

Warszawa, dnia 26/03/2026 r.

1001-1.024.3.2026

Wytyczne
Prokuratora Generalnego
w sprawie prowadzenia postępowań przygotowawczych
dotyczących fałszywych platform inwestycyjnych

Przestępstwa popełniane za pośrednictwem fałszywych platform inwestycyjnych to intensywnie zwiększająca się kategoria spraw, w których sprawcy przestępstw tworzą strony internetowe, kreując całkowicie nowy podmiot pozorujący działalność inwestycyjną lub podszywają się pod legalnie działające instytucje finansowe. Sprawcy wykorzystują przy tym zaawansowane techniki manipulacji bazujące na inżynierii społecznej, tworzą fałszywe reklamy z udziałem znanych osób lub podmiotów prowadzących działalność gospodarczą, fikcyjne opinie inwestorów i profesjonalnie wyglądające strony internetowe, aby wzbudzić zaufanie i nakłonić pokrzywdzonych do wpłat środków pieniężnych.

Negatywne skutki społeczne tego typu przestępczości są bardzo poważne i wielowymiarowe: pokrzywdzeni tracą duże sumy pieniędzy, tego rodzaju przestępstwa osłabiają zaufanie obywateli do rynku finansowego, instytucji inwestycyjnych, a nawet państwowych organów regulacyjnych.

Przestępstwa popełniane za pośrednictwem fałszywych platform inwestycyjnych są zróżnicowane wewnętrznie, a sposoby działania sprawców mogą odbiegać od klasycznego wprowadzenia w błąd, celem doprowadzenia innej osoby do niekorzystnego rozporządzenia mieniem. Niektóre z przestępstw wiążą się np. z przejęciem danych do logowania do bankowości elektronicznej pokrzywdzonych, instalacją na ich urządzeniach oprogramowania do zdalnego pulpitu oraz kradzieżą tożsamości. Odpowiedzialnymi za wskazaną kategorię czynów zabronionych są zorganizowane grupy przestępcze o transgranicznym charakterze, co utrudnia identyfikację sprawców i pociągnięcie ich do odpowiedzialności karnej.

Kluczowa dla skutecznego ścigania sprawców odpowiedzialnych za czyny popełniane za pośrednictwem fałszywych platform inwestycyjnych jest szybkość prowadzenia czynności procesowych oraz zabezpieczania danych i dowodów zarówno w kraju, jak również poza jego granicami. W tym celu niezbędne jest sprawne podejmowanie decyzji procesowych, albowiem każde opóźnienie może prowadzić do utraty kluczowych danych i dowodów.

Biorąc powyższe pod uwagę, działając na podstawie art. 13 § 1 ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2024 r. poz. 390 z późn. zm.), w celu podniesienia sprawności i efektywności prowadzonych postępowań przygotowawczych oraz wyeliminowania ewentualnych nieprawidłowości, przekazuję poniższe wytyczne:

1. W toku prowadzonego postępowania należy dążyć do ustalenia jaki był charakter działalności sprawcy i czy rzeczywiście dany podmiot prowadził działalność polegającą na oferowaniu produktów i usług inwestycyjnych, czy też wykorzystywał działalność gospodarczą do popełnienia przestępstw i pod pozorem dokonywania inwestycji w instrumenty pochodne, wprowadzał swoich klientów w błąd co do charakteru prowadzonej działalności, a następnie doprowadzał ich do niekorzystanego rozporządzenia mieniem, stosowanie do treści **art. 286 § 1 k.k.** albo samodzielnie dokonywał transferów środków posługując się oprogramowaniem do zdalnego pulpitu.

W przypadku ustalenia, że podmiot rzeczywiście prowadził działalność inwestycyjną, nie posiadając wymaganego przez prawo zezwolenia lub upoważnienia, należy przyjmować jako zasadniczą kwalifikację prawną z **art. 178 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi** (Dz. U. z 2024 r. poz. 722 z późn. zm.). Przepis ten wprowadza karalność nielegalnego obrotu instrumentami finansowymi w każdym aspekcie, w zakresie prowadzenia działalności bez uprawnienia, jak i z nadużyciem uprawnienia przez podmioty legalnie prowadzące działalność gospodarczą.

