงแก้ไขและยังสามารถเข้าใช้งานได้
7.	ธปท. ควรประกาศฟิลด์ข้อมูล sensitive data ให้ชัดเจน เพื่อให้เป็นมาตรฐานเดียวกันกับทุกสถาบันการเงิน	สถาบันการเงินแต่ละแห่งกำหนดข้อมูล sensitive ไม่เหมือนกัน ขึ้นอยู่กับปัจจัยต่าง ๆ เช่น ประเภทธุรกิจ กลุ่มลูกค้าเป้าหมาย เป็นต้น อย่างไรก็ตามทุกแห่งมีเกณฑ์การจัดชั้นความลับของข้อมูล (data classification) ที่ประกาศใช้อย่างเป็นทางการ ดังนั้นการกำหนดข้อมูล sensitive สถาบันการเงินจึงควรอ้างอิงตามหลักเกณฑ์ดังกล่าว
8.	กรณี fake app ขอทราบความเหตุผลที่ ธปท. กำหนดเรื่องนี้	เนื่องด้วย fake app เป็นวิธีการที่ใช้ในการล่อล่วงให้ใช้งานเพื่อโจรกรรมข้อมูลลูกค้า ซึ่งนำไปสู่การทุจริตทำให้เกิดความเสียหายต่อลูกค้าและอาจส่งผลกระทบต่อเนื่องมายังความเชื่อมั่นที่มีต่อสถาบันการเงิน การที่สถาบันการเงินสามารถตรวจจับและควบคุม fake app ได้รวดเร็ว จะช่วยลดความเสี่ยงดังกล่าว