Sekretariat Rady Konsultacyjnej ds. Ochrony Konsumentów

Departament Nadzoru Właścicielskiego i Gospodarki

Urząd Marszałkowski Województwa Małopolskiego

# Protokół z XXVIII posiedzenia Rady Konsultacyjnej ds. Ochrony Konsumentów z dnia 24 marca 2022 r.

W posiedzeniu wzięli udział członkowie Rady Konsultacyjnej ds. Ochrony Konsumentów (Rady) oraz zaproszeni goście: **Pani Katarzyna Urbańska**, Dyrektor Departamentu Prawnego oraz **Pan Jarosław Biegański**, Zastępca Dyrektora Zespołu Bezpieczeństwa Banków, Związek Banków Polskich, **Pan Emil Chojnacki**, Dyrektor Pionu Orzecznictwa, Izba Administracji Skarbowej w Krakowie, **Pani Dorota Grudzień-Barbachowska**, Dyrektor Departamentu Polityki Konsumenckiej, Urząd Komunikacji Elektronicznej, **Pan Waldemar Jurasz**, Dyrektor Delegatury Urzędu Ochrony Konkurencji i Konsumentów w Krakowie, **Pan Podkomisarz Dariusz Rusinek**, Specjalista Wydziału do walki z Cyberprzestępczością, Komenda Wojewódzka Policji w Krakowie. Obrady miały miejsce 24 marca 2022 roku, w godzinach 12.00-14.40, w formie wideokonferencji.

## Otwarcie posiedzenia, przyjęcie porządku obrad

**Posiedzenie otworzył Pan Andrzej Bańka** – Zastępca Dyrektora Departamentu Nadzoru Właścicielskiego i Gospodarki, który w imieniu Marszałka Województwa Małopolskiego, Pana Witolda Kozłowskiego (Przewodniczącego Rady) oraz własnym, przywitał Członków Rady oraz zaproszonych Gości, następnie przedstawił porządek obrad, który został przyjęty przez uczestników bez uwag.

**Pan Andrzej Bańka** przypomniał o obchodzonym w dniu 15 marca Światowym Dniu Konsumenta, znanym też jako Światowy Dzień Praw Konsumenta. Po raz pierwszy obchody Światowego Dnia Konsumenta odbyły się w 1983 roku w rocznicę przemówienia prezydenta Johna F. Kennedy’ego, wygłoszonego w roku 1962 w Kongresie Stanów Zjednoczonych. Dotyczyło ono projektu ustawy o ochronie praw konsumenta. Wówczas prezydent USA sformułował cztery podstawowe prawa konsumentów: do informacji, do wyboru, do bezpieczeństwa, do reprezentacji. Z jego ust padło też stwierdzenie: „Konsumenci to my wszyscy”. W Polsce Światowy Dzień Konsumenta obchodzony jest oficjalnie od roku 2000. Do obchodów włącza się Urząd Ochrony Konkurencji i Konsumentów
i organizacje pozarządowe.

Następnie **Pan Andrzej Bańka** przedstawił tematy spotkania tj.: Zakupy towarów przez Internet w ramach tzw. dropshippingu oraz Oszustwa internetowe w bankowości elektronicznej, a w dalszej kolejności przekazał prowadzenie spotkania Panu Jerzemu Gramatyce, Miejskiemu Rzecznikowi Konsumentów w Krakowie, Wiceprzewodniczącemu Rady.