W sytuacji gdy w toku prowadzonego postępowania nie uzyskano dowodów na to, że przedstawiciele występującego w sprawie podmiotu prowadzili działalność inwestycyjną, a jedynie pozyskiwali środki pieniężne od pokrzywdzonych,

w celu wytransferowania ich na specjalnie przygotowane do tego rachunki bankowe lub portfele kryptowalut, takie zachowanie należy kwalifikować co do zasady **na podstawie art. 286 § 1 k.k.** (w podstawowym scenariuszu działania sprawców), **pomijając art. 178 ustawy o obrocie instrumentami finansowymi.**

2. W toku prowadzenia spraw objętych wytycznymi należy w każdym przypadku rozważyć, czy nie doszło do popełnienia w zbiegu realnym lub w ramach kumulatywnej kwalifikacji, następujących przestępstw:
 - art. 286 § 1 k.k.- przy uwzględnieniu sytuacji, gdy pokrzywdzony samodzielnie przekazuje środki na rachunek powiązany z fikcyjną platformą inwestycyjną,
 - art. 279 § 1 k.k.- jeżeli sprawcy przełamują zabezpieczenia, przejmują dane logowania do bankowości elektronicznej pokrzywdzonego i wykorzystują je do samodzielnego dokonywania transferów środków z jego rachunku,
 - art. 267 § 1 k.k. – gdy następuje przełamanie zabezpieczeń bankowości elektronicznej i uzyskanie nieuprawnionego dostępu do danych,
 - art. 287 § 1 k.k. – w przypadkach, w których sprawcy działają w celu osiągnięcia korzyści majątkowej i bez uprawnienia wpływają na automatyczne przetwarzanie danych informatycznych, w szczególności poprzez wprowadzanie nowych zapisów danych na rachunku bankowym pokrzywdzonego.
3. Wszczynając postępowanie należy każdorazowo rozważyć, czy nie zachodzą podstawy do wszczęcia śledztwa o czyn z **art. 299 § 1 k.k.**, z uwagi na to, że uzyskane od pokrzywdzonych środki pieniężne, są następnie transferowane na kolejne przygotowane do tego rachunki bankowe lub portfele kryptowalut lub podejmowane są inne czynności mające na celu udaremnienie lub znaczne utrudnienie stwierdzenia ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycia, zajęcia albo orzeczenia przepadku. W sprawie należy równolegle prowadzić, bez zbędnej zwłoki, czynności dowodowe zarówno w kierunku dokumentowania procesowego czynów bazowych, jak i działań następnych sprawców w kontekście zaistnienia przestępstwa z art. 299 k.k.

4. W zależności od sposobów działania sprawców zachodzi konieczność rozważenia wyczerpania znamion innych czynów zabronionych, w szczególności:
- posługiwania się oprogramowaniem komputerowym, w celu przechwytywania haseł za pomocą aplikacji służących do zdalnego pulpitu, w ten sposób sprawcy mogą uzyskać dane logowania do bankowości elektronicznej (art. 267 § 1-3 k.k., art. 269b § 1 k.k.);
 - kradzieży tożsamości (art. 190a § 2 k.k.) – zarówno na szkodę osób, których tożsamość została wykorzystana do wytworzenia materiałów promujących fałszywą platformę inwestycyjną, w celu osiągnięcia socjotechnicznego efektu (w tym nagrań wygenerowanych przy pomocy sztucznej inteligencji), jak również na szkodę osób, które zmanipulowane przez sprawców przekazały swoje dane lub zainstalowały oprogramowanie do zdalnego pulpitu.
5. Przyjmując **zawiadomienie o przestępstwie** lub przesłuchując pokrzywdzonego w charakterze świadka, należy dążyć do wyjaśnienia wszystkich okoliczności związanych z zapoznaniem się z ofertą, rozpoczęciem inwestowania, dokonaniem opłaty za oferowane usługi lub produkty inwestycyjne, sposobem kontaktu z przedstawicielami platformy inwestycyjnej, zawartości strony internetowej, za pośrednictwem której oferowano usługi. W sytuacji, gdy kontakt z przedstawicielami platformy nastąpił za pośrednictwem strony internetowej, należy ustalić jej dokładną nazwę (adres internetowy).
6. W toku podjętych czynności w sprawie należy uzyskać od pokrzywdzonego lub zawiadamiającego wszelkiego rodzaju dokumenty, które uzyskał od przedstawicieli platformy inwestycyjnej (umowa, regulamin, certyfikaty), potwierdzające przeprowadzone transakcje oraz płatności za nie (potwierdzenia wykonania transakcji, płatności za usługi lub produkty). Kluczowe znaczenie ma zabezpieczenie raportów podsumowujących przeprowadzone transakcje (historie transakcji). Dzięki ich analizie będzie można ustalić, czy dokonane transakcje faktycznie miały miejsce (poprzez ich porównanie do historycznych wartości rynkowych w ustalonej dacie inwestycji).

