ธนาคารแห่งประเทศไทย

คู่มือการรายงาน
เหตุการณ์ภัยคุกคามด้านการฉ้อโกง(Fraud Incident)

ฝ่ายชำระเงินและพันธบัตร

ธนาคารแห่งประเทศไทย

คำนำ

ตามที่ ธปท. ได้นำส่งแนวปฏิบัติ เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต ลงวันที่ 1 กุมภาพันธ์ 2564 เพื่อให้สถาบันผู้ใช้บริการบาทเนตมีแนวทางในการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ รวมถึงแนวทางในการบริหารจัดการความเสี่ยงจากภัยฉ้อโกงที่เกี่ยวข้องกับการโอนเงินผ่านระบบบาทเนต ซึ่งสอดคล้องกับแนวทางของ BIS–CPMI ในการจัดการความเสี่ยงจากการฉ้อโกงที่เกี่ยวข้องกับการโอนเงินผ่านระบบ RTGS ของธนาคารกลางในระดับสากล นั้น

ธปท. จึงได้จัดทำคู่มือการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident) เพื่อให้ สถาบันผู้ใช้บริการบาทเนต มีความรู้ ความเข้าใจในขั้นตอน รวมถึงวิธีการและรายละเอียด **การรายงาน Fraud Incident เฉพาะที่เกี่ยวข้องกับการโอนเงินผ่านระบบบาทเนต** ตามช่องทางที่ ธปท. กำหนดได้อย่างเหมาะสมและทันการณ์ เพื่อให้สถาบันผู้ใช้บริการบาทเนต และทุกฝ่ายที่เกี่ยวข้องสามารถรับมือกับ Fraud incident ได้อย่างทันท่วงที

สารบัญ

หัวข้อ **หน้า**

การรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

สำหรับผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับและบริการการชำระเงินภายใต้การกำกับ

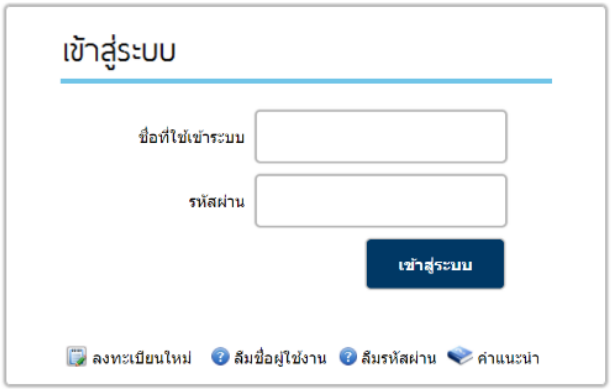
สถาบันผู้ใช้บริการบาทเนตที่เป็นผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับและบริการการชำระเงินภายใต้การกำกับ สามารถรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident) โดยใช้ช่องทางการรายงานเดียวกันกับการรายงานผ่านระบบการรายงานเหตุการณ์ที่มีนัยสำคัญ (Event Report) เหมือนในปัจจุบัน โดยมีขั้นตอนการดำเนินงาน ดังนี้

1. เมื่อพบเหตุการณ์ Fraud Incident สถาบันผู้ใช้บริการบาทเนตสามารถรายงานเหตุการณ์ดังกล่าวให้ ธปท. ผ่านระบบ Event Report (รายละเอียดตาม **หัวข้อที่ 1: การรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)**)
2. เมื่อได้รับการติดตามจาก ธปท. สถาบันผู้ใช้บริการบาทเนตต้องดำเนินการแจ้งปิดรายงานผ่านระบบ Event Report (รายละเอียดตาม **หัวข้อที่ 2: การปิดรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)**)

หัวข้อที่ 1: การรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

1. ขั้นตอนการเข้าใช้งานระบบ Event Report

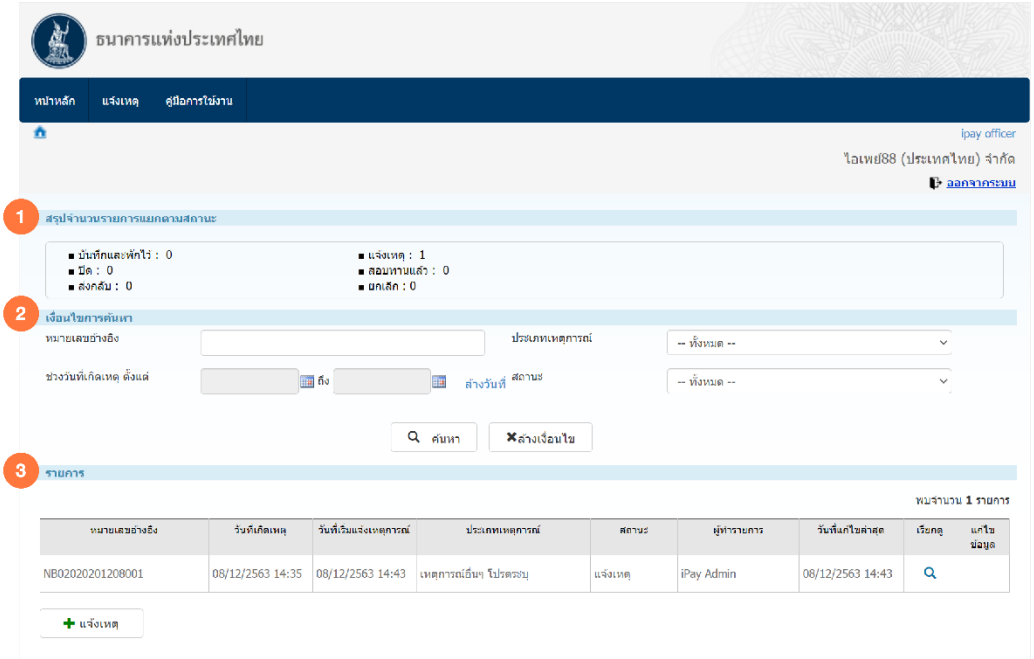
1.1 พิมพ์ URL: https://ilogin.bot.or.th/idp/Authn/UserPassword
กรอก Username และ Password เพื่อเข้าสู่ระบบ



รูปที่ 1: หน้าจอเพื่อใส่ Username และ Password ผู้ใช้งาน

1.2 เข้าสู่หน้าจอหลักของระบบ Event Report ซึ่งประกอบด้วย 3 ส่วน ดังนี้

1) สรุปจำนวนรายการแยกตามสถานะ: สรุปจำนวนรายการในการแจ้งเหตุของสถาบันท่านแยกตามสถานะการแจ้งเหตุ
2) เงื่อนไขการค้นหา: ค้นหารายการแจ้งเหตุของสถาบันท่าน โดยการระบุเงื่อนไข
3) รายการ: แสดงรายการแจ้งเหตุโดยย่อ โดยสามารถเรียกดูรายละเอียดของเหตุการณ์เพิ่มเติมได้