**Pan Jerzy Gramatyka** na wstępie przypomniał, że dwuletni okres pandemii poskutkował niezwykle dynamicznym wzrostem w sprzedaży e-commerce na świecie (w latach 2019-2020 wzrost o 30 %). Podkreślił istotną rolę umów zawieranych przy pomocy środków na odległość, niezwykle wygodnych i korzystnych, ale niosących też ryzyko. Mowa o dropshippingu. Dropshipping to model logistyczny wykorzystywany w sprzedaży przez internet polegający na przeniesieniu procesu wysyłki towaru na dostawcę. Rola sklepu internetowego w tym modelu logistycznym sprowadza się do zbierania zamówień i przesyłania ich do dostawcy, który realizuje wysyłkę towaru do klienta. W przypadku dropshippingu ma miejsce duża skala nadużyć w zakresie przestrzegania praw konsumenta. Zdiagnozowany problem to udawanie przez pośredników internetowych sprzedawców, podczas gdy faktycznie towar jest nabywany od sprzedających z krajów głównie Dalekiego Wschodu, czego konsekwencją są zarówno ukryte opłaty (cła, akcyza), problemy związane ze złożeniem reklamacji (z tytułu rękojmi czy gwarancji) często znacznie wydłużające tę procedurę oraz ograniczanie prawa do odstąpienia od umowy. Stosownie do treści art. 27 ustawy z dnia 30.05.2014 r. o prawach konsumenta (Dz. U. z 2014 r. poz. 827 ze zm.) konsument, który nabył towar za pomocą środków porozumiewania się na odległość np. przez Internet, nabywa także prawo do bezwarunkowego i bezkosztowego odstąpienia od umowy. Podstawowym prawem konsumenta jest prawo do informacji nie wprowadzającej go w błąd, która ma umożliwić dokonanie świadomego i racjonalnego wyboru co do podmiotu, z którym zawiera umowę oraz celu jakim jest przedmiot zawartej umowy. Pan Jerzy Gramatyka dodał także, że przy okazji takich płatności pojawia się dodatkowe ryzyko związane z oszustwami internetowymi w bankowości elektronicznej. W skali roku odnotowuje się kilkanaście tysięcy naruszeń w zakresie dropshippingu.

Następnie **Pan Jerzy Gramatyka** przekazał głos zaproszonym **Gościom.**

## Wystąpienia i dyskusja dotycząca tematu posiedzenia

**Pan Jerzy Gramatyka** poprosił o wypowiedzi zaproszonych gości, rozpoczynając od Pani **Katarzyny Urbańskiej**, Dyrektor Departamentu Prawnego oraz **Pana Jarosława Biegańskiego**, Zastępcy Dyrektora Zespołu Bezpieczeństwa Banków ze Związku Banków Polskich (ZBP).

**Pan Jarosław Biegański** w swej wypowiedzi odniósł się do doświadczeń bankowego centrum cyberbezpieczeństwa ZBP oraz pracy w Grupie Allegro:

1. Najważniejszą sprawą przy dropshippingu jest świadomość kupującego, że dokonuje zakupu np. w Chinach;
2. Należy korzystać ze sprawdzonych platform sprzedażowych, gdzie dostawca usługi (administrator platformy sprzedażowej) weryfikuje czy sprzedający jest podmiotem mającym prawo działać na terenie Polski;
3. Istnieją specjalne programy ochrony kupujących pozwalające odzyskać środki od platformy sprzedażowej, w przypadku gdy kupujący zostanie wprowadzony w błąd przez sprzedawcę. Swoje roszczenia należy zgłaszać zarówno do dostawcy płatności, jak i platformy sprzedażowej;
4. Platformy sprzedażowe (np. Allegro) stosują procedurę, w ramach AML’a– przeciwdziałania praniu brudnych pieniędzy, zwaną „on boarding” (poznaj swojego klienta), której celem jest weryfikacja sprzedawców realizujących swe usługi na danej platformie sprzedażowej.
5. W dropshippingu, sprzedający powinien poinformować klienta o przewidywanym terminie dostawy towaru w momencie jego zakupu.
6. Największym problemem, który pojawia się w ramach cyberprzestępczości to ryzyko dostawcy. W takich przypadkach należy korzystać z odpowiednich instrumentów płatniczych. Warto korzystać ze sklepów, które mają podpisaną umowę z polskim agentem rozliczeniowym, który oferuje płatności kartami lub innymi metodami płatniczymi typu przelew ekspresowy Blik czy PayPall link.
7. Zasada jest taka, że to agent rozliczeniowy np. FirstData, PayYou, Pekao SA, zanim podpisze umowę ze sprzedawcą, wcześniej go zweryfikuje, co jest gwarancją dla klienta, że sprzedawca działa w określonym reżimie (zgodnym z regulacjami VISA, MasterCard).
8. W kontekście cyberbezpieczeństwa, jeżeli konsument poda numer karty fałszywemu sklepowi internetowemu, istnieje ryzyko, że jego dane w sposób niekontrolowany mogą zostać wykorzystane. Na tą okoliczność działają usługi silnego uwierzytelnienia tzw. 3D secure. Dodatkowo, dzięki korzystaniu przez konsumenta z karty płatniczej przy dokonywaniu transakcji, konsument zostaje objęty ochroną chargé back (obciążenie zwrotne). Wówczas, jeśli towar nie zostanie dostarczony lub jest niezgodny z umową, konsument może zwrócić się do banku - wydawcy karty, o usługę chargé back, podając przyczynę np. towar niedostarczony. W oparciu o tę usługę środki zostaną konsumentowi zwrócone.
9. Ważne jest aby świadomie podejmować decyzje o sposobie zapłaty. Przy płatności przelewem, Blikiem, konsument nie eksponuje numeru karty płatniczej na poznanie przez osobę nieuprawnioną, ale też nie jest objęty ochroną chargé back, gdyż ta usługa obejmuje wyłącznie płatności kartowe.