7. Na wstępnym etapie należy każdorazowo dokonać sprawdzenia w publicznie dostępnych rejestrach prowadzonych przez Urząd Komisji Nadzoru Finansowego, czy występująca w sprawie platforma inwestycyjna: działa w oparciu o wymagane przez prawo zezwolenie lub upoważnienie, w dostępnym publicznie **rejestrze podmiotów nadzorowanych** (pod adresem: https://www.knf.gov.pl/podmioty/wyszukiwarka_podmiotow), jak również czy została wpisana na listę ostrzeżeń publicznych (dostępną pod adresem: https://www.knf.gov.pl/dla_konsumenta/ostrezenia_publiczne) oraz czy znajduje się na **liście ostrzeżeń zagranicznych organów nadzoru** (dostępnej pod adresem: https://www.knf.gov.pl/dla_konsumenta/ostrezenia_zagranicznych_organow_nadzoru).
8. Należy także zwrócić się do **Urzędu Komisji Nadzoru Finansowego**, w celu uzyskania szczegółowych informacji, odnoszących się do funkcjonowania ustalonej w sprawie platformy inwestycyjnej, dotyczących stwierdzenia, czy posiada zezwolenie lub upoważnienie do prowadzenia działalności w zakresie obrotu instrumentami finansowymi, czy były uprzednio składane skargi na jej działalność w zakresie obrotu instrumentami finansowymi oraz czy stwierdzono nieprawidłowości w zakresie świadczonych usług. Powyższa czynność ma **kluczowe znaczenie dla prawidłowego ukierunkowania** prowadzonych w sprawie czynności procesowych, jak również od jej wyników **uzależniony będzie dalszy** tok postępowania oraz rodzaj i charakter podejmowanych czynności procesowych w sprawie.
9. W przypadku dysponowania przez Urząd Komisji Nadzoru Finansowego informacjami lub dokumentami, na które rozciąga się obowiązek zachowania **tajemnicy zawodowej**, konieczne jest wydanie postanowienia o zwolnieniu z tajemnicy zawodowej Przewodniczącego Komisji Nadzoru Finansowego, jego Zastępców, członków Komisji Nadzoru Finansowego, albo pracowników Urzędu Komisji Nadzoru Finansowego i osób zatrudnionych w Urzędzie na podstawie odrębnych umów cywilnych. Niezbędne informacje i dokumenty na potrzeby prowadzonych postępowań, powinny być uzyskiwane również

w oparciu o porozumienie z dnia 13 stycznia 2026 r. w sprawie zasad współpracy oraz przekazywania dokumentów i informacji zawarte pomiędzy Prokuratorem Krajowym, a Przewodniczącym Komisji Nadzoru Finansowego.

