**ПОРЯДОК**

**дій Клієнта у випадку виявлення факту несанкціонованого переказу коштів**

Всі терміни, що використовуються у тексті цього Порядку дій Клієнта у випадку виявлення факту несанкціонованого переказу коштів мають значення, викладені в Договорі комплексного банківського обслуговування

1. **Порядок екстрених дій працівників компанії, з рахунків якої відбулось несанкціоноване списання коштів**

У разі виявлення несанкціонованого переказу коштів в Системі, Клієнту (потерпілому) необхідно:

1. Негайно звернутися до підрозділу АБ «УКРГАЗБАНК» (далі – Банк), відповідального за обслуговування Рахунку (до свого обслуговуючого менеджера, контакт-центру, до працівника банківської безпеки (за необхідності тощо) по телефону або іншим доступним засобом зв’язку та:

1.1. сповістити працівника Банку про факт несанкціонованого переказу коштів;

1.2. обов’язково встановити та занотувати ПІБ, посаду працівника Банку, до якого Клієнт звертався у зв’язку з фактом несанкціонованого переказу коштів в Системі;

1.3. вимагати термінового блокування доступу будь-яких користувачів до свого Рахунку через Систему;

* 1. вимагати призупинення виконання платежу;

1.5. клопотати про повернення коштів (якщо вони ще не зараховані на рахунок отримувача).

2. Відключити комп’ютер від Системи, знеструмивши його (примусово відключити електроживлення в обхід штатної процедури завершення роботи, витягти всі акумуляторні батареї з ноутбука, від’єднати шнур живлення). Якщо робота з Системою виконується через віддалений доступ, необхідно завершити сесію.

3. Негайно сповістити IT підрозділ та внутрішню службу безпеки своєї компанії та/або керівника про інцидент, в разі наявності таких підрозділів та/або такої особи та узгодити свої подальші дії, що наведені нижче у цьому документі.

4. Узгодити із внутрішньою службою безпеки або керівником виклик працівників МВС,за наявності такого підрозділу.

5. Провести фотографування комп’ютера (з підключеними кабелями та іншими периферійними пристроями), робочого місця і його розташування в приміщенні.

6. Забезпечити збереження (цілісність) комп’ютера як можливого засобу вчинення злочину, помістивши його в місце з обмеженим доступом, забезпечивши при цьому захист від розбирання (стікери, наклейки, пластилін, мастична печатка, пломби тощо) і по можливості зафіксувати засоби контролю цілісності фотографуванням з усіх ракурсів. Обов’язково забезпечити захист від ввімкнення комп’ютера, запломбувавши роз’єм живлення, а ноутбук додатково захистити від встановлення батареї. Якщо дозволяють розміри комп’ютера, слід помістити його в непрозорий пакет (мішок) і заклеїти горловину. Для забезпечення безперервності ведення діяльності – задіяти інший комп’ютер.

7. В обов’язковому порядку звернутися в Банк з письмовою заявою про відкликання платежу, повернення коштів і блокування доступу до Системи, а також про компрометацію ключів ЕП і необхідність їх блокування, перегенерації та зміни паролю (закритого ключа). Для оперативності копія заяви може бути попередньо спрямована в Банк факсом або електронною поштою (скановану копію). Оригінал заяви повинен бути наданий до Банку до кінця робочого дня.

8. Забезпечити збереження і незмінність записів за максимальний період часу, як до так і після дати здійснення несанкціонованого переказу:

з внутрішніх та зовнішніх камер систем відеоспостереження;

з журналів систем контролю доступу;

з засобів забезпечення та розмежування доступу в мережу Інтернет;

з журналу систем оновлення програмного забезпечення;

з журналів антивірусних систем;

з журналів систем упередження та виявлення мережевих вторгнень.

9. Провести збір записів з наступних джерел та передати записи слідчому з метою допомоги розслідуванню:

з міжмережевих екранів і інших засобів захисту інформації;

з серверів баз даних та інших компонент клієнтського додатку Системи;

з систем авторизації користувачів (AD, NDS і т.д.);

з комунікаційного обладнання (включаючи АТС);

з комп’ютерів, що використовуються для управління грошовими коштами через Систему;

з пристроїв, які можуть використовуватися для віддаленого управління зазначеними комп'ютерами;

електронну пошту користувачів зазначених комп’ютерів.

10. За можливості отримати у Банку додаткову інформацію та передати її слідчому з метою сприяння у проведенні розслідування:

копію журналу підключень до Системи із зазначенням ІР-адреси та часу підключення;

іншу вичерпну інформацію щодо несанкціонованого списання коштів: час та номер транзакції, реквізити отримувача, суму переведення тощо.

