Ján Šanta, Ivo Šanta, Matúš Husák

Trestný čin neoprávneného vyrobenia a používania platobného prostriedku – aktuálna právna úprava a aplikačná prax

Anotácia: V predmetnom príspevku jeho autori pozornosť zameriavajú na aktuálny fenomén platobných prostriedkov s dôrazom na platobné karty. V súvislosti s nimi popisujú východiskovú právnu úpravu, a to rámcové rozhodnutie 2001/413/SVV o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov, Trestný zákon a zákon č. 492/2009 Z. z. o platobných službách v znení neskorších predpisov. Analyzujú tiež konkrétne spôsoby páchania trestnej činnosti súvisiacej s platobnými prostriedkami v SR a v zahraničí. Orientujú sa tak na represívne, ale aj na preventívne aspekty danej problematiky.

Kľúčové slová: platobný prostriedok, platobná karta, neoprávnená výroba, držba, krádež, podvod, skimming.

Úvod

Počet platieb mobilom, hodinkami a ďalšou nositeľnou elektronikou sa za posledné tri roky strojnásobil. Vďaka technológii tokenizácie dnes dokážeme vytvárať digitálne odtlačky platobných kariet prakticky v akomkoľvek zariadení a navyše využívanie tokenov ešte viac posilňuje bezpečnosť transakcie tým, že v nej vôbec nefiguruje reálne číslo karty.

Niektoré banky pôsobiace v Slovenskej republike v súčasnosti v spolupráci s *Mastercard* a *Niceboy* uvádzajú na slovenský trh platobné náramky, ktoré umožňujú pohodlné a bezpečné platenie bez peňaženky či mobilu. Platobné náramky *Niceboy* sa nikdy nevybijú, sú vodotesné a v prípade straty je možné ich jednoducho deaktivovať prostredníctvom aplikácie v mobilnom telefóne. Svojim majiteľom poskytujú istotu, že budú mať svoje finančné prostriedky kedykoľvek je to potrebné. Náramky fungujú iba s platobnými kartami *Mastercard* vydanými konkrétnou bankou.

Platobné náramky tak po prsteňoch predstavujú ďalší výrazný krok v tomto vývoji. Ide tak o unikátny produkt, ktorý v sebe spája funkčnosť, technológie a exkluzivitu.[1]

Tieto a ďalšie zmeny v oblasti platobných kariet, ktoré sa pripravujú v súčasnosti, radikálne zmenia spôsoby, akými platíme za tovary a služby v online prostredí. Od roku 2030 sa v Európe zavedie nový štandard pre platby, ktorý by mal priniesť vyššiu úroveň bezpečnosti a jednoduchosti pre používateľov. Tieto zmeny sa dotknú aj mnohých tých, ktorí pravidelne nakupujú cez internet.

V súčasnosti, keď je potrebné zaplatiť za tovar alebo službu online, je potrebné zadať množstvo citlivých údajov z platobnej karty vrátane 16-miestneho čísla karty, dátumu exspirácie a bezpečnostného kódu. Tento proces môže byť zdĺhavý, nekomfortný, navyše s obavami o bezpečnosť údajov. Po zavedení nových pravidiel však tento postup nahradí tzv. tokenizácia.

Tokenizácia je proces, pri ktorom sa citlivé údaje, napríklad číslo platobnej karty, nahrádzajú jedinečným náhodne generovaným tokenom. Tento token je použitý pri platobnej transakcii namiesto skutočných údajov o karte, čím sa výrazne znižuje riziko, že by tieto údaje mohli byť odcudzené alebo zneužité. Tokeny sú navyše zabezpečené biometrickou autentifikáciou, čo znamená, že na ich použitie budú potrebné napríklad odtlačok prsta alebo rozpoznanie tváre.

---

[1] FinReport. *mBank po platbách prsteňom prináša aj platobné náramky* [online]. 2024. [cit. 25. septembra 2024]. Dostupné na internete: https://www.interez.sk/na-slovensko-prichadza-novy-typ-platby-znama-banka-svojim-klientom-poskytne-novinku/.

Jednou z najväčších výhod pre zákazníkov bude zvýšený komfort a bezpečnosť, pretože už nebude potrebné manuálne zadávať číslo karty a ďalšie údaje pri každej online platbe. Stačí jednoduché potvrdenie platby pomocou biometrického overenia. Tokenizácia okrem toho prináša aj vyššiu úroveň bezpečnosti. Podľa prieskumu spoločnosti *Juniper Research* sa očakáva, že do roku 2028 straty spôsobené online podvodmi dosiahnu až 91 miliárd dolárov. Tokenizácia by mala tieto čísla výrazne znížiť, čo je pozitívne zistenie nielen pre zákazníkov, ale aj pre obchodníkov, ktorí tak môžu ponúkať bezpečnejšie platobné riešenia.

Európa sa považuje za lídra v oblasti platobných inovácií. Bezpečnostné opatrenia, ako sú bezkontaktné platby a online bankovníctvo, sa tu rýchlo rozšírili a získali si popularitu medzi spotrebiteľmi, preto už aj tokenizácia zaznamenáva značný nárast a očakáva sa, že do roku 2030 bude táto technológia bežnou súčasťou každodenných transakcií.

Napriek tomu, že ide o významný pokrok, je potrebné zabezpečiť, aby všetky zúčastnené strany vrátane bánk a obchodníkov boli pripravené na túto zmenu. Okrem toho bude dôležité, aby si zákazníci osvojili nové postupy a cítili sa pri používaní tokenizácie komfortne. Zatiaľ nie je možné presne odhadnúť, ako veľmi tento krok zníži počet online podvodov, prvotné prognózy však naznačujú výrazné zlepšenie.