10. Dokonując oceny legalności działalności ustalonej w sprawie platformy inwestycyjnej należy każdorazowo przeanalizować jej regulamin oraz umowę, w celu ustalenia, czy ich zapisy odpowiadają polskim uregulowaniom prawnym, w szczególności określonym w ustawie z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi. Podmiot świadcząc usługę maklerską na rzecz klienta detalicznego, zobligowany jest do świadczenia jej na podstawie regulaminu i umowy. Regulamin określa sposób świadczenia usługi maklerskiej na rzecz klienta, w tym prawa i obowiązki firmy inwestycyjnej z tego tytułu, a także warunki zawierania i rozwiązywania umowy. W umowie natomiast podmiot prowadzący działalność inwestycyjną powinien wskazać, w sposób niebudzący wątpliwości i niewprowadzający w błąd, jakiego rodzaju działalność maklerska będzie świadczona na rzecz klienta.
11. W przypadku instrumentów pochodnych podmiot prowadzący działalność inwestycyjną zobowiązany jest zwrócić się do potencjalnego klienta detalicznego o przedstawienie informacji w zakresie jego wiedzy i doświadczenia inwestycyjnego. Efektem tych czynności ma być ustalenie, czy instrument finansowy, świadczony na podstawie umowy, jest odpowiedni dla danego klienta. Przeprowadzenie **testu odpowiedniości** klienta ma dać odpowiedź, czy dana usługa lub instrument finansowy są dla niego odpowiednie oraz czy zdaje sobie sprawę z ryzyka związanego z przyszłymi inwestycjami. Brak przeprowadzenia testu odpowiedniości jest ważnym elementem wskazującym na to, czy dany podmiot działa zgodnie z przepisami prawa, tym samym, czy prowadzi działalność legalnie.
12. Istotnym elementem dokonywanych ustaleń winno być uzyskanie informacji o standardzie i warunkach **przekazywania informacji** klientowi. Poprawność działania podmiotu inwestycyjnego przy reklamowaniu lub promocji świadczonych usług określona została w art. 83c ust. 2 ustawy o obrocie instrumentami finansowymi, który wskazuje, by informacje upowszechnianie

przez firmę w celu reklamy i promocji oferowanych usług były rzetelne i zrozumiałe (niewprowadzające w błąd).

13. Wskazane powyżej czynności powinny doprowadzić do weryfikacji, czy uzyskane od pokrzywdzonych środki pieniężne były inwestowane, ewentualnie gdzie zostały wytransferowane. Podkreślenia wymaga fakt, iż usługi świadczone na pozagiełdowym rynku forex, **nie mają jednego miejsca obrotu**, do którego trafiają zlecenia klientów, dlatego też dane dotyczące transakcji (ich historia) mogą znajdować się na nośnikach danych, pozostających w dyspozycji osób zarządzających lub obsługujących ustaloną w sprawie platformą inwestycyjną.
14. Jeżeli środki pieniężne pokrzywdzonego zostały wytransferowane za pośrednictwem rachunków bankowych, należy uzyskać z właściwych banków informacje stanowiące **tajemnicę bankową** dotyczące ustalonych rachunków bankowych w jak najszerszym zakresie. W odniesieniu do rachunków pokrzywdzonych, już na etapie składania zawiadomienia o przestępstwie celowe jest uzyskanie od dysponenta rachunku stosownego **upoważnienia** do przekazania niezbędnych w postępowaniu informacji objętych tajemnicą bankową – stosownie do treści art. 104 ust. 3 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (Dz. U. z 2024 r. poz. 1646 z późn. zm.), co niewątpliwie wpłynie na szybkość prowadzonego postępowania. Stosownie do uregulowań tego przepisu, banku nie obowiązuje, z zastrzeżeniem ust. 4 i 4a, zachowanie tajemnicy bankowej wobec osoby, której dotyczą informacje objęte tajemnicą. Osobom trzecim informacje te mogą być ujawnione, z zastrzeżeniem art. 105, art. 106a i art. 106b wyłącznie, gdy osoba, której informacje te dotyczą, na piśmie upoważni bank do przekazania określonych informacji wskazanej przez siebie osobie lub jednostce organizacyjnej.
15. W sytuacji ustalenia, iż na rachunku bankowym powiązonym z platformą inwestycyjną znajdują się środki płatnicze wpłacone przez pokrzywdzonego, w związku z popełnionym na jego szkodę przestępstwem, należy niezwłocznie dokonać ich **blokady**, stosownie do treści art. 106a ust. 6 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe. Natomiast gdy uzyskano informację

od Generalnego Inspektora Informacji Finansowej lub gdy zachodzi podejrzenie, iż występujący w sprawie rachunek bankowy służy do **tzew. prania pieniędzy** i znajdują się na nim środki płatnicze, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, należy niezwłocznie dokonać **blokady** tych środków w oparciu o art. 86 ust. 9 i 11 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2025 r. poz. 644).