W odpowiedzi na pytanie Pana Andrzeja Bańki o niechęć banków do uruchamiania usługi chargé back, opierając się na własnych doświadczeniach, Pan Jarosław Barański stwierdził, że nie identyfikuje powyższych problemów.

Kolejno głos zabrała Pani **Katarzyna Urbańska**, Dyrektor Departamentu Prawnego, która w uzupełnieniu do odpowiedzi na pytanie Pana Bańki dodała, że problem dotyczy autoryzowanych
i nieautoryzowanych transakcji. Charge back dotyczy kart kredytowych. Jeśli klient zlecił transakcję bankowi i ją potwierdził, następnie okazała się oszustwem, wówczas znacznie trudniej jest odzyskać środki, gdyż transakcja była autoryzowana przez klienta i na nim spoczywa cała odpowiedzialność. Dodatkowo Pan Biegański poinformował, że regulacje europejskie PSD2 również obejmują RTS-y tj. standardy techniczne dla przeprowadzania transakcji, które mówią kiedy podmiot może zrezygnować z silnego uwierzytelnienia. Co oznacza, że podmiot, który rezygnuje z silnego uwierzytelnienia (np. platforma sprzedażowa typu Allegro czyli dostawca płatności, na której odbywają się transakcje handlowe) bierze na siebie ryzyko finansowe. Poza konsumentem zapada decyzja czy transakcja jest silnie uwierzytelniona czy też nie. Jeśli nie jest silnie uwierzytelniona, konsument powinien w łatwy sposób te pieniądze odzyskać.

Kolejno głos w omawianym temacie zabrał **Pan Emil Chojnacki,** **Dyrektor Pionu Orzecznictwa, Izba Administracji Skarbowej w Krakowie,** który odniósł się do dropshippingu od strony podatkowej. Zjawisko to pojawiło się w interpretacjach podatkowych Krajowej Informacji Podatkowej już kilka lat temu. Rzeczywistość dropshippingu i handlu e-commerce zmieniła się w dniu 1 lipca 2021 r. w związku ze zmianą przepisów o podatku VAT dot. opodatkowania przesyłek o niskiej wartości, które przychodziły najczęściej z Chin, ale także od podmiotów chińskich z terenu UE. Z punktu widzenia podatkowego najistotniejsze to, kim są strony transakcji. Najczęstszym przypadkiem, który występuje w dropshippingu (dostarczanych drobnych przesyłkach) to model pośrednictwa. W modelu tym nigdy nie dochodzi do nabycia prawa do rozporządzania rzeczą jako właściciel po stronie sprzedawcy np. na Allegro. To ma poważne implikacje podatkowe, ponieważ często kupujący nie wiedzą, że ten nabywca nie płaci ani podatku VAT, ani ewentualnych należności celnych. Należności celne oraz tzw. VAT importowy obciążają tego kto jest „importerem na Allegro”, czyli konsumenta – osobę fizyczną, która kupuje na Allegro.