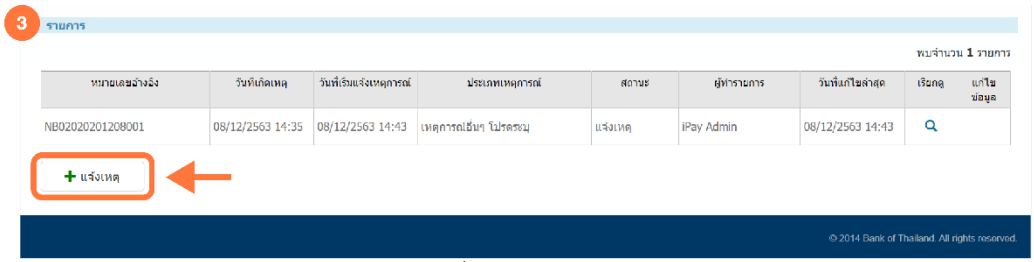


รูปที่ 2: หน้าจอหลักของระบบ Event Report

2. ขั้นตอนการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

2.1 ในส่วนที่ 3 ของหน้าจอหลัก: รายการ

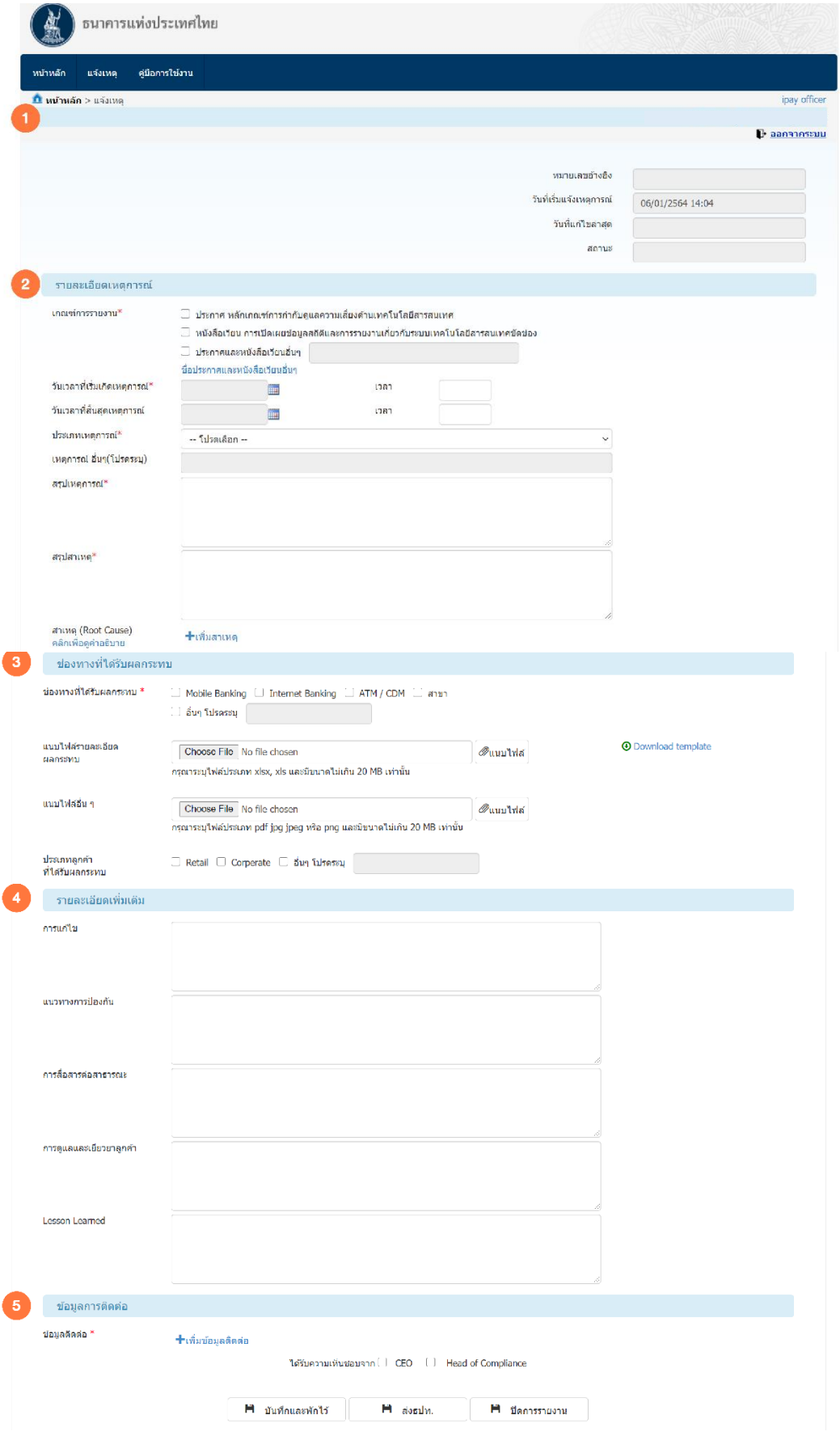
ผู้ใช้งานเลือก **ปุ่ม “แจ้งเหตุ”** เพื่อรายงานเหตุการณ์ Fraud Incident 



รูปที่ 3: รายการ

2.2 เข้าสู่หน้าจอแจ้งเหตุ (หน้าหลัก > แจ้งเหตุ) ซึ่งจะประกอบด้วยข้อมูล 5 ส่วน ดังนี้

- ส่วนที่ 1 รายละเอียดรายการแจ้งเหตุ: รายละเอียดของรายการ Fraud Incident ซึ่งระบบ Event Report จะระบุข้อมูลให้แบบอัตโนมัติ เมื่อมีการแจ้ง Fraud Incident มาที่ ธปท.
- ส่วนที่ 2 รายละเอียดเหตุการณ์: เพื่อระบุรายละเอียดของ Fraud Incident
- ส่วนที่ 3 ช่องทางที่ได้รับผลกระทบ: เพื่อระบุช่องทางที่ได้รับผลกระทบจาก Fraud Incident
- ส่วนที่ 4 รายละเอียดเพิ่มเติม: เพื่อระบุรายละเอียดเพิ่มเติมเมื่อต้องการปิดการรายงาน
- ส่วนที่ 5 ข้อมูลการติดต่อ: เพื่อระบุข้อมูลของผู้ประสานงานในกรณีที่ ธปท. ต้องการข้อมูลเพิ่มเติม



รูปที่ 4: หน้าจอแจ้งเหตุ

2.3 ผู้ใช้งานรายงานเหตุการณ์ Fraud incident โดยระบุข้อมูล ดังนี้

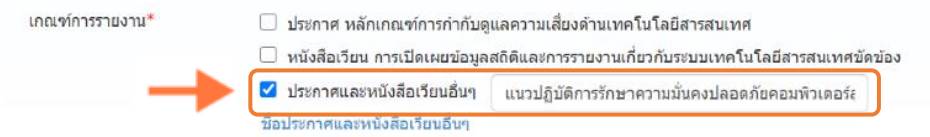
- ส่วนที่ 1 ของหน้าจอแจ้งเหตุ: รายละเอียดของรายการ Fraud Incident ซึ่งระบบ Event Report จะระบุข้อมูลให้แบบอัตโนมัติ เมื่อมีการแจ้ง Fraud Incident มาที่ ธปท. ส่วนที่ 2 ของหน้าจอแจ้งเหตุ: รายละเอียดเหตุการณ์

1) เกณฑ์การรายงาน

1.1) เลือก => **ประกาศและหนังสือเวียนอื่น ๆ**

1.2) กรอก เกณฑ์การรายงานในช่องว่างหลัง check box ประกาศและหนังสือเวียนอื่นๆ ดังนี้

=> **ฝชพ.(ว.) 3/2564 เรื่องการนำส่งแนวปฏิบัติ เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต**