11. Рекомендовано, оперативно звернутися з листом (Додаток 3) до свого Інтернет - провайдера або оператора зв’язку для отримання в електронній формі журналів доступу до мережі Інтернет з електронного пристрою Клієнта або з його локальної обчислювальної мережі не менш ніж за три місяці, що передували факту несанкціонованого переказу. За наявності у провайдера будь-яких послуг із захисту клієнтів – запитати всю інформацію, яку додатково він може зібрати власними силами.

12. До здійснення слідчої дії – огляду не вживати дій для самостійного або із залученням сторонніх ІТ-фахівців пошуку і видалення комп’ютерних вірусів, відновлення працездатності комп’ютера з Системою, не відправляти комп’ютер в сервісні служби ІТ для відновлення працездатності.

13. Перед передачею комп’ютера із Системою слідчому для подальшого розслідування подати клопотання про отримання точної копії (побітової копії) жорсткого диску цього комп’ютера. Копію диску робить в ході огляду місця події слідчий або спеціаліст за його дорученням із зазначенням цього факту, зазначаючи про цей факт у протоколі. Слідчий повинен переконатися, що інформація на оригінальному диску не була ушкоджена або змінена, про що складається акт. Копію диску за можливості долучити до власного розслідування IT спеціалістами з метою виявлення інформації щодо методів та обставин здійснення несанкціонованого переказу. Результати власного розслідування доцільно передати слідчому або працівнику оперативного підрозділу у вигляді звіту в довільній формі.

1. **Порядок звернення Клієнта до правоохоронних органів та юридичні заходи щодо подальшого повернення коштів з рахунку неправомірного отримувача**

1. Клієнт (потерпілий) звертається до районного відділу внутрішніх справ (за місцем фактичного розташування офісу підприємства або підрозділу Банку) з заявою, повідомленням про вчинене кримінальне правопорушення за фактом викрадення грошових коштів (Додаток 2). Не бажано (але не заборонено) адресувати заяву до оперативних підрозділів (заяву має як найскоріше отримати саме слідчий) або УМВС, ГУМВС в областях, адже в такому разі заяву все одно скеровуватимуть до територіального підрозділу за місцем вчинення злочину (яку повинен розглянути слідчий, що має право зареєструвати її в Єдиному реєстрі досудових розслідувань). Додатково, потерпілий може інформувати будь-яким чином (факсом, електронною поштою) територіальний підрозділ боротьби з кіберзлочинністю, працівники якого зможуть підготуватись до виконання доручення слідчого та вжити можливих дій для запобігання зняття коштів.

У зверненні (заяві) необхідно зазначити:

детальні відомості про шахрайські операції: точна дата та час; сума переказів; назви, коди ЄДРПОУ/реєстраційний номер облікової картки платника податків та номери рахунків відправника та одержувача коштів; призначення платежу;

коли, ким і за яких обставин виявлено факт несанкціонованого списання коштів;

чи має потерпіле підприємство/особа договірні відносини або організаційні зв’язки з підприємством або фізичною особою, на рахунок якої перераховано кошти;

чи є у потерпілого підприємства (керівників або працівників)/особи підозри про причетність до вчинення даного злочинного посягання;

чи помічали представники потерпілого підприємства/помічала потерпіла особа збої в роботі комп’ютерної техніки протягом останнього часу;

у кого зберігаються носії інформації з ЕП доступу до Системи;

хто має доступ до комп’ютера, який використовується для роботи з Системою, хто здійснює технічне обслуговування даного комп’ютера та комп’ютерної мережі підприємства/особи в цілому;

де фактично знаходиться даний комп’ютер, яким чином він підключений до мережі Інтернет (дротовим чи бездротовим способом) чи не проводився його ремонт до або після виявлення шахрайської операції;

який Інтернет - провайдер забезпечує доступ компанії до глобальної комп’ютерної мережі.

Зазначені обставини бажано викласти в самому тексті заяви, а також долучити в якості додатків завірені копії документів: роздрукованого платіжного доручення; договору про відкриття та обслуговування банківського рахунку, з якого списано кошти; реєстраційних документів підприємства тощо. У зверненні обов’язково зазначається необхідність залучення до проведення перевірки працівників підрозділу по боротьбі з кіберзлочинністю.

До заяви про вчинення злочину від уповноваженого представника потерпілого підприємства бажано надати письмову згоду на розкриття банківської таємниці в межах, необхідних для одержання відомостей про шахрайські операції. З метою одержання необхідних для слідства відомостей відповідну заяву в подальшому слідчий долучатиме до запиту, який буде направлено до Банку.

Крім того, заявник надає на запит працівників правоохоронних органів усі можливі докази для встановлення особи та розшуку злочинців. Заявник виступає у порушеному кримінальному провадженні як потерпіла особа, та на усіх стадіях кримінального провадження дотримується положень Кримінального процесуального кодексу України.