16. Jeśli środki transferowane były na **giełdy kryptowalut**, należy zwrócić się do podmiotu prowadzącego giełdę, w celu uzyskania danych dotyczących danego użytkownika – w tym danych osobowych, adresu e-mail, adresów IP logowań (wraz z numerami portów), numerów rachunków bankowych, na które dokonywano wypłat, jak również informacji dotyczących weryfikacji tożsamości użytkownika (w tym np. nagrań z wideoweryfikacji), a następnie podjąć działania mające na celu zabezpieczenie ujawnionych w sprawie kryptowalut.
17. Gdy postępowanie przygotowawcze dotyczy również czynu z art. 299 § 1 k.k. należy przekazać Generalnemu Inspektorowi Informacji Finansowej informacje, stosownie do treści art. 81 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, m.in. o wydaniu postanowienia o blokadzie rachunku lub wstrzymaniu transakcji i wszczęciu postępowania. Przekazanie informacji, następuje niezwłocznie, nie później niż w terminie 7 dni od dnia dokonania czynności. Przekazywane informacje winny w szczególności wskazywać na okoliczności dotyczące popełnienia przestępstwa, wraz ze wskazaniem posiadanych danych identyfikacyjnych osób fizycznych, osób prawnych lub jednostek organizacyjnych nieposiadających osobowości prawnej oraz sygnaturę akt. W związku z przekazanymi informacjami Generalny Inspektor Informacji Finansowej niezwłocznie informuje prokuratora o posiadaniu informacji pozostających w związku z prowadzonym postępowaniem. Tym samym, już na wstępnym etapie sprawy, można uzyskać istotne informacje o stronach transakcji finansowych, których przedmiotem są środki pokrzywdzonych oraz wykorzystywanych przez sprawców rachunkach

bankowych. Dodać należy, że Generalny Inspektor Informacji Finansowej udostępnia, na pisemny wniosek, informacje lub dokumenty, w tym informacje lub dokumenty objęte tajemnicami prawnie chronionymi, zgromadzone na podstawie przepisów ustawy, sądom i prokuratorom na potrzeby postępowania karnego (zgodnie z art. 104 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu). Natomiast w celu weryfikacji danych zawartych w zawiadomieniu o podejrzeniu popełnienia przestępstwa tzw. prania pieniędzy, prokurator może żądać od Generalnego Inspektora Informacji Finansowej udostępnienia informacji lub dokumentów, w tym informacji lub dokumentów objętych tajemnicami prawnie chronionymi (stosownie do treści art. 104 ust. 2 cyt. ustawy).

18. Dla ustalenia tożsamości osób kierujących przestępnym procederem oraz innych wykorzystywanych do prania pieniędzy rachunków bankowych celowe jest bieżące prowadzenie w toku postępowania **analizy przepływów finansowych** obejmującej w szczególności ujawnione rachunki bankowe, adresy kryptowalut oraz inne dane związane z transferami środków płatniczych lub kryptoaktywów.
19. Po ustaleniu **adresu strony internetowej**, za pośrednictwem której platforma inwestycyjna prowadzi działalność, należy dokonać niezwłocznego procesowego utrwalenia zawartości strony poprzez dokonanie oględzin. Z przeprowadzonych oględzin należy sporządzić protokół, do którego jako załącznik należy dołączyć informatyczny nośnik danych (np. płytę CD, DVD, pendrive), na którym zostanie zapisany obraz lub kopia strony internetowej wraz ze wszystkimi podstronami, obejmujący wszystkie jej funkcjonalności, dokumentująca w szczególności strukturę strony, ofertę skierowaną do klientów, regulaminy i umowy znajdujące się na stronie, rachunki demonstracyjne lub konta demo, za pośrednictwem których klienci mogą wypróbować funkcjonalność oprogramowania udostępnionego inwestorowi do działalności inwestycyjnej, linki do pobrania aplikacji do zdalnego pulpitu, jak też znajdujące się na stronie pliki tekstowe, dźwiękowe oraz video. Powyższa czynność umożliwi **zabezpieczenie materiału dowodowego** na potrzeby prowadzonego postępowania na wypadek, gdyby w jego trakcie strona przestała działać lub

została zamknięta. Czynność ta powinna objąć również strony oraz konta w mediach społecznościowych, na których reklamowana jest platforma inwestycyjna.