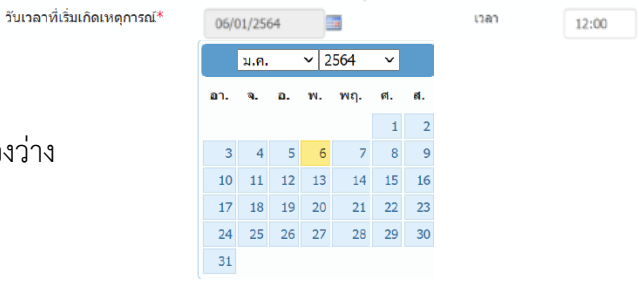


รูปที่ 5: เกณฑ์การรายงาน

2) วันเวลาที่เริ่มเกิดเหตุการณ์

เลือก => **วันที่เกิดเหตุการณ์**

กรอก => **เวลาเกิดเหตุการณ์** ในช่องว่าง



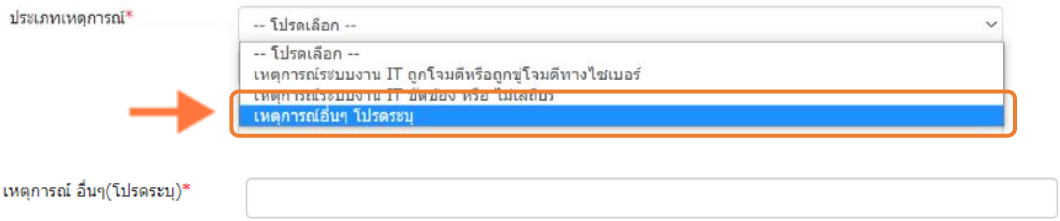
รูปที่ 6: วันและเวลา

3) ประเภทเหตุการณ์

เลือก => **เหตุการณ์อื่น ๆ โปรดระบุ**

กรอก ประเภทเหตุการณ์ในช่องเหตุการณ์อื่น ๆ (โปรดระบุ) ดังนี้

=> **เหตุการณ์เกี่ยวข้องกับระบบบาทเนต**

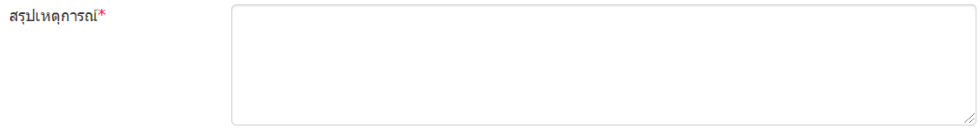


รูปที่ 7: ประเภทเหตุการณ์

4) สรุปเหตุการณ์

กรอก => **รายละเอียดสรุปเหตุการณ์**

เช่น ธนาคารพบการทำธุรกรรมของนิติบุคคลสัญชาติไทยประเภทบริษัทจำกัดแห่งหนึ่ง มีการรับโอนเงินจากบริษัทแห่งหนึ่งในประเทศออสเตรเลียจำนวนมากกว่า 4 แสนบาท วัตถุประสงค์การโอน คือ เป็นค่าสินค้าออก และบริษัทในประเทศไทยที่รับโอนเงินได้ถอนเงินออกเกือบทั้งหมดในวันถัดมา จากนั้น ในช่วงต้นเดือนมกราคม 2562 ธนาคารต้นทางในต่างประเทศได้ส่งคำสั่งขอยกเลิกการจ่ายเงินดังกล่าวมายัง ธนาคารปลายทางในประเทศไทย เป็นต้น

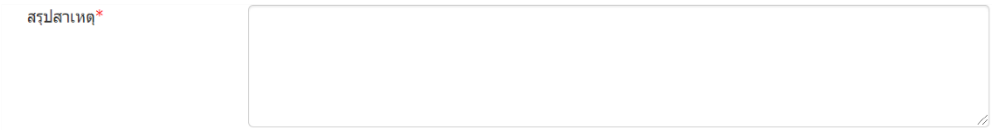


รูปที่ 8: สรุปเหตุการณ์

5) สรุปสาเหตุ

กรอก => **สาเหตุของการเกิด Fraud incident**

เช่น ธนาคารต้นทางระบุว่ารายการธุรกรรมดังกล่าวเกี่ยวข้องกับ E-mail hacking scam เป็นต้น



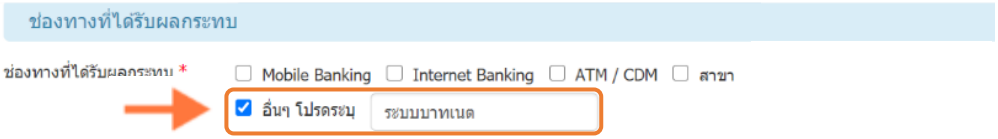
รูปที่ 9: สรุปสาเหตุ

- ส่วนที่ 3 ของหน้าจอแจ้งเหตุ: ช่องทางที่ได้รับผลกระทบ

1) ช่องทางที่ได้รับผลกระทบ

1.1) เลือก => **อื่นๆ โปรดระบุ**

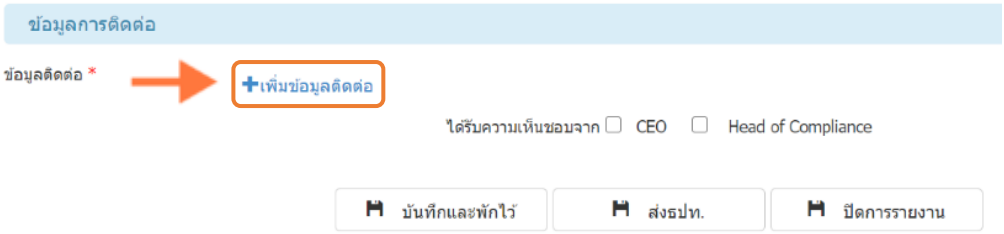
1.2) กรอก ช่องทางที่ได้รับผลกระทบในช่องหลัง Checkbox อื่นๆ โปรดระบุ => **ระบบบาทเนต**



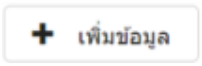
รูปที่ 10: ช่องทางที่ได้รับผลกระทบ

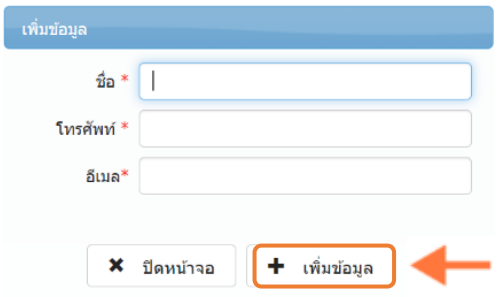
- ส่วนที่ 4 ของหน้าจอแจ้งเหตุ: รายละเอียดเพิ่มเติม
  Optional กรอกรายละเอียดเพิ่มเติมเมื่อต้องการปิดการรายงาน
- ส่วนที่ 5 ของหน้าจอแจ้งเหตุ: ข้อมูลการติดต่อ

1) การเพิ่มข้อมูลผู้ประสานงาน
   เลือก ปุ่ม **“เพิ่มข้อมูลติดต่อ”** 



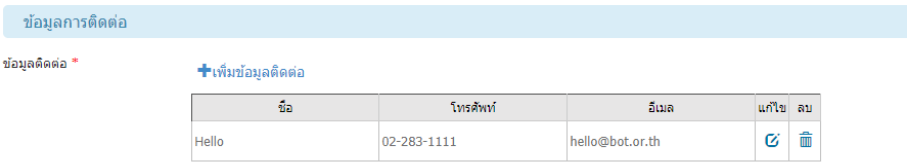
รูปที่ 11: ข้อมูลการติดต่อ

2) ระบบปรากฏ Popup
   กรอก => **ข้อมูลของผู้ที่สามารถให้รายละเอียดเหตุการณ์ได้ เช่น ผู้ประสานงาน ด้าน Compliance ดังนี้**
   2.1) **ชื่อ**
   2.2) **เบอร์ติดต่อ**
   2.3) **อีเมล**
   2.4) เลือก **ปุ่ม “เพิ่มข้อมูล”** เพื่อยืนยันการเพิ่มข้อมูลผู้ประสานงาน 



รูปที่ 12: Popup การเพิ่มข้อมูล

2.5) ระบบจะแสดงข้อมูลผู้ประสานงาน



รูปที่ 13: ข้อมูลการติดต่อ

- การยืนยันข้อมูลและแจ้งเหตุการณ์ Fraud Incident

  3.1) เลือก => **ได้รับความเห็นชอบจาก CEO หรือ Head of Compliance**

  3.2) เลือก =>

  3.2.1) หากยังกรอกข้อมูลไม่ครบถ้วน เลือก **“บันทึกและพักไว้”**

  3.2.2) หากกรอกข้อมูลครบถ้วนแล้ว เลือก **“ส่ง ธปท.”** ระบบ Event Report จะส่ง Email มายังผู้ที่เกี่ยวข้องของ ธปท.

