До Офісу Генерального прокурора
01011, м. Київ, вул. Різницька, 13/15

До Департаменту кіберполіції
Національної поліції України
02000, м. Київ, вул. Боричів Тік, 8

До Слідчого управління ГУНП
в Одеській області
65014, м. Одеса, вул. Єврейська, 12

Потерпілий: **[ПІБ ПОТЕРПІЛОГО - ПРИХОВАНО]**
Паспорт: **[ДАНІ ПАСПОРТА - ПРИХОВАНО]**
РНОКПП (ІПН): **[ІПН - ПРИХОВАНО]**
Адреса: **[АДРЕСА РЕЄСТРАЦІЇ - ПРИХОВАНО]**
Телефон: **[ТЕЛЕФОН ПОТЕРПІЛОГО - ПРИХОВАНО]**

ЗАЯВА

pro vchynennya kryminalnoho pravoporushennya u skladi orhanizovanoyi hrupy
(в порядку ст. 214 КПК України)

Попередній розгляд звернень Головним управлінням Національної поліції в Одеській області (включаючи відповідь від 27.05.2026 року) було проведено поверхнево, без належного дослідження цифрових доказів та залучення профільних спеціалістів у сфері кібербезпеки. Висновок про наявність виключно «цивільно-правових відносин» є правово необґрунтованим, протиправним та таким, що прямо суперечить фактичним матеріалам справи. З боку зловмисників мав місце заздалегідь спланований, прямий умисел на заволодіння грошовими коштами в особливо великих розмірах під виглядом надання фіктивних інвестиційних послуг на платформі, що повністю виключає цивільний характер спору.

Повідомляю, що у правоохоронних органах України вже перебуває кримінальне провадження щодо аналогічних системних шахрайських дій цієї ж платформи, а саме: **ЄРДР № [НОМЕР ПРОВАДЖЕННЯ ДНІПРО - ПРИХОВАНО] від 23.05.2022 року**. Злочинна діяльність вказаної групи не припинена і є триваючою до теперішнього часу.

З огляду на вищезазначене та нововиявлені технічні дані, повідомляю про вчинення транснаціонального кіберзлочину організованою групою осіб за ознаками кримінальних правопорушень, передбачених **ч. 5 ст. 190 (Шахрайство), ч. 2 ст. 361 (Несанкціоноване втручання в роботу інформаційних (автоматизованих) систем) та ч. 2 ст. 209 (Легалізація (відмивання) майна, одержаного злочинним шляхом) Кримінального кодексу України**.

1. ОБСТАВИНИ ЗЛОЧИНУ ТА СУБ'ЄКТИВНА СТОРОНА (ОБМАН ТА ШАНТАЖ)

Залучення до фіктивного інвестиційного проекту та подальшу безпосередню координацію дій з метою виманювання коштів здійснювала особа, яка представилася вигаданим ім'ям (менеджер проекту). Даний фігурант використовував два зафіксовані канали зв'язку:

1) **Український номер стільникового зв'язку оператора: [НОМЕР ТЕЛЕФОНУ МЕНЕДЖЕРА - ПРИХОВАНО]** (використовувався для первинних дзвінків, введення в оману та координації на території України).

2) **Міжнародний акаунт у месенджері WhatsApp: [МІЖНАРОДНИЙ НОМЕР WHATSAPP +44 - ПРИХОВАНО]**, через який надходили прямі інструкції, реквізити для транзакцій, а згодом здійснювався жорсткий психологічний тиск і вимагання грошей під приводом «рятування рахунку від анулювання» та штучного блокування балансу.

Прямий кримінальний умисел фігуранта та його спільників беззаперечно підтверджується їхньою посткримінальною поведінкою. Після остаточного блокування виведення активів, згаданий менеджер надіслав цинічні текстові повідомлення, відкрито знущаючись з факту обману. Крім того, у травні 2026 року на телефон потерпілого надійшов прямий дзвінок від невстановленої особи (жіночий голос), яка здійснювала психологічний тиск та протиправно вимагала додатково **6 000 доларів США** (аудіозапис вимагання збережено), надіславши посилання на новий сторонній Telegram-канал для продовження злочинної діяльності. Офіційно зазначаю, що Національний банк України (НБУ) визнав вказану інвестиційну платформу неліцензованою фінансовою компанією.