20. Po ustaleniu adresu strony internetowej platformy inwestycyjnej należy pozyskać dane dotyczące rejestracji nazw domenowych powiązanych z działalnością platformy oraz dane dotyczące usługi hostingowej oraz zażądać danych abonenta domeny (rejestrującego) od podmiotu prowadzącego rejestr nazw domenowych (dla domeny .pl jest to Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy (NASK)), rejestratora (pośrednika w rejestracji nazwy domenowej) i hostingodawcy. W zakresie ustaleń dotyczących podmiotu korzystającego z usługi hostingowej należy zwrócić się do dostawcy usługi hostingowej o przekazanie również pełnej kopii danych zapisanych przez sprawców w usłudze hostingowej wraz z logami połączeń.
21. W toku postępowania należy także weryfikować dane dotyczące **kampanii reklamowych**. W tym celu należy dążyć do ustalenia, gdzie prezentowane były reklamy oferujące usługi platformy inwestycyjnej, kto dokonał płatności za kampanię reklamową. Od podmiotu, z którym zawarto umowę na prowadzenie akcji reklamowej, należy uzyskać dokumenty potwierdzające zawarcie umowy, w tym rachunki, faktury lub potwierdzenia przelewów za usługi reklamowe. Na podstawie tych dokumentów będzie możliwe ustalenie danych personalnych osób, które wykupiły reklamy, a następnie zweryfikowanie ich procesowej roli w sprawie.
22. W zakresie stron fałszywych platform inwestycyjnych oraz platform, na których promowano fałszywe inwestycje, celowe jest wykorzystanie mechanizmów wskazanych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych, Dz.U. L 277 z 27.10.2022, pp. 1–102), ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513 z późn. zm.) oraz ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (t.j. Dz. U. z 2024 r. poz. 1803), mających na celu doprowadzanie

do usunięcia lub ograniczenia dostępności treści prowadzących pokrzywdzonych do utraty środków finansowych oraz reklam fałszywych platform inwestycyjnych – w tym w szczególności reklam, w których w sposób nieuprawniony wykorzystano wizerunek innych osób.

23. Po pozyskaniu danych związanych z rejestracją nazw domenowych, usługami hostingowymi, kampaniami reklamowymi, wykorzystanymi rachunkami bankowymi, kontami w kantorach kryptowalut itp., na bieżąco należy dokonywać ich analizy i żądać kolejnych danych, w tym w szczególności danych abonentów usługi poczty elektronicznej oraz zawartości kont poczty elektronicznej wykorzystywanych przez sprawców, danych abonentów usług telekomunikacyjnych w zakresie ustalonych numerów telefonów oraz adresów IP ujawnionych w logach oraz innych danych związanych z użytkowanymi przez sprawców usługami. Z uwagi na brak określonego w przepisach prawa okresu retencji danych internetowych (danych pochodzących od podmiotów świadczących usługi drogą elektroniczną tj. hostingodawców, dostawców usług poczty elektronicznej) oraz krótki okres retencji danych telekomunikacyjnych wynoszący 12 miesięcy, brak niezwłocznego zabezpieczenia danych może skutkować ich utratą i niemożnością dokonania ustaleń faktycznych. Mając na względzie powyższe, w zakresie zabezpieczania danych od podmiotów zagranicznych (np. hostingodawców, giełd kryptowalut, podmiotów świadczących usługi telekomunikacyjne), należy korzystać także z możliwości niezwłocznego zabezpieczania danych w trybie określonym art. 29 Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r. za pośrednictwem punktu kontaktowego dostępnego 24 godziny na dobę przez 7 dni w tygodniu (24/7) prowadzonego przez **Centralne Biuro Zwalczenia Cyberprzestępczości**.

24. W toku prowadzonego postępowania celowe jest również pozyskiwanie danych z dostępnych rejestrów publicznych (np. REGON, KRS), Monitora Sądowego i Gospodarczego, baz WHOIS w zakresie nazw domenowych czy ustalonych adresów IP oraz zlecanie przeprowadzenia ustaleń i analiz w oparciu o dane pozyskiwane z powszechnie dostępnych źródeł. Wykonując czynności

analityczne, w celu zweryfikowania, jaka była zawartość ustalonej w sprawie strony internetowej oraz jak ona działała w różnych przedziałach czasowych, można dokonać sprawdzenia w archiwum cyfrowym (Wayback Machine, pod adresem <https://web.archive.org>).