Pośrednik rozlicza się od kwoty prowizji, którą sobie potrącił za realizację zamówienia od podmiotu np. z Hongkongu. Do 1 lipca 2021 r. obowiązywało zwolnienie z podatku VAT dla niskich kwot (do 22 euro), zwolnienie celne (do 150 euro) stąd rzadko kiedy te paczki były kontrolowane przez urzędy celne. Pakiet e-commerce, który wszedł w życie w lipcu 2021 r. bardzo zmienił sposób opodatkowania tych transakcji wprowadzając na platformy sprzedażowe obowiązek naliczania podatku od przesyłek, które były sprzedawane przez np. podmioty chińskie. Druga rzecz, która się zmieniła dotyczy przesyłek drobniejszych (do 150 euro) z Azji. Poczta i inni operatorzy tacy jak DHL mają obowiązek same przedstawić te przesyłki do odprawy celnej, a następnie pobrać od adresata przesyłki naliczony podatek VAT. Były próby ze strony administracji skarbowej potraktowania pośredników jak sprzedawców, gdyż w skrajnych przypadkach zachowują się tak jak sprzedawcy. Nie przyniosły one jednak oczekiwanego rezultatu. W wyniku rozstrzygnięć sądów administracyjnych, model dropshippingu powinien być opodatkowany analogicznie jak stosowany jest w opodatkowaniu pośrednika. Pierwsze analizy KE obejmujący półrocze od 1 lipca 2021 r. pokazują wiele korzyści dla budżetów poszczególnych państw wynikających z opodatkowania przesyłek z Azji. **Pan Jerzy Gramatyka** zapytał o statystykę w zakresie liczby zgłoszeń konsumenckich dot. uiszczenia ceł/podatku. W odpowiedzi Pan Emil Chojnacki w przybliżeniu podał liczbę milionów przesyłek. Kwota 1,8 mld euro to suma wpływów wynikających z wpływów z opodatkowania przesyłek w ramach modelu dropshippingu i handlu e-commerce.

Kolejno głos zabrała **Pani Dorota Grudzień-Barbachowska**, Dyrektor Departamentu Polityki Konsumenckiej, Urząd Komunikacji Elektronicznej, która na wstępie przedstawiła rolę UKE (głównie legislacja konsumencka), a także podkreśliła potrzebę rozwijania świadomości konsumenckiej, edukacji w zakresie możliwych narzędzi, nowych technologii, które powinny być bazą dla umiejętności korzystania z usług takich jak dropshipping, bankowość elektroniczna, administracja cyfrowa. UKE adresuje swoje usługi edukacyjne, w tym w zakresie zagrożeń w obszarze rynku usług cyfrowych, do wszystkich grup wiekowych (od dzieci po seniorów).

* Phishing – oszustwo polegające na wyłudzeniu osobistych, istotnych danych (login, hasło, numer karty płatniczej itp.), podszywanie się pod instytucje dobrze znane ofiarom (bank, urząd, dostawca usług).
* Vishing – voice + phishing, wyłudzenie danych z wykorzystaniem połączeń głosowych, podszywanie się pod pracowników banków, urzędów lub przedstawicieli handlowych, wyłudzanie kodów BLIK.
* Smishing – sms + phishing – czyli oszustwo na SMS-a, kradzież z wykorzystaniem spreparowanych wiadomości SMS, podszywanie się pod instytucje przez edycję pola „nadawca”, groźniejszy niż phishing z wykorzystaniem e-mail.
* Najczęściej atakowane domeny zarejestrowane od 2020 r. : FB, OLX, Orlen, InPost, inne, Onet, PGE, TVN, TESLA, PGNiG (źródło: CERT).
* UKE przygotowało trzy kursy edukacyjne dla konsumentów: Bankowość on-line, Zakupy w internecie, Sprawy urzędowe przez internet, a także jest w trakcie opracowywania gry symulacyjnej skierowanej do młodszego pokolenia (6-8 klasa szkoły podst.) pt. Nie daj się złapać! Cele dydaktyczne gry to m.in.:
* Zapoznanie się z pojęciem phishingu;
* Znajomość zasad postępowania w przypadku natrafienia na zainfekowane pliki w sieci;
* Zapoznanie z zasadami bezpieczeństwa związanymi z płatnościami w internecie
* Wiedza nt. udostępniania danych osobowych w sieci.