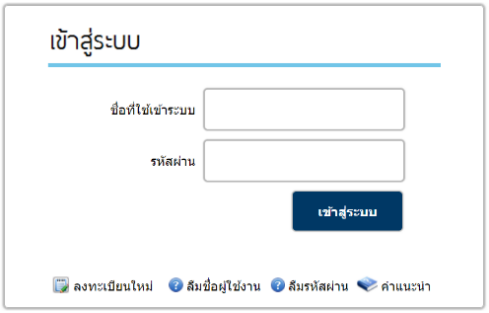
รูปที่ 14: การบันทึกและนำส่งข้อมูล

<u>หัวข้อที่ 2: การปิดรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)</u>

1. ขั้นตอนการเข้าใช้งานระบบ Event Report

1.1 พิมพ์ URL: https://ilogin.bot.or.th/idp/Authn/UserPassword

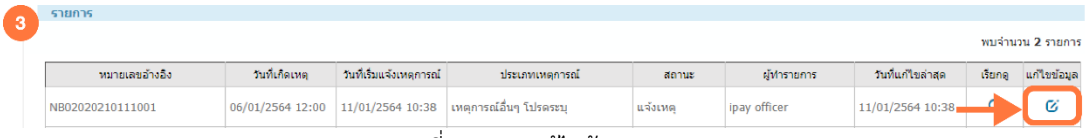
กรอก Username และ Password เพื่อเข้าสู่ระบบ



รูปที่ 15: หน้าจอให้ใส่ Username และ Password ผู้ใช้งาน

1.2 เข้าสู่หน้าจอหลักของระบบ Event Report

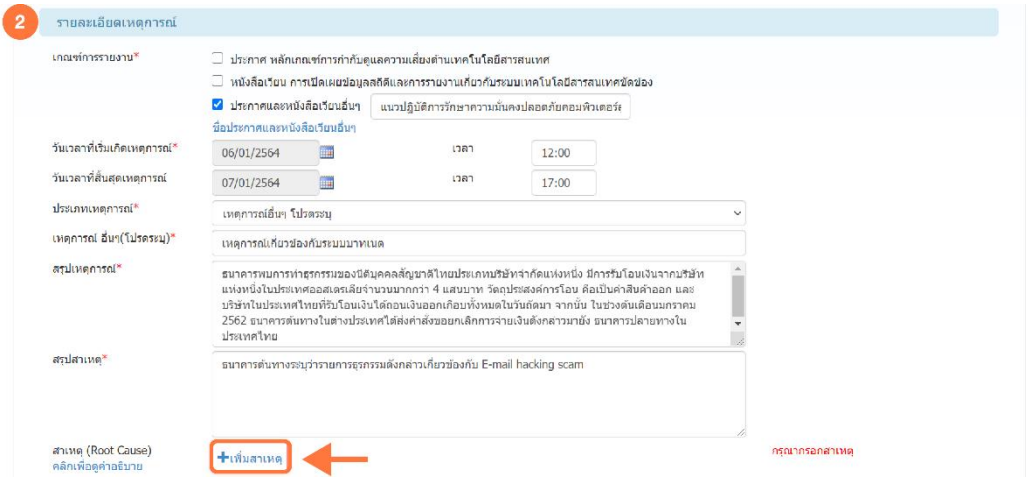
- ส่วนที่ 3 ของหน้าจอหลัก: รายการ
  เลือก => **แก้ไขข้อมูล** เพื่อแก้ไขเหตุการณ์ Fraud Incident ที่เคยแจ้งไว้



รูปที่ 16: การแก้ไขข้อมูล

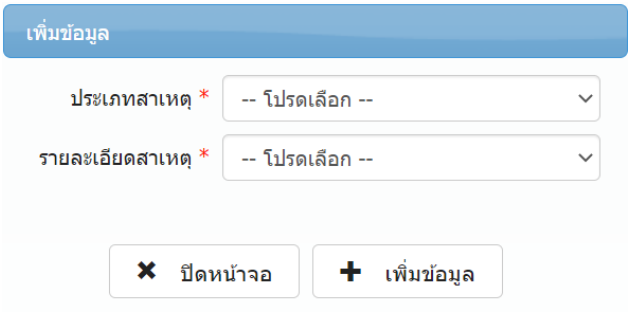
1.3 เข้าสู่หน้าจอแจ้งเหตุ (หน้าหลัก > แจ้งเหตุ)

- ส่วนที่ 2 ของหน้าจอแจ้งเหตุ: รายละเอียดเหตุการณ์:
  1) เลือก => **เพิ่มสาเหตุ**

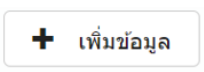


รูปที่ 17: การเพิ่มสาเหตุ

2) ระบบจะปรากฏ Popup
เลือก => **ประเภทสาเหตุ และรายละเอียดสาเหตุ** เพื่อระบุและจัดกลุ่มเหตุการณ์

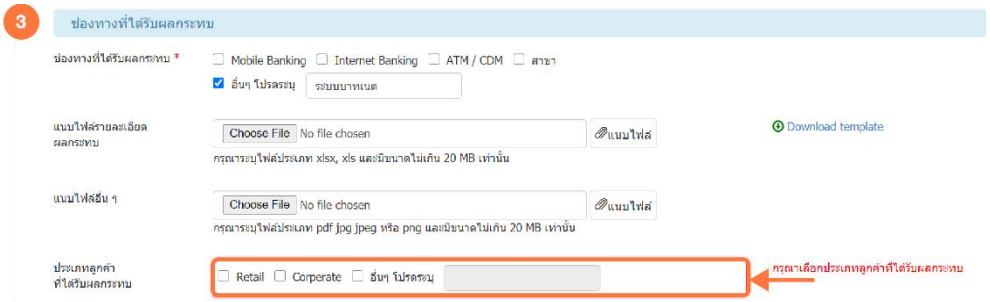


รูปที่ 18: ประเภทและรายละเอียดสาเหตุ

3) เลือก => **“เพิ่มข้อมูล”** 

เพื่อยืนยันสาเหตุของ Fraud Incident

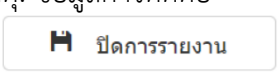
- ส่วนที่ 3 ของหน้าจอแจ้งเหตุ: รายละเอียดเหตุการณ์
  เลือก => **ประเภทลูกค้าที่ได้รับผลกระทบ** เพื่อระบุประเภทของลูกค้าที่ได้รับผลกระทบ



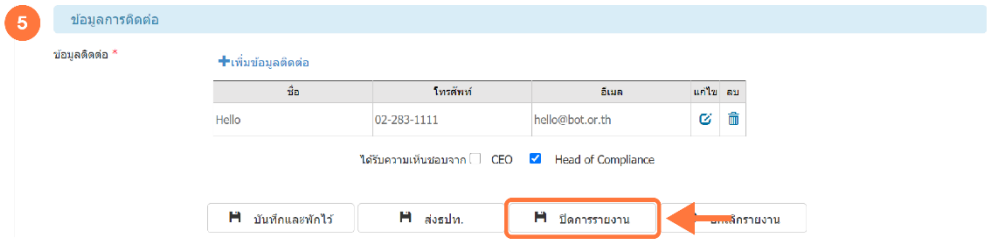
รูปที่ 19: ประเภทลูกค้าที่ได้รับผลกระทบ

- ส่วนที่ 4 ของหน้าจอแจ้งเหตุ: รายละเอียดเพิ่มเติม
  กรอก ข้อมูลลงในช่องวางตามหัวข้อ ดังนี้
  4.1) **การแก้ไข**
  4.2) **แนวทางการป้องกัน**
  4.3) **การสื่อสารต่อสาธารณะ**
  4.4) **การดูแลเยียวยาลูกค้า**