Uvádzané plánované zmeny v oblasti online platieb môžu priniesť priam revolučné zmeny, pokiaľ ide o spôsob, akým spotrebitelia kupujú na internete. Vďaka tokenizácii však budú platby bezpečnejšie a pohodlnejšie, čo ocení každý, kto sa pri online nákupoch obáva o bezpečnosť svojich údajov. Európa, ktorá sa často stavia do úlohy lídra v technologických inováciách, bude aj tentoraz na čele tejto významnej zmeny. Bude však zaujímavé sledovať, ako rýchlo sa nová technológia rozšíri a aký dopad bude mať na globálny trh.[2]

Východisková právna úprava

Boj proti podvodom a falšovaniu bezhotovostných platobných prostriedkov je jednou z oblastí legislatívnej činnosti EÚ. Jeho právnym základom je rámcové rozhodnutie 2001/413/SVV o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov. Cieľom tohto rámcového rozhodnutia je zabezpečenie toho, aby sa podvody a falšovanie týkajúce sa všetkých foriem bezhotovostných platobných prostriedkov považovali za trestné činy a podliehali účinným, primeraným a odrádzajúcim sankciám vo všetkých členských štátoch.[3] Má pomáhať v boji proti podvodom a falšovaniu týkajúcemu sa bezhotovostných platobných prostriedkov spolu s ostatnými nástrojmi, ktoré už Rada odsúhlasila, ako sú Spoločná akcia 98/428/JHA o vytvorení Európskej súdnej siete, Spoločná akcia 98/733/JHA o uznaní účasti v zločineckej organizácií za trestný čin v členských štátoch Európskej únie, alebo Spoločná akcia 98/699/JHA o praní špinavých peňazí.

Uvádzané rámcové rozhodnutie 2001/413/SVV o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov ako východiskový pojem definuje platobný nástroj ako hmotný nástroj, iný ako zákonné platidlo (bankovky a mince), ktorý vďaka svojej osobitnej povahe sám alebo spolu s iným (platobným) nástrojom umožňuje držiteľovi alebo používateľovi prevádzať peniaze alebo peňažné hodnoty, napríklad kreditné karty, eurošekové karty, ostatné karty vydávané finančnými inštitúciami, cestovné šeky, eurošeky, ostatné šeky a zmenky, ktoré sú chránené pred napodobovaním alebo podvodným používaním, napríklad dizajnom, kódovaním alebo podpisom.

---

[2] MARCIČIAK, M. *Veľké zmeny pri platení cez internet. Bude bezpečnejšie, ale komplikovanejšie* [online]. 2024. [cit. 25.septembra 2024]. Dostupné na internete:https://www.techbyte.sk/2024/09/slovaci-zvyknut-platobne-karty-zmeny/.

[3] KLIMEK, L. Boj proti podvodom a falšovaniu bezhotovostných platobných prostriedkov na úrovni Európskej únie. Bratislava. In: *Justičná revue*. 2016, roč. 68, 2016, č. 1, s. 95.

Článok 2 tohto rámcového rozhodnutia definuje trestné činy týkajúce sa platobných nástrojov. Za takéto trestné činy je potrebné považovať také konania, ktoré sú spáchané úmyselne aspoň v súvislosti s kreditnými kartami, eurošekovými kartami, ostatnými kartami vydávanými finančnými inštitúciami, cestovnými šekmi, eurošekmi, ostatnými šekmi alebo zmenkami:

a) krádež alebo iné nezákonné prisvojenie si platobného nástroja;

b) napodobovanie alebo falšovanie platobného nástroja s cieľom použiť ho na účely podvodu;

c) prijatie, získanie, preprava, predaj a poskytovanie iným osobám alebo vlastnenie ukradnutého, alebo inak nezákonne si prisvojeného alebo napodobeného alebo falzifikovaného platobného nástroja s cieľom použiť ho na účely podvodu;

d) podvodné používanie ukradnutého alebo inak nezákonne si prisvojeného, alebo napodobeného alebo falzifikovaného platobného nástroja.

Článok 3 zakotvuje trestné činy týkajúce sa počítačov. Nimi sú také konania, ktoré sú spáchané úmyselne, a to vykonanie alebo navádzanie k prevodu peňazí alebo peňažnej hodnoty, a tým spôsobenie neoprávnenej straty na majetku inej osoby s úmyslom nadobudnúť neoprávnenú výhodu pre osobu páchajúcu trestný čin alebo tretiu stranu prostredníctvom:

- neoprávneného vkladania, pozmeňovania, vymazávania alebo odstraňovania údajov, najmä identifikačných, alebo
- neoprávneného zasahovania do fungovania počítačového programu alebo systému.

Článok 4 upravuje trestné činy týkajúce sa zvláštne upravených zariadení. Nimi sú úmyselne podvodné vyrábanie, prijatie, získanie, predaj alebo poskytovanie inej osobe alebo vlastníctvo:

- nástrojov, článkov, počítačových programov a akýchkoľvek ďalších prostriedkov výhradne prispôsobených na spáchanie ktoréhokoľvek z trestných činov uvedených v článku 2 písm. b);
- počítačových programov na účely spáchania ktoréhokoľvek z trestných činov opísaných v článku 3.

Predmetné rámcové rozhodnutie je súčasťou právne záväzných aktov Európskej únie, ktoré sú súčasťou Trestného zákona a jednotlivé jeho ustanovenia vrátane ďalej uvedených sú v súlade s týmto rámcovým rozhodnutím.

Právnou normou upravujúcou predmetnú problematiku je aj Trestný zákon, ktorý v § 131 ods. 6 definuje pojem platobný prostriedok ako nehmotné alebo hmotné chránené zariadenie, predmet, záznam alebo ich kombinácia vrátane platobnej karty, ktorá je chránená pred falšovaním alebo neoprávneným použitím a ktorá držiteľovi alebo používateľovi sama alebo spolu s nejakým postupom alebo súborom postupov umožňuje prevod peňazí, elektronických peňazí alebo virtuálnej meny.