Pani Dyrektor podkreśliła rolę organów administracji publicznej we włączanie się w akcje edukacji konsumenckiej, szczególnie adresowanej do seniorów i młodego pokolenia.

 **Pan Jerzy Gramatyka** przed oddaniem głosu kolejnemu mówcy, odniósł się do analizy raportu dotyczącego transakcji płatniczych opublikowanego przez Rzecznika Finansowego za 2020 r. Z szacunków opartych o dostarczone dane wynika, że w skali rynku do banków trafia od 15 do 18 tysięcy zgłoszeń miesięcznie, dotyczących nieautoryzowanych transakcji. Co wynika także z niniejszego raportu, to utrzymywanie przez część banków niezgodnych z prawem procedur działania w zakresie nierealizowania przez banki obowiązków wynikających z treści przepisów. W szczególności dotyczy to nieprzestrzegania terminu zwrotu środków na konto klienta wynikających z nieautoryzowanych transakcji, co powinno nastąpić kolejnego dnia roboczego po dniu zaistnienia nieautoryzowanej transakcji lub po dniu zgłoszenia tego przez klienta (zasada D+1). Wyjątkiem odstąpienia od tej zasady są tu należycie udokumentowane próby oszustwa ze strony klienta banku. Ciężar dowodu spoczywa w tym zakresie na banku. Bank powinien oddać klientowi pieniądze i jeśli posiada uzasadnione podejrzenie, że klient w całości lub części odpowiada za nieautoryzowane transakcje, powinien dochodzić tej kwoty od klienta w postępowaniu regresowym przed sądem. Część banków wdrożyła te procedury i stosuje je w 90%. Dla wielu podmiotów jest to nadal odsetek zwrotów jednocyfrowy. Oznacza to, że w bardzo wielu przypadkach nie zwracają one pieniędzy na konto klienta w terminie D+1 od dnia zgłoszenia.

Do wypowiedzi Pana Jerzego Gramatyki odniosła się **Pani Katarzyna Urbańska ze ZBP**, która zwróciła uwagę na następujące kwestie. Dyrektywa PSD1 i PSD2 zostały źle zaimplementowane do polskiego porządku krajowego, co przełożyło się na słabą jakość przepisów o usługach płatniczych. ZBP jest w toku procesu legislacyjnego naprawiającego te błędy, co wpłynie na poprawę praktyki stosowanej obecnie przez banki (dot. przepisów o usługach płatniczych, tak aby odzwierciedlały przepisy dyrektywy PSD1 i PSD2).

Następnie Pan Jerzy Gramatyka przekazał głos Panu **Waldemarowi Juraszowi**, **Dyrektorowi Delegatury Urzędu Ochrony Konkurencji i Konsumentów w Krakowie**, z prośbą o informację nt. podejmowanych przez UOKIK działań w omawianym zakresie. Pan Waldemar Jurasz omówił specyfikę 3 modeli dropshippingu:

1. Sklep internetowy występuje jako sprzedawca, natomiast podmiot z krajów azjatyckich występuje jako dostawca towaru – model najbardziej optymalny dla konsumenta, ponieważ może on dochodzić wszystkich swoich uprawnień wynikających ze sprzedaży towaru;
2. Pośrednik, który działa w imieniu i na rzecz kupującego - w regulaminie określa on, jakie obowiązki przyjmuje na siebie. Zdarza się, że obowiązki przyjmuje w całym zakresie tj. zachowuje się jak sprzedawca lub przyjmuje część obowiązków sprzedawcy (np. przyjmuje od klienta towar z tytułu reklamacji, natomiast nie przyjmuje towaru z tytułu odstąpienia od umowy);
3. Pośrednik ogranicza się wyłącznie do roli pośrednika – najbardziej niebezpieczna sytuacja dla konsumenta, z uwagi na fakt, że bardzo często w swoim regulaminie wyłącza wszelkie obowiązki jakie ciążą na sprzedawcy.

