Інформаційний додаток
до Договору на розрахункове обслуговування за дистанційною системою

ПОРЯДОК
дій Клієнта у випадку виявлення факту несанкціонованого переказу коштів

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

У разі виявлення несанкціонованого переказу коштів в дистанційній системі (далі-Система), Клієнту необхідно:

1. Негайно звернутися до підрозділу АТ«МетаБанк» (далі – Банк), відповідального за обслуговування Рахунку (до працівника банку відповідального за ведення рахунку, контакт-центру, Управління інформаційною безпекою (за необхідності тощо) по телефону або іншим доступним засобом зв'язку (з подальшим письмовим зверненням до Банку) та:

1.1. сповістити працівника Банку про факт несанкціонованого переказу коштів;

1.2. обов'язково встановити та зафіксувати 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;

1.4. вимагати призупинення виконання платежу;

1.5. клопотати про повернення коштів (якщо вони ще не зараховані на рахунок отримувача) Додаток 1 до цього Порядку.

2. Відключити комп'ютер від Системи, 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 ІТ 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. Прийняти рішення на рівні свого підприємства про виклик працівників МВС та надання заяви (повідомлення) про кримінальне правопорушення .

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

6. Забезпечити 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, а ноутбук додатково захистити від встановлення батареї. Якщо дозволяють розміри комп'ютера, слід помістити його в 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 особистого ключа Клієнта усіх уповноважених осіб. 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(за наявністю);

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(в разі звернення з заявою до працівників МВС) з метою допомоги розслідуванню:

з міжмережевих екранів і інших засобів захисту інформації;

з серверів баз даних та інших компонентів 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. Рекомендовано, оперативно звернутися з листом (приклад у Додатку 2 до цього Порядку) 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.

11. 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.

12. В разі потреби передачі комп'ютера із Системою слідчому, для подальшого розслідування,слід 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 ІТ спеціалістами з метою виявлення інформації щодо методів та обставин здійснення несанкціонованого переказу. Результати власного розслідування (якщо таке проводилось) доцільно передати слідчому або працівнику оперативного підрозділу у вигляді звіту в довільній формі.

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

1. Клієнт 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 до органів МВС для подальшого розгляду справи слідчим з реєстрацією її в Єдиному реєстрі досудових розслідувань. Додатково, Клієнт може інформувати будь-яким чином (факсом, електронною поштою) територіальний підрозділ боротьби з кіберзлочинністю для подальшого вживання ними можливих дій по запобіганню 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 Клієнт (підприємство/уповноважена особа Клієнта) договірні відносини або організаційні зв'язки з підприємством або фізичною особою, на рахунок якої перераховано кошти;

чи є у Клієнта (керівників або працівників) підозри про причетність до вчинення даного злочинного посягання тих чи інших осіб;

чи помічали представники Клієнта збої в роботі комп'ютерної техніки протягом останнього часу;

у кого зберігаються носії інформації з доступу до Системи (носії кваліфікованого електронного підпису (КЕП);

хто має доступ до комп'ютера, який використовується для роботи з Системою, хто здійснює технічне обслуговування даного комп'ютера та комп'ютерної мережі Клієнта 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 Клієнта бажано надати письмову згоду на розкриття банківської таємниці в межах, необхідних для одержання відомостей про шахрайські операції.

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, Банк 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 з уповноваженими працівниками 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 повинно бути вказано – повернення безпідставно отриманих коштів.

У випадку відмови отримувача щодо 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 Управління інформаційної безпеки Банку.

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

Додаток 1

_____
_____
(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 та тимчасово заблокувати доступ до Системи дистанційного обслуговування АТ «МетаБанк» . Повернуті кошти зарахувати на мій рахунок в повному обсязі.

_____ (дата) _____ (_____)

Додаток 2

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 IP-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) _____ (_____)