25. W sytuacji ustalenia, iż sprawcy przy użyciu oprogramowania do zdalnego pulpitu przeprowadzili nieuprawnione transakcje na rachunku bankowym pokrzywdzonego, w toku przesłuchania pokrzywdzonego w charakterze świadka, należy dodatkowo ustalić **numer rachunku bankowego**, do którego sprawcy uzyskali nieuprawniony dostęp, jego historię z okresu objętego przedmiotem postępowania, jak również sposób autoryzacji transakcji na rachunku.
26. Jeśli pokrzywdzony zainstalował na urządzeniu (komputerze, telefonie lub tablecie) **aplikację służącą do zdalnego pulpitu** (np. program AnyDesk lub Team Viewer), należy dokonać oględzin sprzętu elektronicznego, w celu ustalenia między innymi: jaki program do zdalnego pulpitu został zainstalowany na urządzeniu, w jakim okresie korzystano z oprogramowania, kiedy został zainstalowany, jak też wyselekcjonowania i zidentyfikowania adresów IP występujących w logach oraz danych dotyczących nawiązanego połączenia z urządzeniem. Po ustaleniu numeru ID użytkownika (nadany numer użytkownika w aplikacji) należy zażądać wydania od producenta oprogramowania danych dotyczących informacji o adresach IP występujących w logach do programu, natomiast w sytuacji wykupienia płatnych usług oprogramowania - rachunków, faktur, czy potwierdzeń przelewów za korzystanie z aplikacji.
27. W toku postępowania zasadnym jest także dążenie do ustalenia **struktury organizacyjnej podmiotu** oferującego produkty i usługi inwestycyjne, jak i mechanizmu jego funkcjonowania, w tym zidentyfikowania osób zajmujących się organizowaniem przestępczego procederu. Czynności prowadzonego postępowania powinny się również koncentrować wokół osób pośrednio biorących w nim udział, tj. konsultantów telefonicznych, którzy kontaktują

- się z pokrzywdzonymi i namawiają ich do zainwestowania środków pieniężnych za pośrednictwem ustalonej w sprawie platformy inwestycyjnej.
28. Po ustaleniu siedziby platformy inwestycyjnej lub miejsca pobytu jej przedstawicieli lub pracowników, należy dokonać **przeszukania** ustalonych lokalizacji i zażądać wydania rzeczy, mających związek z przestępstwami będącymi przedmiotem prowadzonego postępowania lub służących do ich popełnienia w postaci m.in.: komputerów, tabletów, serwerów, routerów, modemów, telefonów komórkowych, kart SIM oraz wszelkich informatycznych nośników danych. Z uwagi na stosowanie przez sprawców cyberprzestępstw szyfrowania danych należy dążyć do zabezpieczenia od tych osób włączonego komputera.
29. Podkreślenia wymaga fakt, iż obecnie działalność przestępcza związana z prowadzeniem fałszywych platform inwestycyjnych lub tzw. praniem pieniędzy ma charakter głównie **transgraniczny**, co ma istotne znaczenie dla sposobu gromadzenia materiału dowodowego. Dlatego też w toku postępowania część czynności powinna zostać wykonana odpowiednio w ramach międzynarodowej pomocy prawnej (na podstawie Europejskiego Nakazu Dochodzeniowego lub wniosku o międzynarodową pomoc prawną). W celu niezwłocznego zabezpieczania danych informatycznych należy korzystać także z Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r. Pamiętać należy, że w razie konieczności zabezpieczenia danych informatycznych i retencyjnych we wniosku o pomoc prawną należy każdorazowo uwzględnić **strefę czasową**, w której są one gromadzone. Błędne określenie czasu zdarzenia może spowodować, iż nie będzie możliwym zabezpieczenie żądanych danych lub uzyskane dane nie będą prawidłowe.
30. Każdorazowo, przed skierowaniem wniosków o międzynarodową pomoc prawną lub wydania Europejskich Nakazów Dochodzeniowych, w zakresie uzyskania danych od usługodawców, należy zweryfikować czy danych tych nie da się zabezpieczyć lub pozyskać w drodze bezpośredniej komunikacji z ustalonym w sprawie podmiotem, jego europejskim oddziałem lub przedstawicielstwem,

w szczególności z wykorzystaniem platform online służących do komunikacji pomiędzy organami ścigania, a dostawcami tego rodzaju usług (np. LERS, Kodex).