รูปที่ 20: รายละเอียดเพิ่มเติม

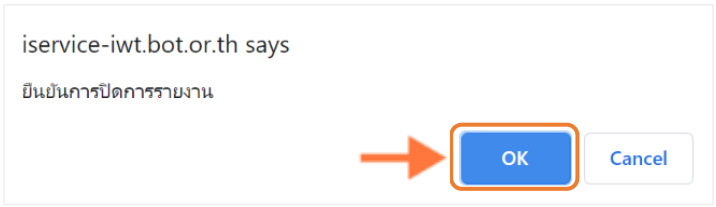
- ส่วนที่ 5 ของหน้าจอแจ้งเหตุ: ข้อมูลการติดต่อ
  เลือก => **ปิดการรายงาน** 

  เพื่อให้ Event Report บันทึกปิดการรายงาน



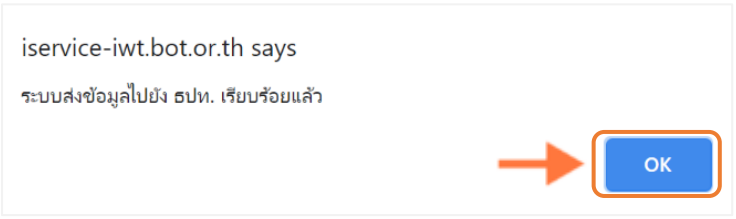
รูปที่ 21: การปิดรายงาน

- ระบบปรากฏ Popup เพื่อยืนยันการปิดรายงาน
  เลือก => **ok** 



รูปที่ 22: ยืนยันการปิดรายงาน

- ระบบปรากฏ Popup แจ้งการบันทึกรายงาน
  เลือก => **ok** 



รูปที่ 23: แจ้งการบันทึกรายงาน

การรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

สำหรับสถาบันผู้ใช้บริการบาทเนตอื่นๆ

สถาบันผู้ใช้บริการบาทเนต ที่ไม่ได้อยู่ภายใต้การกำกับดูแลของ ธปท. สามารถรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident) โดยใช้แบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident) (ตามแนบ ในภาคผนวก) ส่งมายังทีมบาทเนต ผ่านช่องทาง E-mail (bnhelpdesk@bot.or.th) โดยมีรายละเอียด ขั้นตอนการรายงาน รวมถึงเกณฑ์การกำหนดระดับผลกระทบของเหตุการณ์ทันทีที่ทราบเหตุการณ์และได้รับความเห็นชอบจากผู้บริการ หรือ Head of Compliance แล้ว ดังนี้

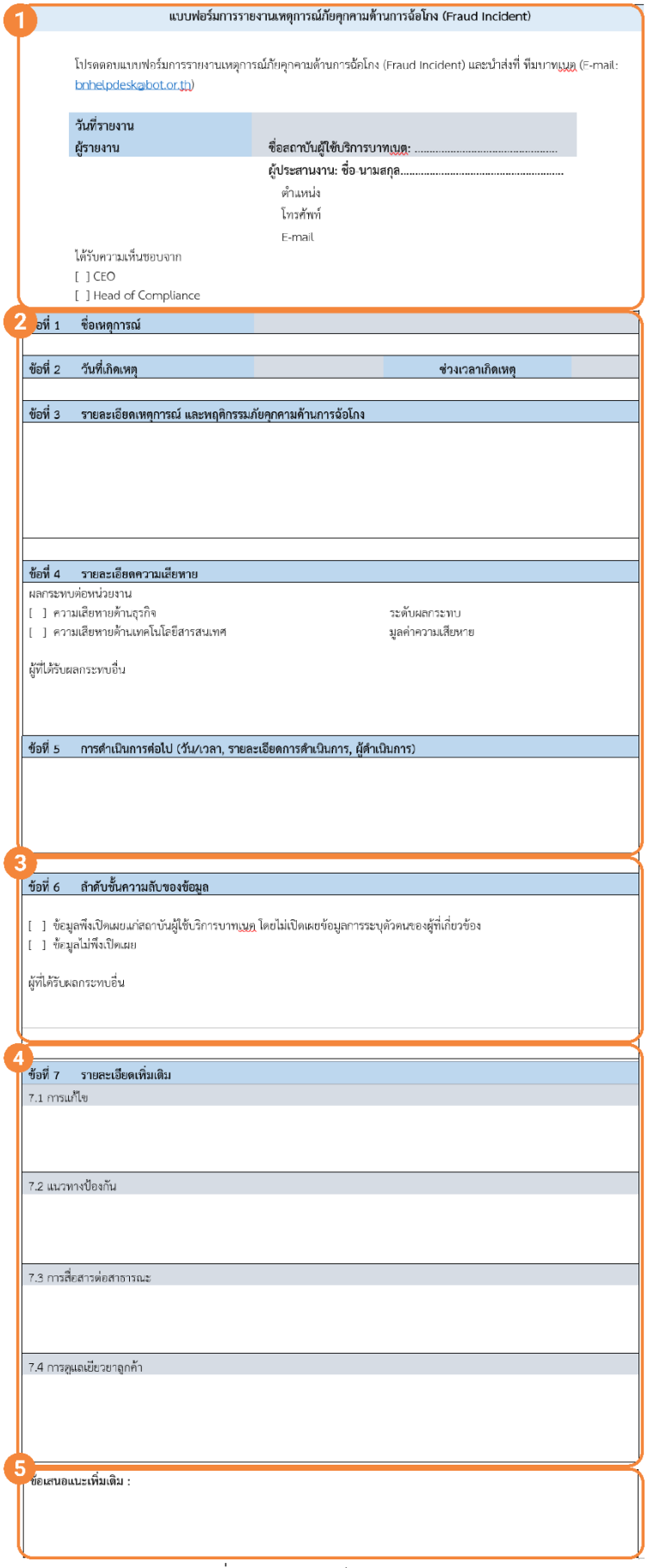
1. เมื่อพบเหตุการณ์ภัยคุกคามด้านการฉ้อโกงที่เกี่ยวข้องกับการโอนเงินผ่านระบบบาทเนต สถาบันผู้ใช้บริการบาทเนตสามารถรายงานเหตุการณ์ดังกล่าว โดยใช้แบบฟอร์มฯ ส่งมายังทีมบาทเนต (รายละเอียดตาม **หัวข้อที่ 1: การรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)**)
2. เมื่อได้รับการติดตามจาก ธปท. สถาบันผู้ใช้บริการบาทเนตต้องดำเนินการแจ้งปิดรายงานโดยใช้แบบฟอร์มฯ ส่งมายังทีมบาทเนต (รายละเอียดตาม **หัวข้อที่ 2: การปิดรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)**)

หัวข้อที่ 1: การรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

1. แบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

แบบฟอร์มการรายงานฯ ประกอบด้วยข้อมูล 5 ส่วน ดังนี้

- ส่วนที่ 1 รายละเอียดของสถาบันและผู้ประสานงาน
- ส่วนที่ 2 รายละเอียดเหตุการณ์
- ส่วนที่ 3 การจัดลำดับชั้นของข้อมูล
- ส่วนที่ 4 รายละเอียดเพิ่มเติม
- ส่วนที่ 5 ข้อเสนอแนะเพิ่มเติม



แบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

โปรดตอบแบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident) และนำส่งที่ ทีมบาทเนต (E-mail: bnhelpdesk@bot.or.th)

วันที่รายงาน	
ผู้รายงาน	**ชื่อสถาบันผู้ใช้บริการบาทเนต:** .....
	ผู้ประสานงาน: ชื่อ นามสกุล.....
	ตำแหน่ง
	โทรศัพท์
	E-mail