Nadväzujúcim ustanovením Trestného zákona je § 219 zakotvujúci trestný čin Neoprávneného vyrobenia a používania platobného prostriedku.

Podľa odseku 1 sa tohto trestného činu dopustí ten, kto neoprávnene prechováva, prepravuje, obstará si alebo inak zadováži alebo poskytne inému platobný prostriedok.

Podľa odseku 2 kto neoprávnene použije platobný prostriedok, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

Rovnako ako v odseku 2 sa potrestá, kto falšuje, pozmení, napodobní alebo neoprávnene vyrobí platobný prostriedok alebo kto takýto platobný prostriedok prechováva, prepravuje, obstará si alebo inak zadováži, použije alebo poskytne inému (odsek 3).

V zmysle ods. 4 tohto ustanovenia kto vyrobí, sebe alebo inému zadováži alebo prechováva nástroj, počítačový program alebo iný prostriedok špeciálne prispôsobený na spáchanie činu uvedeného v odseku 3, potrestá sa odňatím slobody až na dva roky.

Nakoniec pojem platobný prostriedok vymedzuje aj zákon č. 492/2009 Z. z. o platobných službách v znení neskorších predpisov, ktorý § 2 ods. 19 platobný prostriedok definuje ako personalizované zariadenie alebo súbor postupov dohodnutý medzi používateľom platobných služieb a poskytovateľom platobných služieb, ktoré sa používajú na účely predkladania platobného príkazu, najmä platobná karta, internet banking alebo iné platobné aplikácie elektronického bankovníctva.[4]

Platobnou kartou sa podľa ods. 20 tohto zákona rozumie platobný prostriedok, ktorý umožňuje používateľovi platobných služieb prístup k finančným prostriedkom čerpaným do výšky limitu povoleného poskytovateľom platobných služieb. Platobnými kartami sú napríklad vernostné, klubové karty, karty na čerpanie pohonných hmôt, telefónne karty, stravovacie karty, SAD karty, MHD karty a podobne určené na použitie v sieti jedného poskytovateľa služieb alebo v rámci limitovanej alebo obmedzenej siete viacerých poskytovateľov, alebo na nákup limitovaného alebo obmedzeného rozsahu tovarov alebo služieb.

Aplikačná prax

V praxi orgánov činných v trestnom konaní dominuje majetková kriminalita, pričom v rámci tejto praxe často dochádza k odcudzeniu osobných dokladov, finančnej hotovosti ako aj platobných kariet a iných platobných prostriedkov.

Odcudzenie platobnej karty spoločne aj s inými osobnými dokladmi samo o sebe napĺňa skutkovú podstatu trestného činu krádeže podľa § 212 ods. 1 Trestného zákona (napríklad vrecková krádež peňaženky, ktorej obsahom je aj platobná karta by napĺňala skutkovú podstatu podľa § 212 ods. 1 písm. d) Trestného zákona), po úmyselnom zmocnení sa platobnej karty a jej neoprávnenom prechovávaní prichádza do úvahy trestný čin podľa § 219 ods. 1 Trestného zákona [5] a napokon jej neoprávnené použitie či už na účel neoprávneného výberu finančnej hotovosti z bankomatu alebo jej použitia na platbu za tovar prípadne služby by hmotnoprávne napĺňalo znaky skutkovej podstaty trestného činu neoprávneného vyrobenia a používania platobného prostriedku podľa § 219 ods. 2 Trestného zákona, pričom pri takomto neoprávnenom výbere finančnej hotovosti pri splnení hmotnoprávnej podmienky o výške malej škody (§ 125 ods. 1 Trestného zákona) vo vzťahu k trestnému činu krádeže podľa § 212 ods. 1 písm. a) Trestného zákona by prichádzal do úvahy aj jednočinný súbeh týchto trestných činov, pričom tento jednočinný súbeh nie je vylúčený z dôvodu subsidiarity trestného činu ohrozovania voči trestnému činu poruchovému.

Znak skutkovej podstaty trestného činu podľa § 219 ods. 1 Trestného zákona v slovnom spojení „inak zadováži“ však môže naplniť aj samotný nález platobnej karty, pokiaľ si ju páchateľ ponechá vo svojej dispozícii bez úmyslu ju odovzdať príslušnej banke alebo orgánom polície. [6]

Predmetný trestný čin sa však neobmedzuje iba na platobné karty, ale jeho záber je podstatne širší, nakoľko jeho objektom je vlastnícke právo k akémukoľvek prostriedku, ktorý umožňuje využívanie služieb elektronického bankovníctva alebo iného prostriedku, ktorý plní uhradzovaciu funkciu.

---

[4] KLIMEK, L. Falšovanie bezhotovostných platobných prostriedkov v teórii a praxi. In: Szabová, E., K. Vrtíková a I. Mokrá. *Tradičné a netradičné prístupy v trestnom práve. Zborník príspevkov z konferencie „Trnavské právnické dni 2024: Tradičné a netradičné v práve“,* 329 s.

[5] *Uznesenie NS ČR zo dňa 26.03.2003 sp. zn.: 7Tdo 320/2003: III.* Pro naplnění skutkové podstaty tr. činu neoprávněného držení platební karty postačuje, když úmysl pachatele směřuje k opatření platební karty nebo předmetu způsobilého plnit jej funkci. Není tudíž rozhodné, zda pachatel platební kartu nebo předmět způsobilý plnit její funkci k placení zboží nebo služeb skutečně použil nebo se o to alespoň pokusil, protože k trestnosti postačuje její pouhé neoprávněné opatření.

[6] R 46/2008.