2. ТЕХНІЧНИЙ СПОСІБ ВЧИНЕННЯ ЗЛОЧИНУ (ст. 361 ККУ)

Заволодіння активами відбулося за чітким технічним алгоритмом із використанням спеціалізованого програмного забезпечення:

- **Програма AnyDesk:** Зловмисники, використовуючи технічні ідентифікатори **[ID СЕСІЙ ANYDESK - ПРИХОВАНО]**, отримали несанкціонований віддалений доступ до комп'ютерних пристроїв для повного контролю над фінансовими операціями.
- **Програмне забезпечення XCritical Black (Android):** Під безпосереднім керівництвом фігурантів потерпілого змусили встановити цей мобільний додаток під виглядом «торговельного термінала». Встановлено, що дана програма не має відношення до реальних біржових торгів, а використовувалася виключно як інструмент візуалізації фіктивного балансу. Повний контроль над відображуваними графіками та цифрами здійснювався адміністраторами через внутрішню CRM-систему з метою введення в оману та вимагання нових грошових траншей.

3. ТРАСУВАННЯ ВИКРАДЕНИХ АКТИВІВ ТА ЛЕГАЛІЗАЦІЯ (ст. 209 ККУ)

Внаслідок серійного обману та модифікації даних було викрадено активи на загальну суму **68 000 доларів США**. Переказ коштів здійснювався у криптовалюті. Зафіксовано точний цифровий ланцюжок руху активів:

- **Транзитний гаманець зловмисників (мережа TRON): [АДРЕСА КРИПТОГАМАНЦЯ - ПРИХОВАНО]**
- **Кінцева точка виводу:** Зазначені активи шляхом розщеплення транзакцій було легалізовано через верифікований акаунт криптобіржі Binance, оформлений на підставну особу (громадянина Болгарії) через зареєстровану у Республіці Болгарія компанію-нерезидента.

4. МАСОВІСТЬ ТА СИСТЕМНІСТЬ ЗЛОЧИННОЇ СХЕМИ

Дана шахрайська група діє серійно та транснаціонально. На платформі Google Play Market зафіксовано понад 50 аналогічних детальних відгуків постраждалих громадян України (усі дані зафіксовано) за період 2024–2026 років. Усі вони описують абсолютно тотожний почерк злочину: AnyDesk → XCritical → штучне малювання збитків → шантаж. Вказаний модус операнді повністю збігається з матеріалами офіційних обшуків та ліквідації правоохоронними органами мережі шахрайських кол-центрів.

На підставі викладеного, керуючись статтями 55, 60, 98, 214, 217, 542, 543 Кримінального процесуального кодексу України, —

ПРОШУ:

1. Невідкладно (не пізніше 24 годин з моменту отримання заяви) внести відомості за даним фактом до Єдиного реєстру досудових розслідувань за ознаками кримінальних правопорушень, передбачених **ч. 5 ст. 190, ч. 2 ст. 361, ч. 2 ст. 209 КК України**, або невідкладно направити матеріали для їх об'єднання до чинного кримінального провадження за фактом діяльності даної платформи.

2. Розпочати досудове розслідування та невідкладно надати Пам'ятку про процесуальні права та обов'язки потерпілого, а також Витяг з ЄРДР.

3. Провести офіційний огляд та долучити до матеріалів провадження речові докази: відеозаписи екрана, повний цифровий експорт чату месенджера з фігурантом, а також аудіозаписи його голосу та голосу третьої особи з фактами вимагання за травень 2026 року (для проведення фоноскопічної експертизи).

4. Скерувати офіційні процесуальні запити до операторів зв'язку для встановлення осіб власників та геолокації номерів зв'язку в моменти координації дій та дзвінків вимагання.

5. В межах міжнародного співробітництва (ст. 542, 543 КПК України) ініціювати запити про правову допомогу до компетентних органів Республіки Болгарія (щодо встановлення

бенефіціара акаунта криптобіржі) та США (щодо надання логів авторизації AnyDesk та Google по вказаних ID).

Додатки до заяви:

1. Матеріали ідентифікації та ID сесій AnyDesk (Знеособлені).
2. Технічні дані блокчейн-транзакцій та адреса гаманця TRON (Знеособлені).
3. Документи трасування виводу коштів на акаунт біржі.
4. Роздруківка профілю месенджера з фактами погроз, посилань та копії повідомлень.
5. Роздруківка відгуків інших постраждалих громадян з Google Play Market (докази серійності злочину).
6. Копія офіційної відповіді ГУНП від 27.05.2026 року.

«28» травня 2026 року _____ / [Мельник В.І. - ПРИХОВАНО] /