ได้รับความเห็นชอบจาก
[ ] CEO
[ ] Head of Compliance

ข้อที่ 1 ชื่อเหตุการณ์

ข้อที่ 2 วันที่เกิดเหตุ **ช่วงเวลาเกิดเหตุ**

ข้อที่ 3 รายละเอียดเหตุการณ์ และพฤติกรรมภัยคุกคามด้านการฉ้อโกง

ข้อที่ 4 รายละเอียดความเสียหาย

ผลกระทบต่อหน่วยงาน
[ ] ความเสียหายด้านธุรกิจ ระดับผลกระทบ
[ ] ความเสียหายด้านเทคโนโลยีสารสนเทศ มูลค่าความเสียหาย

ผู้ที่ได้รับผลกระทบอื่น

ข้อที่ 5 การดำเนินการต่อไป (วัน/เวลา, รายละเอียดการดำเนินการ, ผู้ดำเนินการ)

ข้อที่ 6 ลำดับชั้นความลับของข้อมูล

[ ] ข้อมูลพึงเปิดเผยแก่สถาบันผู้ใช้บริการบาทเนต โดยไม่เปิดเผยข้อมูลการระบุตัวตนของผู้ที่เกี่ยวข้อง
[ ] ข้อมูลไม่พึงเปิดเผย

ผู้ที่ได้รับผลกระทบอื่น

ข้อที่ 7 รายละเอียดเพิ่มเติม

7.1 การแก้ไข

7.2 แนวทางป้องกัน

7.3 การสื่อสารต่อสาธารณะ

7.4 การดูแลเยียวยาลูกค้า

ข้อเสนอแนะเพิ่มเติม :

รูปที่ 24: แบบฟอร์มการรายงาน

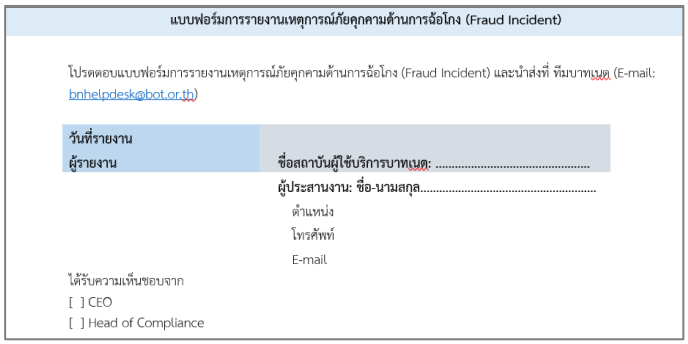
2. ขั้นตอนการรายงานโดยใช้แบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

- ส่วนที่ 1 รายละเอียดของสถาบันและผู้ประสานงาน:

  กรอก =>

  1) **วันที่รายงาน** ระบุวันที่สถาบันผู้ใช้บริการบาทเนตรายงานเหตุการณ์ Fraud Incident ให้ ธปท.

  2) **รายละเอียดของผู้รายงาน** ระบุข้อมูลของผู้รายงานเหตุการณ์ Fraud Incident


แบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

โปรดตอบแบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident) และนำส่งที่ ทีมบาทเนต (E-mail: bnhelpdesk@bot.or.th)

วันที่รายงาน
ผู้รายงาน
ชื่อสถาบันผู้ใช้บริการบาทเนต: .....
ผู้ประสานงาน: ชื่อ-นามสกุล.....
ตำแหน่ง
โทรศัพท์
E-mail

ได้รับความเห็นชอบจาก
[ ] CEO
[ ] Head of Compliance

รูปที่ 25: ของสถาบันและผู้ประสานงาน

- ส่วนที่ 2 รายละเอียดเหตุการณ์:

  กรอก =>

  1) **ชื่อเหตุการณ์** ระบุชื่อของเหตุการณ์ Fraud Incident

  เช่น Email Hacking Scam


ข้อที่ 1 ชื่อเหตุการณ์ Email Hacking Scam

รูปที่ 26: ชื่อเหตุการณ์

  2) **วันที่เกิดเหตุการณ์** ระบุวันที่เกิดเหตุการณ์ Fraud Incident

  เช่น 23/11/2020

  3) **ช่วงเวลาที่เกิดเหตุการณ์** ระบุช่วงเวลาที่เกิดเหตุการณ์ Fraud Incident

  เช่น 14:00 – 17:00


ข้อที่ 2 วันที่เกิดเหตุ 23/11/2020 ช่วงเวลาเกิดเหตุ 14:00 – 17:00

รูปที่ 27: วันและช่วงเวลาที่เกิดเหตุการณ์

  4) **รายละเอียดเหตุการณ์และพฤติกรรมการโอนเงินต้องสงสัย** ระบุรายละเอียดของเหตุการณ์ Fraud Incident / พฤติการณ์การโอนเงินต้องสงสัยที่เกิดขึ้น

  เช่น ธนาคารพบการทำธุรกรรมของนิติบุคคลสัญชาติไทยประเภทบริษัทจำกัดแห่งหนึ่ง มีการรับโอนเงินจากบริษัทแห่งหนึ่งในประเทศออสเตรเลียจำนวนมากกว่า 4 แสนบาท วัตถุประสงค์การโอน คือเป็นค่าสินค้าออก และบริษัทในประเทศไทยที่รับโอนเงินได้ถอนเงินออกเกือบทั้งหมดในวันถัดมา จากนั้น ในช่วงต้นเดือนมกราคม 2562 ธนาคารต้นทางในต่างประเทศได้ส่งคำสั่งขอยกเลิกการจ่ายเงินดังกล่าวมายัง ธนาคารปลายทางในประเทศไทย

ข้อที่ 3 รายละเอียดเหตุการณ์ และพฤติกรรมภัยคุกคามด้านการฉ้อโกง (Fraud Incident)
ธนาคารพบการทำธุรกรรมของนิติบุคคลสัญชาติไทยประเภทบริษัทจำกัดแห่งหนึ่ง มีการรับโอนเงินจากบริษัทแห่งหนึ่งในประเทศออสเตรเลียจำนวนมากกว่า 4 แสนบาท วัตถุประสงค์การโอน คือเป็นค่าสินค้าออก และบริษัทในประเทศไทยที่รับโอนเงินได้ถอนเงินออกเกือบทั้งหมดในวันถัดมา จากนั้น ในช่วงต้นเดือนมกราคม 2562 ธนาคารต้นทางในต่างประเทศได้ส่งคำสั่งขอยกเลิกการจ่ายเงินดังกล่าวมายัง ธนาคารปลายทางในประเทศไทย

รูปที่ 28: รายละเอียดเหตุการณ์และพฤติกรรมการโอนเงินต้องสงสัย

5) **รายละเอียดความเสียหาย** ระบุรายละเอียดความเสียหายที่เกิดขึ้นจากเหตุการณ์ Fraud Incident ประกอบด้วยข้อมูล 4 ส่วน ดังนี้

เลือก => **ผลกระทบต่อหน่วยงาน** เพื่อระบุว่าความเสียหายที่เกิดขึ้น มีผลกระทบในด้านธุรกิจ และ/หรือ เทคนิค

กรอก => **ระดับผลกระทบ** เพื่อระบุระดับของผลกระทบที่เกิดขึ้น อ้างอิงตาม **เกณฑ์การกำหนดระดับผลกระทบของเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)** ในภาคผนวก

กรอก => **มูลค่าความเสียหาย** เพื่อระบุมูลค่าความเสียหายที่เกิดขึ้น ในรูปแบบจำนวนเงิน

กรอก => **ผู้ได้รับผลกระทบอื่น** เพื่อระบุผู้ได้รับผลกระทบอื่น นอกเหนือจากสถาบันผู้ใช้บริการบาทเนตที่เป็นผู้แจ้ง