Z konštrukcie ustanovenia § 219 Trestného zákona je zrejmé, že v prípade tohto trestného činu sa naskytujú rôzne *modus operandi,* teda okrem samotného neoprávneného použitia prichádza do úvahy aj prechovávanie, prepravovanie, obstarávanie alebo iné zadováženie, falšovanie, pozmeňovanie, napodobovanie a neoprávnená výroba platobného prostriedku. Samostatnú kategóriu *modus operandi* predstavuje zadováženie alebo prechovávanie nástroja, počítačového programu alebo iného prostriedku špeciálne prispôsobeného na falšovanie alebo pozmeňovanie platobného prostriedku, pričom však azda najčastejšie je spáchanie tohto trestného činu podľa ods. 2.

Odhalenie, vyšetrenie, zákonné prejednanie a spravodlivé potrestanie takejto trestnej činnosti môže vyvolávať zdanie jednoduchosti, avšak v skutočnosti tomu tak nemusí byť. Pokiaľ si odmyslíme zadržanie páchateľa trestného činu podľa § 219 ods. 2 Trestného zákona *in flagranti delicto*, stojí pred orgánmi činnými v trestnom konaní neľahké dokazovanie, že konkrétna osoba neoprávnene použila platobný prostriedok.

V tomto smere bude podstatné najmä stotožnenie osoby, ktorá mala neoprávnene použiť platobný prostriedok a zabezpečenie dôkazov o tomto použití. Bude teda potrebné napr. preverovať miesto neoprávneného výberu, zabezpečiť kamerové záznamy z bankomatu a jeho okolia a vykonať oboznámenie a stotožnenie osoby podozrivej z trestnej činnosti, prípadne za týmto účelom použiť prostriedky operatívno-pátracej činnosti. Stotožnenie páchateľa z kamerového záznamu, či už z bankomatu alebo z prevádzky, kde k takémuto použitiu došlo, sa musí vykonať prostredníctvom kriminalistickej antropológie. Pri znaleckom posudku z odboru kriminalistickej antropológie sa však nie vždy podarí s absolútnou určitosťou stanoviť záver, že konkrétna osoba, ktorá neoprávnene použila platobný prostriedok, je osoba obvineného, čo v prípade procesného štádia vznesenia obvinenia môže postačovať na dôvodný záver o spáchaní trestného činu, avšak v konaní pred súdom takýto dôkaz nemôže obstáť najmä s poukazom na to, že v súdnom konaní nebude postačovať pravdepodobnosť týkajúca sa osoby obžalovaného ako páchateľa trestného činu, a teda súd nemôže postaviť rozhodnutie o vine na dôkaze, ktorý iba pravdepodobne usvedčuje obžalovaného. Na základe uvedeného teda dokazovaním v prípravnom konaní by mali byť zaistené aj iné dôkazy, ktoré usvedčujú obvineného. Súdna prax dospela k názoru, že v prípade, ak v trestnom konaní existuje iba jeden usvedčujúci dôkaz, musí byť takému dôkazu venovaná mimoriadna pozornosť, ako aj náležitá pozornosť jeho preverenia a hodnotenia, pričom činnosť orgánov prípravného konania musí smerovať k tomu, aby na takýto dôkaz nadväzovali aj na iné, hoci aj nepriame dôkazy.[7]

Povinnosť orgánov činných v trestnom konaní zistiť skutkový stav veci bez dôvodných pochybností (§ 2 ods. 10 Trestného poriadku), ako aj ich povinnosti, ktoré sú vyjadrené v rámci zásady oficiality, musia byť naplnené aj v prípade dôkaznej núdze, resp. v prípade existencie iba jedného usvedčujúceho dôkazu.

Konkrétne zistené skutočnosti v podobe dôkazov sa však musia vzťahovať aj na preukázanie subjektívnej stránky skutkovej podstaty trestného činu podľa § 219 Trestného zákona. Na stanovenie a odôvodnenie eventuálneho úmyslu páchateľa, teda jeho zákonného vyjadrenia podľa § 15 písm. b) Trestného zákona, nebude postačovať iba konštatácia, že obžalovaný musel predpokladať, že poškodený môže mať platobné karty vo svojich osobných veciach, ale musí byť riadne preukázané, že páchateľ konal s úmyslom odcudziť platobný prostriedok, v opačnom prípade by sa takéto zdôvodnenie obmedzilo iba na konštatáciu údajnej notoriety. Pri dokazovaní v trestnom konaní je takýto spôsob argumentácie neprijateľný.[8] V konkrétnom prípade išlo o odcudzenie celej tašky, teda súboru viacerých osobných vecí, medzi ktorými bola aj peňaženka poškodeného, a teda vzhľadom na takýto spôsob spáchania nemožno bez ďalšieho dokazovania učiniť záver o splnení znakov

[7] *ÚS 81/2004*
[8] *Nález ÚS ČR zo dňa 17. júna 2004 sp. zn. IV. ÚS 37/200.*

subjektívnej stránky skutkovej podstaty trestného činu podľa § 219 Trestného zákona v neprospech páchateľa.

Z uvedeného vyplýva, že pre trestnosť konania páchateľa podľa § 219 ods. 1 Trestného zákona nebude postačovať ani samotné odcudzenie peňaženky alebo iných vecí zvyčajne slúžiacich na uloženie osobných vecí, finančných prostriedkov, dokladov alebo iných platobných prostriedkov, v ktorých sa nachádza platobná karta. Konanie páchateľa by napĺňalo znaky skutkovej podstaty tohto trestného činu až vtedy, ak páchateľ konal aspoň v nepriamom úmysle použiť v budúcnosti neoprávnene zaobstaranú kartu alebo ju na ten účel prechovával.