31. Z uwagi na transgraniczność, skomplikowany stan faktyczny, wielość pokrzywdzonych oraz rozmiar szkody związany z aktywnością zorganizowanych grup przestępczych odpowiedzialnych za tworzenie fałszywych platform inwestycyjnych, postępowania z tego zakresu prowadzone powinny być co najmniej na poziomie **prokuratur okręgowych** w działach do spraw cyberprzestępczości, w przypadku gdy zostały utworzone lub przez prokuratorów specjalizujących się w zwalczaniu tego rodzaju przestępczości. Prokuratorom tym należy zapewnić możliwość brania udziału w szkoleniach dotyczących problematyki cyberprzestępczości oraz transgranicznego zabezpieczania elektronicznego materiału dowodowego.
32. W przypadku ustalenia, że przedstawiciele podmiotu objętego postępowaniem, faktycznie prowadzili działalność inwestycyjną, **postępowanie należy prowadzić w kierunku przestępstwa z art. 178 ustawy z dnia 29 lipca 2005r. o obrocie instrumentami finansowymi. Jednostką właściwą rzeczowo, niezależnie od miejsca jego popełnienia, będzie Prokuratura Okręgowa w Warszawie**, zgodnie z § 1 pkt 3 rozporządzenia Ministra Sprawiedliwości z dnia 1 września 2016 r. w sprawie określenia właściwości Prokuratury Okręgowej w Warszawie w sprawach o poszczególne rodzaje przestępstw, niezależnie od miejsca ich popełnienia (t.j. Dz.U. z 2016 r. poz. 1484).
33. W sprawach szczególnie skomplikowanych podmiotowo lub przedmiotowo, **należy rozważyć zasadność powołania zespołu prokuratorów**, składającego się z prokuratorów, a także funkcjonariuszy innych służb państwa, stosowanie do treści art. 56 § 2 ustawy z dnia 28 stycznia 2016 r. Prawo o prokuraturze (Dz.U. z 2024 r. poz. 390 z późn. zm.).
34. Należy również zwrócić szczególną uwagę na kwestię prawidłowego prowadzenia tego rodzaju postępowań przygotowawczych, gdzie występuje **wielość osób pokrzywdzonych**, zaś poszczególne zawiadomienia o popełnieniu czynów związanych z działaniem ustalonej platformy, złożone zostały

w różnych jednostkach organizacyjnych prokuratury, a dotyczą tej samej platformy inwestycyjnej. Jednym postępowaniem przygotowawczym powinny zostać objęte wszystkie czyny pozostające w związku podmiotowym lub przedmiotowym z czynem stanowiącym podstawę jego wszczęcia, chyba że zachodzą okoliczności, o których mowa w art. 34 § 3 k.p.k. Gdy prowadzone postępowanie dotyczy **tej samej platformy inwestycyjnej**, zgodnie z zasadą ekonomiki procesowej, powinno obejmować **wszelkie przestępcze zachowania**, związane z jej działalnością.

35. Dla zapewnienia skutecznej koordynacji, bieżącego monitorowania oraz łączenia postępowań dotyczących tej samej platformy inwestycyjnej z wykorzystaniem systemu **PROK-SYS**, adres strony internetowej platformy powinien być bezwzględnie wskazany w opisie sprawy, czynu lub zarzutu, a postępowanie powinno być **oznaczone kategorią koordynacji „platformy inwestycyjne”** w podsystemie LIBRA. Przed rejestracją nowego postępowania dotyczącego platformy inwestycyjnej, każdorazowo należy zweryfikować przy wykorzystaniu systemu PROK-SYS, czy nie jest już prowadzone inne postępowanie pozostające w związku przedmiotowym lub podmiotowym.

36. Niniejsze wytyczne wchodzi w życie z dniem podpisania.

PROKURATOR GENERALNY

Waldemar Żurek