2. Клієнт звертається до слідчого із клопотанням про направлення відповідного доручення до підрозділу по боротьбі з кіберзлочинністю у відповідному регіоні. В дорученні має бути вказано на необхідність вжиття термінових заходів щодо повернення неправомірно списаних коштів. За необхідності та за згодою Клієнта працівник департаменту банківської безпеки Банку з свого боку надає Клієнту та працівникам МВС необхідну інформаційну та організаційну підтримку.

Після отримання доручення працівниками підрозділу по боротьбі з кіберзлочинністю за місцем відкриття рахунку отримувача спільно зі працівниками департаменту банківської безпеки Банку можуть бути здійснені заходи з розшуку уповноваженого представника отримувача, виклику його до відділення Банку отримувача та здійснення ним добровільного повернення коштів зі свого рахунку на рахунок платника. Під час оформлення платежу в призначенні платежу слід вказати – повернення безпідставно отриманих коштів.

У випадку відмови здійснення добровільного повернення коштів, або якщо отримувача не знайдено, Клієнт звертається до слідчого з клопотанням про вжиття необхідних судових заходів з накладення арешту на рахунок неправомірного отримувача в рамках відкритого кримінального провадження.

3. Упродовж 24 годин після звернення до правоохоронних органів із заявою Клієнт повинен отримати Витяг про початок досудового розслідування та номер, за яким відомості про кримінальне правопорушення внесені до Єдиного реєстру досудових розслідувань, прізвище та контактні дані слідчого та, у разі необхідності, надати цю інформацію до департаменту банківської безпеки Банку.

4. Клієнт (потерпілий) за власним вибором звертається до суду з позовною заявою до неналежного одержувача грошових коштів (вказавши всі відомі реквізити одержувача) про стягнення грошових коштів, а також з клопотанням про вжиття судом заходів забезпечення позову у вигляді арешту коштів на рахунку неналежного одержувача в сумі безпідставно отриманих грошових коштів відповідно до Цивільного процесуального кодексу України чи Господарського процесуального кодексу України, або під час кримінального провадження до початку судового розгляду пред’явити цивільний позов до підозрюваних, обвинувачених осіб відповідно до ст.128 Кримінального процесуального кодексу України. Виконання рішення у вищевказаних випадках здійснюється відповідно до Закону України «Про виконавче провадження».

5. У разі наявності підстав для подання скарги на неправомірні дії або бездіяльність слідчого, оперативних працівників, яким слідчий надав доручення, необхідно звертатись до керівництва відповідного органу внутрішніх справ, або до прокуратури (за кожним кримінальним провадженням після його реєстрації в Єдиному реєстру досудових розслідувань закріплюється процесуальний керівник з числа працівників прокуратури).

Копії необхідних документів направляються Клієнтом до Банку для проведення останнім внутрішнього розслідування за фактом втручання в Систему та систем інформаційної безпеки.

Додаток 1 до Порядку дій Клієнта у випадку виявлення факту несанкціонованого переказу коштів

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(назва банку, адреса,*

*поштовий індекс)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(посада особи, П.І.Б.)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(П.І.Б. в родовому відмінку)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(*адреса, поштовий індекс,*

*інші засоби зв’язку*)

ЗАЯВА

У зв’язку з встановленням факту несанкціонованого переказу та списання коштів з рахунку (назва підприємства, ЄДРПОУ/реєстраційний номер облікової картки платника податків) № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ у сумі \_\_\_\_\_\_\_\_\_ від «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р. на рахунок № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в банку \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, призначення платежу – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, прошу відкликати вказаний платіж, повернути кошти на мій рахунок в повному обсязі та тимчасово заблокувати доступ до системи дистанційного обслуговування АБ «УКРГАЗАНК».

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (дата) \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_)

Додаток 2 до Порядку дій Клієнта у випадку виявлення факту несанкціонованого переказу коштів

\_\_\_\_\_\_\_\_ РВ УМВС України в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(*адреса, поштовий індекс*).

Потерпілий:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(П.І.Б.)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(*адреса, поштовий індекс,*

*інші засоби зв’язку*)

**ЗАЯВА (ПОВІДОМЛЕННЯ)**

**про кримінальне правопорушення за (ч. 3 ст. 190 КК України / ст. 200 КК України / ст. 361 КК України)**

Я, громадянин України \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(П.І.Б.), \_\_\_\_\_ року народження, повідомляю наступне:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (дата і час) з рахунку \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (найменування Клієнта, що збігається з найменуванням, яке заявлено в установчих документах Клієнта), №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ на рахунок \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (назва підприємства/П.І.Б. особи, ЄДРПОУ/реєстраційний номер облікової картки платника податків) №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ було переведено \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (сума, валюта), призначення платежу - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Факт несанкціонованого списання коштів було виявлено \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (П.І.Б. особи, посада) \_\_\_\_\_\_\_\_\_\_\_\_\_ (дата і час) за таких обставин: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (потерпіле підприємство/потерпіла особа) має (не має) договірні відносини/організаційні зв’язки з \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (підприємство або фізична особа, на рахунок якого/ї перераховано кошти).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (потерпіле підприємство/потерпіла особа) має (не має) підозри щодо \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (П.І.Б. особи) про причетність до вчинення даного злочинного посягання.