V praktickej rovine možno takýto úmysel páchateľa odvodiť spravidla od jeho prechádzajúcej vedomosti o existencií platobného prostriedku, ktorý je v dispozícií poškodeného alebo od preukázania motívu páchateľa následne ho použiť ako pravý. Bude tomu tak aj vtedy, ak páchateľ platobný prostriedok použije ako pravý alebo sa o to pokúsi.[9] Pri fyzickej krádeži platobnej karty páchateľ spravidla využije to, že videl predtým zadávaný PIN (cielená krádež konkrétnej platobnej karty) alebo že je PIN napísaný na platobnej karte, alebo na inom doklade v peňaženke (krádež zameraná na akékoľvek majetkové hodnoty, medzi ktorými sa nachádza aj platobná karta). Existuje i variant, keď páchateľ monitoruje doručené listiny majiteľa platobnej karty a zmocní sa karty a takejto listiny obsahujúcej PIN.[10]

Vo vzťahu k falšovaniu, pozmeňovaniu, napodobeniu alebo neoprávnenej výrobe platobného prostriedku ide o trestnú činnosť značne sofistikovanejšiu, ako je napríklad trestná činnosť podľa ods. 1 a 2. Predmetom falšovania a pozmeňovania môžu byť rozličné formy platobných prostriedkov, napríklad príkaz na bezhotovostnú úhradu[11], privátny kľúč k peňaženke virtuálnej meny, prípadne iné predmety slúžiace na disponovanie s virtuálnymi menami, ale aj platobná zmenka (ako osobitný bezhotovostný druh platobného prostriedku v zmysle zákona č. 191/1950 Zb. v znení neskorších predpisov) a šek.

V praxi boli zaznamenané konkrétne prípady zneužitia telefonického bankovníctva [12], tankovacej, resp. palivovej karty [13], Premia kariet k revolvingovým úverom [14] a mnohých iných.

Súdna prax zastáva názor, že falšovanie je činnosť smerujúca k tomu, aby predmet, na ktorom sa falšovanie realizuje, nadobudol vzhľad pravého predmetu.[15] Listinné príkazy na úhradu môžu byť falšované napríklad tým, že páchateľ neoprávnene vyhotoví takýto platobný prostriedok napodobením podpisu oprávneného disponenta. V prípade príkazov na úhradu, ktoré sú vyhotovované v rámci internet bankingu, nahrádza faktický podpis disponenta séria bezpečnostných operácií v podobe prístupového hesla a autorizačných kódov, ktoré buď generuje banka prostredníctvom rôznych systémov, alebo formou fyzickej čítačky. Prekonanie takýchto bezpečnostných opatrení a získanie neoprávneného prístupu do internetového bankovníctva, v ktorom sa následne neoprávnene vyplní a odošle príkaz na úhradu, predstavuje vytvorenie falošného platobného prostriedku podľa § 219 ods. 3 Trestného zákona.[16]

Iným príkladom páchania trestnej činnosti súvisiacej s platobnými kartami sú prípady aktuálne vo väčšom počte evidované v Českej republike, kde sa objavil Android malvér, ktorý dokáže zneužiť bezkontaktnú technológiu na odcudzenie peňazí z bankomatu. Použitý malvér má schopnosť prenášať údaje z platobných kariet poškodených prostredníctvom

---

[9] *Stanovisko generálneho prokurátora SR zo 17. decembra 2018 sp. zn. IV/1 Spr 390/17/1000, por. č. 2/2018*
[10] SMEJKAL, V. *Kybernetická kriminalita*, s. 732-733.
[11] *R 21/2001*
[12] *Rozsudok OS Stará Ľubovňa z 25.1.2013, sp. zn. 7T/1/2013*
[13] *Rozsudok OS Rožňava z 26.3.2012, sp. zn. 1T/18/2012*
[14] *Rozsudok OS Topoľčany zo 16.8.2013, sp. zn. 1T/57/2013*
[15] *R 1698/1924*
[16] *Uznesenie NS ČR zo dňa 16.05.2018 sp. zn. 4 Tdo 456/2018*

škodlivej aplikácie nainštalovanej v ich zariadeniach so systémom Android do rootnutého Android telefónu útočníka.

Páchateľ pritom prenáša údaje z fyzických platobných kariet poškodených prostredníctvom ich kompromitovaných Android smartfónov pomocou škodlivého softvéru do svojho zariadenia a následne tieto údaje používa na vykonanie bankomatových transakcií. Ak táto metóda zlyháva, páchateľ má záložný plán na prevod finančných prostriedkov z účtov poškodených na iné bankové účty.

Poškodení si takto v konkrétnych prípadoch stiahli a nainštalovali škodlivý softvér po tom, čo boli uvedení do omylu o tom, že komunikujú so svojou bankou a že ich zariadenie je ohrozené. V skutočnosti nevedomky kompromitovali svoje vlastné Android zariadenia ešte predtým, keď si v prvom kroku stiahli a nainštalovali aplikáciu z odkazu v podvodnej SMS správe o možnom vrátení daní. Je dôležité poznamenať, že malvér nebol nikdy dostupný v oficiálnom obchode Google Play.

Páchatelia teda skombinovali štandardné škodlivé techniky, a to sociálne inžinierstvo, phishing a malvér pre Android. Podľa údajov Eset Brand Intelligence Service pôsobili v Českej republike od novembra 2023 a od marca 2024 vylepšili svoju techniku prostredníctvom nasadenia Android malvéru NGate. Útočníci zároveň dokázali pomocou neho klonovať NFC údaje z fyzických platobných kariet poškodených a prenášať tieto údaje do zariadenia útočníka, ktoré dokáže emulovať pôvodnú kartu a vybrať peniaze z bankomatu.

Zabezpečenie ochrany pred takýmito komplexnými útokmi si vyžaduje použitie určitých proaktívnych krokov proti hrozbám, najmä kontrolovanie URL adresy webových stránok, sťahovanie aplikácie z oficiálnych obchodov, udržiavanie PIN kódov v tajnosti, používanie bezpečnostných aplikácií v smartfónoch, vypínanie funkcie NFC, keď nie je potrebná, používanie ochranných puzdier alebo virtuálnych kariet chránených autentifikáciou.[17]

Skimming, shimming, carding, spywar

Platobné prostriedky vo všeobecnosti nosia v sebe určité znaky odlišnosti a jedinečnosti, ktoré sú väčšinou uložené v čipe karty, resp. v magnetickom krúžku karty, pričom predmetom falšovania je spravidla tento čip, resp. jeho naprogramovanie, tak aby jeho prostredníctvom bola možnosť vykonávať činnosti, na ktoré je oprávnený iba držiteľ pôvodného platobného prostriedku.