Każdy z tych modeli jest dopuszczalny, pod warunkiem, że konsument otrzyma pełną informację jak działa dany sklep internetowy. Odwołując się do wypowiedzi **Pani Grudzień-Barbachowskiej**, **Pan Waldemar Jurasz** podkreślił rolę edukacji i świadomości konsumenckiej, która pomaga w wychwyceniu, z którym modelem dropshippingu kupujący ma do czynienia. W każdym przypadku pośrednik-sprzedawca powinien przekazywać konsumentowi ściśle określone informacje na podstawie ustawy o prawach konsumenta. W przypadku modelu 3., powinien informować o danych prawdziwego sprzedawcy. **Pan Waldemar Jurasz** odnotowuje niewielką ilość zgłoszeń do UOKIK ze strony konsumentów dotyczących naruszeń w dropshippingu – 37 skarg na przestrzeni lat 2020-2022. Działania podjęte przez UOKIK w tym okresie:

- urząd skierował do podmiotów działających w modelu dropshippingu 8 wystąpień „miękkich” na podstawie art. 49 Ustawy o ochronie konkurencji i konsumentów (prowadzenie mniej sformalizowanych działań poza postępowaniami wyjaśniającymi), co przyniosło pozytywny skutek jeśli chodzi o reakcję podmiotów działających w modelu dropshippingu, przeprowadził jedno postępowanie wyjaśniające oraz wydał jedną decyzję.

Najczęstsze naruszenia podmiotów działających w modelu dropshippingu zdiagnozowanych przez UOKIK:

* Wprowadzające w błąd informacje na stronie internetowej (sugerowanie klientom, że sklep internetowy jest sprzedawcą towarów a nie pośrednikiem);
* Nieprzekazywanie przed zawarciem umowy wymaganych prawem informacji o tym kto jest sprzedawcą;
* Nieprzekazywanie informacji komu zwrócić towar w razie odstąpienia od umowy;
* Ograniczanie możliwości zwrotu towaru poprzez np. tylko w oryginalnym opakowaniu;
* Nieprzekazywanie pełnej informacji o cenie towaru tj. pomijanie informacji o konieczności poniesienia opłaty cłowej/podatku VAT.

 Dodatkowo **Pan Waldemar Jurasz** poinformował o prowadzonej przez Prezesa UOKIK współpracy z platformą Allegro, która pozwala skutecznie ograniczać niedozwolone czynności przez podmioty działające w modelu dropshippingu. Ponadto UOKIK prowadzi działania edukacyjne poprzez stronę [www.konsument.edu.pl](http://www.konsument.edu.pl). W kwestii procedury chargé back Pan Waldemar Jurasz poinformował, że UOKIK nie odnotowuje zgłoszeń reklamacyjnych związanych z tą procedurą. W odniesieniu do nieautoryzowanych transakcji, zaznaczył, że do UOKIK, w tym delegatury w Krakowie, wpływa tysiące skarg konsumenckich związanych z wyłączeniem odpowiedzialności banków i innych naruszeń w tym obszarze. Prezes UOKIK prowadzi 18 postępowań wyjaśniających przeciwko wszystkim bankom komercyjnym w Polsce.