Представники потерпілого підприємства / фізична особа помічали/а (не помічали/а) збої в роботі комп’ютерної техніки протягом останнього часу.

При цьому носії інформації з електронно-цифровими ключами доступу до системи дистанційного обслуговування зберігаються у \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (П.І.Б. особи, посада).

Доступ до комп’ютера, який використовується для роботи з дистанційною системою віддаленого управління рахунками, мають такі особи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (П.І.Б. осіб, посади).

Технічне обслуговування відповідного комп’ютера та комп’ютерної мережі підприємства в цілому здійснює \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (П.І.Б. особи, посада).

Відповідний комп’ютер фактично знаходиться \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (адреса, конкретне місце знаходження); підключений до мережі Інтернет дротовим (бездротовим) способом; його ремонт до (після) виявлення вищезазначених операцій проводився (не проводився).

Доступ до глобальної комп’ютерної мережі Інтернет забезпечує \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (назва Інтернет - провайдера).

Вважаю, що вказані дії утворюють склад злочину, за який відповідно до \_\_\_\_\_\_\_\_\_\_\_\_\_ КК України передбачена кримінальна відповідальність.

Враховуючи викладене, відповідно до \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ КК України, на основі статей 55, 56, 214 КПК України,

ПРОШУ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_:

* прийняти мою заяву про кримінальне правопорушення за \_\_\_\_\_\_\_\_\_\_\_\_\_ КК України;
* внести відповідні відомості до Єдиного реєстру досудових розслідувань;
* невідкладно розпочати досудове розслідування у формі попереднього слідства, з підстави вчинення правопорушення, що має ознаки складу злочину, передбаченого \_\_\_\_\_\_\_\_\_\_\_\_ КК України;
* залучити до проведення перевірки вказаної інформації працівників підрозділу по боротьбі з кіберзлочинністю;
* визнати мене, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(П.І.Б.)*,* потерпілим від кримінального злочину, передбаченого \_\_\_\_\_\_\_\_\_\_\_\_ КК України;
* вручити мені пам’ятку про процесуальні права і обов’язки потерпілого;
* надати мені можливість дати додаткові свідчення;
* повідомити мене письмово, у встановленому законом порядку і строки, про початок кримінального провадження та закінчення досудового розслідування.

Зі статтями 383 «Завідомо неправдиве повідомлення про вчинення злочину», 384 «Завідомо неправдиве показання» Кримінального кодексу України, ознайомлений.

Надаю згоду на розкриття банківської таємниці під час проведення досудового розслідування в межах, необхідних для одержання відомостей про шахрайські операції.

Додатки:

* копії документів: роздрукованого платіжного доручення; договору банківського рахунку, з якого списано кошти; реєстраційних документів підприємства.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (дата) \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_)

Додаток 3 до Порядку дій Клієнта у випадку виявлення факту несанкціонованого переказу коштів

Дата вих.№

Лист до провайдера, який надає Інтернет послуги

про термінове надання інформації

*Шановний \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_!*

Відповідно до договору \_\_\_ від \_\_\_\_\_\_\_\_\_ Вашим підприємством надаються послуги доступу до мережі Інтернет за адресою \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

У зв’язку зі встановленням факту несанкціонованого втручання в роботу кінцевого обладнання (локальної обчислювальної мережі) нашого підприємства, який відбувся орієнтовно о 00:00 год. 00.00.20\_\_\_, на підставі п. 8. частини 1 ст. 32 та згідно з положеннями пп. 4, 5, 7 частини 1 ст. 39 Закону України «Про телекомунікації» прошу надати деталізовану інформацію про надані телекомунікаційні послуги з позначенням ІР-адресу, точного часу, виду та інших характеристик кожного сеансу передавання даних (термінації трафіку) за \_\_\_ місяці(в).

За наявності будь-яких послуг із захисту даних абонентів, зокрема на виконання п. 17 частини 1 ст. 39 Закону України «Про телекомунікації», прошу надати інформацію про такі послуги, а також сприяти у зборі і наданні інформації щодо вищевказаної події. У разі необхідності додаткової оплати за такі послуги прошу повідомити їх вартість, порядок і терміни надання.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Клієнт) \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_)