Falšovanie sa v tomto prípade zvyčajne deje na základe rôznych čítačiek, emulátorov alebo počítačových programov, ktoré umožňujú vytvoriť falzifikát čipu, resp. jeho naprogramovanie, aby plnil funkciu pôvodného čipu. Často využívanou metódou v tomto smere je zbieranie informácií na karte na účel neoprávnenej výroby platobného prostriedku. Ide o tzv. *skimming,* keď páchateľ neoprávnene nainštaluje do bankomatu (alebo iného zariadenia, pri ktorom sa sníma čip karty) zariadenie umožňujúce kopírovanie údajov z karty (meno a priezvisko držiteľa karty, číslo karty, doba exspirácie a bezpečnostný kód CVC – *card verification code*) a zachytenie PIN kódu či už pomocou falošnej klávesnice alebo jeho nasnímania bankomatovou kamerou, pričom zneužitie platobnej karty je možné iba vtedy, ak sa podarí získať PIN kód a údaje o platobnej karte.

Uvedené *modus operandi* prebieha v podstate v dvoch etapách, kedy sa v prvej etape vyššie uvedeným spôsobom skopírujú údaje z karty a zistí sa PIN kód a v druhej sa tieto údaje nahrajú na inú platobnú kartu, ktorá je falzifikátom pôvodnej karty, pričom následne sa môžu pomocou takejto karty vykonávať neoprávnené transakcie. V prípade *skimmingu,* teda samotnej inštalácie takéhoto zariadenia do bankomatu alebo iného zariadenia na účel výroby falošných platobných kariet, ich následnej výroby na základe takto získaných údajov

[17] JAMNICKÝ, M. *Odhalili malvér, ktorý kradol údaje z platobných kariet.* [online]. 2024. [cit. 27.septembra 2024]. Dostupné na internete: https://uzitocna.pravda.sk/peniaze/clanok/721684/

a napokon ich použitie, naplňuje znaky skutkovej podstaty trestného činu podľa § 219 ods. 3 Trestného zákona.[18] Treba však poukázať na to, že samotné prechovávanie predmetu, ktorý umožňuje vykonať *skimming*, prípadne iné zariadenia, ktoré sú spôsobilé vyrobiť falzifikát platobnej karty, budú trestné podľa § 219 ods. 4 Trestného zákona – teda predmetov, nástrojov alebo počítačových programov, ktoré sú špeciálne prispôsobené na spáchanie trestného činu podľa ods. 3.

Všeobecne možno uviesť, že primárnym objektom trestného činu podľa § 219 Trestného zákona je záujem na bezpečnosti a spoľahlivosti platobných prostriedkov ako základu bezpečného a funkčného finančného styku, ktorý je základom fungujúceho trhového hospodárstva.[19] Z tohto pohľadu možno vnímať *skimming* ako priamy útok na tento záujem, teda útok, ktorého povaha bezprostredne smeruje k spáchaniu trestného činu podľa § 219 ods. 3 Trestného zákona. Inštaláciu tohto zariadenia do bankomatu alebo iného zariadenia, ktorý sníma platobnú kartu, možno právne kvalifikovať ako pokus trestného činu podľa § 219 ods. 3 Trestného zákona. Na účely podrobného opisu konkrétnej situácie, pri ktorej bol použitý *skimming*, odkazujeme na uznesenie Najvyššieho súdu ČR zo dňa 24.05.2017 sp. zn. 15 Tdo 1491/2016, pričom toto rozhodnutie dokumentuje túto trestnú činnosť v zmysle kvalifikačného znaku skutkovej podstaty „vo veľkom rozsahu“, keďže v tomto prípade sa *skimmingom* podarilo neoprávnene skopírovať údaje a prístupové údaje vo vzťahu k 399 platobným kartám.

V prípade pozmeneného platobného prostriedku môže ísť o pravý a platný platobný prostriedok, u ktorého bola vykonaná neoprávnená zmena, aby ho bolo možné používať v rozpore s jeho pôvodným účelom. Takýmto platobným prostriedkom môže byť aj platobná karta, ktorej vypršala exspiračná doba a u ktorej bola vykonaná taká zmena, aby opäť získala svoju platnosť, a teda možno ju v takomto stave použiť na účel výberu hotovosti alebo použitia pri platbe.[20]

Vyššie uvedené spôsoby trestnej činnosti neoprávneného vyrobenia a používania platobného prostriedku bývajú v zahraničnej literatúre často označované, ako tzv. *carding*, odvodený od slova *card*. Aj keď *carding* vo svojej najjednoduchšej forme je spojený práve s vyššie uvedeným *skimmingom* v bankomatoch a platobných termináloch, vo svojich sofistikovanejších formách zahŕňa širšie množstvo aktivít. Medzi najrozšírenejšie a technologicky najjednoduchšie zariadenia využívané na *skimming*, v praxi nazývané ako tzv. *skimmery*, patria čítačky magnetického prúžku platobnej karty. Práve tieto sú umiestňované na vyššie uvedených miestach s čo najvyššou frekvenciou platieb, pričom ich cena sa pohybuje v rozmedzí 100 – 500 €. V rámci kopírovania informácií z magnetického prúžku zaznamenávajú a lokálne ukladajú základné informácie potrebné na prevedenie platby kartou sfalšovanou útočníkom, a to meno držiteľa, číslo karty, dátum platnosti a CVV kód. Okrem klonovania platobnej karty, resp. nahrávania informácií na novo sfalšovaný platobný prostriedok je možné v prípade absencie dvojfázovej verifikácie využiť kartu aj na online nákupy. Aj keď bežný zákazník nemá šancu si *skimmer* pri platbe všimnúť, medzi hlavné nevýhody takéhoto typu *skimmeru* patrí nevyhnutnosť jeho fyzickej inštalácie, čo v praxi znamená zvýšenie šírky a výšky platobného terminálu, ktorú si znalejší platiteľ môže všimnúť. [21]