เช่น ความเสียหายด้านธุรกิจ / ระดับผลกระทบ Low / มูลค่าความเสียหาย 400,000 บาท

ข้อที่ 4 รายละเอียดความเสียหาย		
ผลกระทบต่อหน่วยงาน	☐	
[☑] ความเสียหายด้านธุรกิจ	ระดับผลกระทบ	Low
[ ] ความเสียหายด้านเทคโนโลยีสารสนเทศ	มูลค่าความเสียหาย	400,000 บาท
ผู้ที่ได้รับผลกระทบอื่น		

รูปที่ 29: รายละเอียดความเสียหาย

6) **การดำเนินการต่อไป** ระบุแนวทางในการดำเนินงานต่อไปของสถาบันผู้ใช้บริการบาทเนต

เช่น อยู่ระหว่างการตรวจสอบสาเหตุและที่มาของการฉ้อโกง

ข้อที่ 5 การดำเนินการต่อไป (วัน/เวลา, รายละเอียดการดำเนินการ, ผู้ดำเนินการ)
อยู่ระหว่างการตรวจสอบสาเหตุและที่มาของการฉ้อโกง

รูปที่ 30: การดำเนินการต่อไป

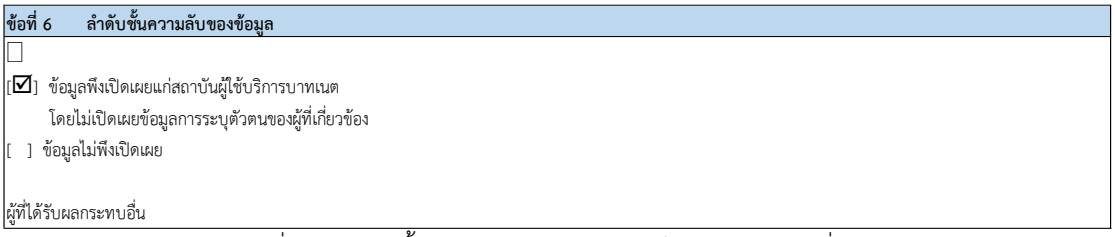
- ส่วนที่ 3 การจัดลำดับชั้นของข้อมูล

  เลือก => **ข้อมูลพึงเปิดเผย หรือ ข้อมูลไม่พึงเปิดเผย** เพื่อระบุลำดับชั้นความลับของข้อมูล

หากเลือก ข้อมูลพึงเปิดเผย: ธปท. จะนำข้อมูลที่ได้รับมาพิจารณาความสำคัญและทำการ Masking ข้อมูลส่วนบุคคล โดยมีคณะทำงานเพื่อกลั่นกรองข้อมูลเป็นผู้พิจารณาเหตุการณ์และเนื้อหาก่อนทำการสื่อสารแจ้งเตือนให้กับสถาบันผู้ใช้บริการบาทเนตรายอื่นที่เกี่ยวข้อง

หากเลือก ไม่พึงเปิดเผย ธปท. จะบันทึกไว้เพื่อให้เป็นข้อมูลในประกอบการจัดหาแนวทาง และยกระดับการป้องกันภัยคุกคามด้านการฉ้อโกง (Fraud Incident) ต่อไป

กรอก => **ผู้ที่ได้รับผลกระทบอื่น (หากมี)**



รูปที่ 31: ลำดับชั้นความลับของข้อมูลและผู้ได้รับผลกระทบอื่น

3. การส่งแบบฟอร์มฯ เพื่อรายงานภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

เมื่อทำการกรอกข้อมูลลงในแบบฟอร์มฯ เรียบร้อยแล้ว สถาบันผู้ใช้บริการบาทเนตสามารถนำส่งให้ **ทีมบาทเนต ผ่านทาง E-mail: bnhelpdesk@bot.or.th**

<u>หัวข้อที่ 2: การปิดรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)</u>

1. ขั้นตอนการปิดรายงานโดยใช้แบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

- ส่วนที่ 4 รายละเอียดเพิ่มเติม

  กรอก =>

  1) **การแก้ไข** เพื่อระบุวิธีการแก้ไขเหตุการณ์

  2) **แนวทางการป้องกัน** ระบุแนวทางเพื่อป้องกันการเกิดเหตุการณ์ในลักษณะเดียวกันขึ้นในอนาคต

  3) **การสื่อสารต่อสาธารณะ** เพื่อระบุรายละเอียดการชี้แจงต่อผู้เกี่ยวข้องการสื่อสารเหตุการณ์ไปยังสาธารณะ

  4) **การดูแลเยียวยาลูกค้า** เพื่อระบุรายละเอียดการดูแลเยียวยาลูกค้า

ข้อที่ 7 รายละเอียดเพิ่มเติม
7.1 การแก้ไข
7.2 แนวทางป้องกัน
7.3 การสื่อสารต่อสาธารณะ
7.4 การดูแลเยียวยาลูกค้า

รูปที่ 32: รายละเอียดเพิ่มเติม

- ส่วนที่ 5 ข้อเสนอแนะเพิ่มเติม

กรอก => **ข้อเสนอแนะเพิ่มเติม** เพื่อระบุรายละเอียด หรือ ข้อเสนอแนะให้กับ ธปท. หรือสถาบันผู้ใช้บริการบาทเนตรายอื่นเพิ่มเติม

ข้อเสนอแนะเพิ่มเติม :

รูปที่ 33: ข้อเสนอแนะเพิ่มเติม

2. การส่งแบบฟอร์มฯ เพื่อปิดรายงานภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

เมื่อทำการกรอกข้อมูลลงในแบบฟอร์มฯ เรียบร้อยแล้ว สถาบันผู้ใช้บริการบาทเนตสามารถนำส่งให้ **ทีมบาทเนต ผ่านทาง E-mail: bnhelpdesk@bot.or.th**

ภาคผนวก 1

เกณฑ์การกำหนดระดับผลกระทบของเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

เกณฑ์การรายงาน

	ระดับความรุนแรง		
	Low	**Medium**	**High**
ผลกระทบ	– มูลค่าความเสียหายไม่เกิน 50 ล้านบาท	– มูลค่าความเสียหายมากกว่า 50 ล้านบาท แต่ไม่เกิน 100 ล้านบาท	– มูลค่าความเสียหายมากกว่า 100 ล้านบาท
	– ไม่กระทบต่อชื่อเสียงและความน่าเชื่อถือ	– กระทบต่อชื่อเสียงและความน่าเชื่อถือเป็นวงกว้าง ในระยะเวลาสั้น	– กระทบต่อชื่อเสียงและความน่าเชื่อถือเป็นวงกว้าง อย่างรุนแรง
	– ไม่กระทบต่อการดำเนินงานของสถาบัน	– กระทบต่อการดำเนินงานและบุคคลากรของสถาบัน	– กระทบต่อการดำเนินในภาพรวมของสถาบัน และอาจส่งผลทำให้ไม่สามารถดำเนินการตามภารกิจหลักได้

ภาคผนวก 2

รายชื่อสถาบันผู้ใช้บริการบาทเนต (ข้อมูล ณ 30 ธันวาคม 2563)