**Pan Podkomisarz Dariusz Rusinek**, Specjalista Wydziału do walki z Cyberprzestępczością z Komendy Wojewódzkiej Policji w Krakowie na początku swej wypowiedzi skupił się na oszustwach internetowych w bankowości elektronicznej. Przytoczone dane statystyczne z trzeciego kwartału 2021 roku – istnieje 16 mln kont internetowych w bankach, 21 mln osób loguje się do bankowości internetowej co najmniej raz w miesiącu. Płatności kartą to 64% ogółu płatności; 22% stanowi gotówka; bankowość internetowa – 7%; W kontekście dropshippingu istotnym problemem jest podszywanie się pod sklepy internetowe. Ten proceder dotyczy także podszywania się pod strony banków, pośredników płatności występujących na rynku przelewów. Okres działalności podszywających się sklepów internetowych to około miesiąca, następnie ich aktywność jest wygaszana. Ma to na celu zgromadzenie jak największej liczby klientów, którzy po dokonaniu opłaty za zakupiony towar, nie otrzymują go, a sklep internetowy przestaje istnieć. Grupy przestępcze działają w sposób zorganizowany tj. są osoby odpowiedzialne za grafikę, copyrighting. W celu uwiarygodnienia swej działalności zajmują się wsparciem dla tych sklepów, obsługą klienta. Pan Podkomisarz przytoczył także inne przykłady oszustw:

* Kopiowanie kart bankomatowych – proceder screeningu, coraz mniej opłacalny dla przestępców w naszym kraju, dość powszechny w krajach Dalekiego Wschodu;
* W zakresie płatności internetowej – współpraca międzynarodowa organów ścigania w wykrywaniu przestępstw, których charakter nie ma granic, z uwagi na obszar aktywności w przestrzeni wirtualnej;
* Facebook – oszustwa typu „wyłudzenia na blika” – polegające na przejęciu konta, a następnie rozsyłaniu z tego konta wiadomości z prośbą o pożyczkę pieniędzy;
* Strony internetowe udające związek z pośrednikiem płatności – podszywanie się pod agentów rozliczeniowych jak np. PayU, zakładanie bliźniaczo podobnych stron do tych utworzonych przez podmioty będące pośrednikami płatności;
* Płatność z urządzeń tj. telefonów, zegarków poprzez formę zbliżeniową;
* Phishing, smishing, o których była mowa wcześniej – należy bardzo uważać w jakie linki klikamy;
* Platformy inwestycyjne w kryptowaluty – schemat telefonów zachęcających w inwestycje w kryptowaluty. „Opiekun klienta” podczas miesięcznego szkolenia nt. inwestycji kryptowalutowych, a także w giełdy towarowe, uczy inwestowania, poruszania się na tym obszarze. Następnie „uczniowie” rozpoczynają samodzielne inwestycje, przelewając na platformy inwestycyjne środki na zakup kryptowalut za pośrednictwem dedykowanych aplikacji. Transfery środków odbywają się poza systemem bankowym i często trafiają w ręce przestępców.

Pan Podkomisarz poinformował słuchaczy o prowadzonych przez Komendę Policji działaniach prewencyjnych, organizowanych w szkołach, na festynach, których celem jest uświadomienie społeczeństwa o zagrożeniach istniejących w cyberprzestrzeni oraz jak się przed nimi chronić.

**Pan Jan Wantuch, UKE, Dyrektor Delegatury w Krakowie**, tytułem uzupełnienia wypowiedzi przedmówców, zwrócił uwagę na kwestię nadzoru rynku wyrobów, którym zajmuje się Prezes UKE. W tym przypadku może występować kwestia odpowiedzialności za wprowadzenie do obrotu wyrobu niezgodnego z dyrektywami unijnymi. Poprzez zakup takiego produktu bezpośrednio u producenta, który znajduje się poza obszarem UE, odpowiedzialność spada na konsumenta, który produkt nabył. Odpowiedzialność konsumenta za ten zakup może zostać wyciągnięta długi czas po zakupie. Jeśli okaże się, że produkt nie spełnia norm UE (w wyniku inspekcji), nie może być przez konsumenta użytkowany.

Na zakończenie spotkania **Pan Jerzy Gramatyka** oraz **Pan Andrzej Bańka** podziękowali wszystkim za udział, a także zachęcili do dalszej aktywności w ramach Rady.

 **Jerzy Gramatyka**

 Wiceprzewodniczący Rady Konsultacyjnej ds. Ochrony Konsumentów

Protokół sporządziła:

Joanna Domańska

Departament Nadzoru Właścicielskiego i Gospodarki

Urząd Marszałkowski Województwa Małopolskiego