Vyššie zmieňované zaznamenávanie PIN kódu v kombinácii s informáciami z magnetického prúžku umožňujú zložitejšie a drahšie skimmery pohybujúce sa v cenovej kategórii od 500 do 1500 €. Najtypickejším mechanizmom je umiestnenie druhej vrstvy

[18] *Uznesenie NS ČR zo dňa 23.09.2015 sp. zn. 5 Tdo 906/2015*
[19] ŠÁMAL, P. a kol. *Trestní zákonník II. § 140 až 421. Komentář*, s. 2129.
[20] ŠÁMAL, P., F. PÚRY a S. RIZMAN. Trestní zákon – Komentář, s. 2365.
[21] FBI. *Skimming* [online]. 2024. [cit. 5.októbra 2024]. Dostupné na internete: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming.

kopírujúcej tlačidlá na terminál, ktorá zaznamenáva informácie zadávané zákazníkom. Alternatívu predstavuje inštalácia oddeleného zariadenia slúžiaceho iba na účely zadávania PINu k originálnemu terminálu so *skimmerom*. Vzhľadom na vyššie náklady spojené so zaobstaraním danej technológie dosahujúce až 2500 € sa zriedkavejšie využívajú aj bezdrôtové *skimmery* doplnené napr. mobilnými modemami, ktoré v reálnom čase PIN spoločne s ďalšími informáciami posielajú na virtuálne úložisko. Vychádzajúc z absencie potreby fyzickej inštalácie a z neho vyplývajúcej náročnosti jeho odhalenia predstavuje bezdrôtový *skimmer* pre útočníka oveľa atraktívnejší variant. V praxi je možné sa stretnúť aj s hybridnými *skimmermi*, ktoré na účel získania práve PIN kódu využívajú kameru nainštalovanú v blízkosti bankomatu alebo platobného terminálu. Za rovnako atraktívne, ba možno aj atraktívnejšie je možné považovať špecificky upravené *skimmery* podľa konkrétnych požiadaviek a potrieb útočníka. Cenové rozmedzie týchto zariadení dosahuje aj vyššie hodnoty, a to nezriedka pohybujúc sa medzi 2500 – 5000 €, pričom výnimkou nie sú ani vyššie sumy. Medzi najrozšírenejšie z tejto kategórie patria tenké *skimmery* zaznamenávajúce rovnaké informácie, ktoré sú na rozdiel od vyššie analyzovaných umiestnené priamo v zariadení a ich vizuálne odhalenie sa tak stáva *de facto* nemožným.

Rovnaký účel ako *skimmery*, resp. za podkategóriu *skimmerov*, bývajú označované tzv. *shimmery* využívajúce na krádež informácií odlišný mechanizmus. Na rozdiel od čítania magnetického prúžku *shimmer* prostredníctvom prístupu k čipu zaznamenáva komunikáciu medzi platobným terminálom a poskytovateľom platobnej karty (v danom prípade označuje termín spracovateľa platieb, napríklad *Visa, Mastercard* a podobne, nie banku), pričom získané informácie je následne možné využiť rovnako ako v prípade *skimmerov*. Pre komplexnejšie pochopenie situácie je potrebné uviesť, že vyššie analyzované zariadenia bývajú často inštalované napríklad konkrétnym zamestnancom bez vedomia majiteľa obchodu, pričom podľa dostupných štatistík patria medzi najrizikovejšie skupiny takto ohrozených podnikateľských subjektov drobné obchody s potravinami, suvenírmi, prípadne malé reštaurácie alebo bary. V kontexte bankomatov boli zaznamenané prípady, v ktorých bol *skimmer* umiestnený technikom spolupracujúcim s organizovanou skupinou alebo mimoriadne sofistikovanými páchateľmi s dostatočnými znalosťami umožňujúcimi obídenie bezpečnostných mechanizmov.

Vzhľadom na špecifiká *skimmingu*, primárne na jeho technologickú náročnosť, predstavuje daná forma problematický fenomén, boj s ktorým je pre kompetentné orgány v súčasnej dobe prinajmenšom značne problematický. Podľa americkej agentúry *Fair Isaac Corporation* hodnotiacej kreditné skóre občanov USA, bol za prvý polrok 2023 zaznamenaný nárast prípadov *skimmingu* o 77 %, dosahujúc tak viac ako 120 000 zasiahnutých kariet, pričom medzi rokmi 2021 – 2022 toto číslo stúplo o šokujúcich 368 %. [22]

Do širšej kategórie *cardingu* spadá aj metóda aplikovaná výhradne vo virtuálnom priestore, a to tzv. digitálny *skimming*, v zahraničnej literatúre označovaný aj ako *web skimming* alebo *site skimming* útoky. Ako vyplýva z názvu, zmieňovaná praktika cieli na online transakcie s cieľom uloženia informácií o platobnom prostriedku na zariadenie útočníka a ich následné využitie rovnako ako v prípade vyššie zmieňovanej formy. Medzi najrozšírenejšie metódy patrí získanie neoprávneného prístupu na webovú stránku obchodníka, na ktorú je následne umiestnený malvér zaznamenávajúci *de facto* všetku aktivitu na danej stránke, s dôrazom na transakcie a v rámci nich spracovávané informácie. Rovnako ako v prípade klasického *skimmingu*, aj digitálny *skimming* disponuje širokým spektrom nástrojov, konkrétny popis ktorých je vzhľadom na technologickú komplexnosť nad rámec tohto článku. Vo všeobecnosti platí, že medzi najrizikovejšie faktory patria laxné

[22] FICO. *Card Skimming and Other Fraud Types Continue to Grow – US Dat* [online]. 2023. [cit. 5.októbra 2024]. Dostupné na internete: https://www.fico.com/blogs/us-card-skimming-grew-nearly-5x-2022-new-fico-data-shows

bezpečnostné opatrenia na strane prevádzkovateľa webu, zastaraný software, prípadne vopred napadnuté *pluginy* poskytované tretími stranami. V prípade napadnutej stránky je pre bežného používateľa nemožné si existenciu hrozby všimnúť, keďže transakcia je spracovaná bez viditeľných komplikácií.