ลำดับ	ชื่อสถาบันผู้ใช้บริการบาทเนต	อยู่ภายใต้การกำกับดูแล (40 ราย)	ไม่อยู่ภายใต้การกำกับดูแล (21 ราย)
	ธนาคารพาณิชย์ไทย		
1	ธนาคารเอเอ็นแซด (ไทย) จำกัด (มหาชน)	✓	
2	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)	✓	
3	ธนาคารแห่งประเทศจีน (ไทย) จำกัด (มหาชน)	✓	
4	ธนาคารกรุงเทพ จำกัด (มหาชน)	✓	
5	ธนาคารเมกะ สากลพาณิชย์ จำกัด (มหาชน)	✓	
6	ธนาคารไอซีบีซี (ไทย) จำกัด (มหาชน)	✓	
7	ธนาคารกสิกรไทย จำกัด (มหาชน)	✓	
8	ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน)	✓	
9	ธนาคารกรุงไทย จำกัด (มหาชน)	✓	
10	ธนาคารแลนด์แอนด์เฮ้าส์ จำกัด (มหาชน)	✓	
11	ธนาคารสแตนดาร์ดชาร์เตอร์ด (ไทย) จำกัด (มหาชน)	✓	
12	ธนาคารไทยพาณิชย์ จำกัด (มหาชน)	✓	
13	ธนาคารซูมิโตโม มิตซุย ทรัสต์ (ไทย) จำกัด (มหาชน)	✓	
14	ธนาคารทิสโก้ จำกัด (มหาชน)	✓	
15	ธนาคารธนชาต จำกัด (มหาชน)	✓	
16	ธนาคารไทยเครดิตเพื่อรายย่อย จำกัด (มหาชน)	✓	
17	ธนาคารทหารไทย จำกัด (มหาชน)	✓	
18	ธนาคารซีไอเอ็มบี ไทย จำกัด (มหาชน)	✓	
19	ธนาคารยูโอบี จำกัด (มหาชน)	✓	
	สาขาธนาคารต่างประเทศ		
20	ธนาคารอินเดียนโอเวอร์ซีส์ สาขากรุงเทพฯ	✓	
21	ธนาคารบีเอ็นพี พารีบาส์ สาขากรุงเทพฯ	✓	
22	ธนาคารแห่งอเมริกา เนชั่นแนล แอสโซซิเอชั่น สาขากรุงเทพฯ	✓	
23	ธนาคารเจพีมอร์แกน เชส สาขากรุงเทพฯ	✓	
24	ธนาคารซิตี้แบงก์ สาขากรุงเทพฯ	✓	

ภาคผนวก 2

25	ธนาคารอาร์ เอช บี จำกัด สาขากรุงเทพฯ	✓	
26	ธนาคารดอยซ์แบงก์ สาขากรุงเทพฯ	✓	
27	ธนาคารฮ่องกงและเซี่ยงไฮ้ แบงกิ้งคอร์ปอเรชั่น จำกัด สาขากรุงเทพฯ	✓	
28	ธนาคารมิซูโฮ จำกัด สาขากรุงเทพฯ	✓	
29	ธนาคารโอเวอร์ซี-ไชนีสแบงกิ้งคอร์ปอเรชั่น จำกัด สาขากรุงเทพฯ	✓	
30	ธนาคารซูมิโตโม มิตซุย แบงกิ้ง คอร์ปอเรชั่น สาขากรุงเทพฯ	✓	
	สถาบันการเงินพิเศษของรัฐ		
31	ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตรฯ	✓	
32	ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย	✓	
33	ธนาคารอาคารสงเคราะห์	✓	
34	ธนาคารออมสิน	✓	
35	ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย	✓	
36	ธนาคารอิสลามแห่งประเทศไทย	✓	
	บริษัทเงินทุนและหลักทรัพย์		
37	บริษัทเงินทุน แอ็ดวานซ์ จำกัด (มหาชน)		✓
38	บริษัทเงินทุน ศรีสวัสดิ์ จำกัด (มหาชน)		✓
39	บริษัทหลักทรัพย์ โนมูระ พัฒนสิน จำกัด (มหาชน)		✓
40	บริษัทหลักทรัพย์ เคจีไอ (ประเทศไทย) จำกัด (มหาชน)		✓
41	บริษัทหลักทรัพย์ ธนชาต จำกัด		✓
42	บริษัทหลักทรัพย์ ทิสโก้ จำกัด		✓
43	บริษัทหลักทรัพย์ เพื่อธุรกิจหลักทรัพย์ จำกัด (มหาชน)		✓
	สถาบันอื่น ๆ		
44	สถาบันคุ้มครองเงินฝาก		✓
45	บริษัท ฟินเน็ต อินโนเวชั่น เน็ตเวิร์ค จำกัด	✓	
46	บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด	✓	
47	บริษัท ศูนย์ประมวลผล จำกัด	✓	
48	บริษัท สำนักหักบัญชี (ประเทศไทย) จำกัด		✓
49	บริษัท ไทย เพย์เมนต์ เน็ตเวิร์ก จำกัด	✓	
50	บริษัท ศูนย์รับฝากหลักทรัพย์ (ประเทศไทย) จำกัด		✓
51	บริษัท วีซ่า อินเตอร์เนชั่นแนล (ประเทศไทย) จำกัด		✓

ภาคผนวก 2

	ส่วนราชการ		
52	กรมบัญชีกลาง		✓
53	กรมสรรพากร		✓
	ส่วนงานภายใน ธปท.		
54	ฝ่ายการเงินและการบัญชี ทีมรับ - จ่ายเงิน		✓
55	ฝ่ายการชำระเงินและพันธบัตร - ทีมเงินฝาก		✓
56	ฝ่ายการชำระเงินและพันธบัตร - ทีมจัดการพันธบัตร, ทีมการเงินพันธบัตร		✓
57	ฝ่ายการชำระเงินและพันธบัตร - ส่วนหักบัญชีเช็ค		✓
58	กองทุนเพื่อการฟื้นฟูและพัฒนาระบบสถาบันการเงิน		✓
59	ฝ่ายบริหารจัดการธนบัตร		✓
60	ฝ่ายการชำระเงินและพันธบัตร - ทีมบาทเนต		✓
61	ฝ่ายการเงินและบัญชี - ส่วนบริหารงานชำระราคา		✓

ภาคผนวก 3

แบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident)

โปรดตอบแบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามด้านการฉ้อโกง (Fraud Incident) และนำส่งที่ ทีมบาทเนต (E-mail: bnhelpdesk@bot.or.th)

วันที่รายงาน	
ผู้รายงาน	**ชื่อสถาบันผู้ใช้บริการบาทเนต: .....**
	ผู้ประสานงาน: ชื่อ-นามสกุล.....
	ตำแหน่ง
	โทรศัพท์
	E-mail

ได้รับความเห็นชอบจาก

[ ] CEO หรือตำแหน่งเทียบเท่า

[ ] Head of Compliance หรือตำแหน่งเทียบเท่า

ข้อที่ 1	**ชื่อเหตุการณ์**	
ข้อที่ 2	**วันที่เกิดเหตุ**	**ช่วงเวลาเกิดเหตุ**
ข้อที่ 3	**รายละเอียดเหตุการณ์ และพฤติกรรมภัยคุกคามด้านการฉ้อโกง**	
ข้อที่ 4	**รายละเอียดความเสียหาย**	

ผลกระทบต่อหน่วยงาน

[ ] ความเสียหายด้านธุรกิจ — ระดับผลกระทบ

[ ] ความเสียหายด้านเทคโนโลยีสารสนเทศ — มูลค่าความเสียหาย

ผู้ที่ได้รับผลกระทบอื่น

ภาคผนวก 3

ข้อที่ 5 การดำเนินการต่อไป (วัน/เวลา, รายละเอียดการดำเนินการ, ผู้ดำเนินการ)

ข้อที่ 6 ลำดับชั้นความลับของข้อมูล

[ ] ข้อมูลพึงเปิดเผยแก่สถาบันผู้ใช้บริการบาทเนต โดยไม่เปิดเผยข้อมูลการระบุตัวตนของผู้ที่เกี่ยวข้อง
[ ] ข้อมูลไม่พึงเปิดเผย

ผู้ที่ได้รับผลกระทบอื่น

ข้อที่ 7 รายละเอียดเพิ่มเติม

7.1 การแก้ไข

7.2 แนวทางป้องกัน

7.3 การสื่อสารต่อสาธารณะ

7.4 การดูแลเยียวยาลูกค้า

ภาคผนวก 3

ข้อเสนอแนะเพิ่มเติม :