Dostupné štatistiky od prelomu rokov 2020 – 2021 poukazujú na jasný trend vo forme jednoznačnej dominancie digitálneho *skimmingu* v porovnaní s vyššie uvedeným fyzickým, pričom ide o obrat v porovnaní s predchádzajúcimi rokmi. Za hlavný faktor vedúci k danému obratu je možné považovať prijaté opatrenia v súvislosti s globálnou pandémiou COVID-19, pričom zvýšený presun trestnej činnosti do virtuálneho priestoru je sústavne zaznamenávaný v rôznych odvetviach. Podľa nezávislej agentúry *Insikt Group* za rok 2021 bolo zaznamenaných takmer 60 miliónov prípadov nahrania odcudzených osobných informácií na *dark web* pochádzajúcich z digitálneho *skimmingu* s cieľom ich predaja, pričom v prípade fyzického *skimmingu* sa daná metrika pohybovala okolo 36 miliónov. Nasledujúci rok 2022 priniesol v oboch prípadoch zníženie objemu predávaných údajov, a to na 45,6 milióna v prípade digitálneho a 13,8 milióna v prípade fyzického *skimmingu*. Za tento krátkodobý klesajúci trend je s najväčšou pravdepodobnosťou zodpovedný konflikt medzi Ruskom a Ukrajinou, a to najmä zintenzívnené aktivity lokálnych orgánov činných v trestnom konaní v snahe minimalizovať škody pochádzajúce z ekonomickej kriminality a využívanie daných prostriedkov na vojenské účely oboch strán. Pre lepšie pochopenie situácie je potrebné uviesť, že práve predajcovia predmetných informácií nachádzajúcich sa v Rusku a na východnej Ukrajine predstavujú z globálneho hľadiska percentuálne dominantnú skupinu, pričom predávané informácie pochádzajú z rôznych krajín, a to primárne z USA, krajín západnej Európy a zmieňovaného Ruska a Ukrajiny. [23]

Zreteľnejšiu formu digitálneho *skimmingu* predstavujú stránky špecificky vytvorené na účel zhromažďovania informácií. Aj keď je možné sa stretnúť so širokou plejádou subjektov spadajúcich do tejto kategórie, vo všeobecnosti platí, že portály takýchto „obchodníkov" disponujú relatívne lacným, nekvalitným grafickým dizajnom, zväčša neexistujú recenzie daného portálu, stránka ponúka tovar za podozrivo lacné ceny a chýbajú kľúčové informácie o ochrane osobných údajov, právnickej osobe prevádzkujúcej portál atď.[24]

V kontexte digitálnej formy *skimmingu* je potrebné venovať priestor aj mierne odlišnej forme trestnej činnosti s rovnakým konečným výsledkom. Vyššie uvedené informácie môže páchateľ získať aj prostredníctvom prelomenia bezpečnostnej bariéry zariadenia používateľa, napríklad počítača, telefónu alebo tabletu a nainštalovania *spywaru*. Vzhľadom na špecifiká danej metódy ide z perspektívy obete ešte o nebezpečnejšiu taktiku, ktorá môže poskytnúť páchateľovi prístup k *de facto* všetkým osobným informáciám. Na rozdiel od digitálneho *skimmingu*, ktorý zaznamenáva iba platobné informácie, môže *spyware* v prípade umiestnenia takýchto citlivých informácií na zariadení získať prístup napríklad k fotografiám osobných dokumentov, adrese obete a podobne. Tie môžu byť následne zneužité pre overenie identity, na základe čoho môže páchateľ získať úplný prístup napríklad k bankovému účtu, z ktorého môže vykonávať a overovať transakcie.

V kontexte súčasných *spyware* hrozieb kontroverzie vzbudzuje populárny čínsky obchodný portál *Temu*, presnejšie aplikácia, prostredníctvom ktorej je možné nakupovať rozličný tovar za mimoriadne výhodné ceny v porovnaní s európskymi alebo americkými obchodníkmi. Pred stiahnutím aplikácie v apríli 2024 varovala aj česká spotrebiteľská organizácia dTest, podľa ktorej aplikácia vzhľadom na svoje možnosti cielene zbiera citlivé informácie o jej používateľoch, pričom nie je jasné, ako ďalej s týmito informáciami pracuje,

[23] INSIKT GROUP. *Annual Payment Fraud Intelligence Report: 2022*. [online]. 2022. [cit. 5.októbra 2024]. Dostupné na internete: https://www.recordedfuture.com/research/annual-payment-fraud-intelligence-report-2022
[24] HUMAN. *What is Digital Skimming?* [online]. 2023. [cit. 5.októbra 2024]. Dostupné na internete: https://www.humansecurity.com/learn/topics/what-is-digital-skimming

čo v praxi môže predstavovať výrazné bezpečnostné riziko. Podobne ako v prípade *Temu,* aj v prípade iných stránok fungujúcich na podobnej báze predstavuje podniknutie konkrétnych krokov pre kompetentné orgány problém, keďže ide o zahraničné subjekty, na ktoré domáce inštitúcie nemajú potrebný dosah. [25]

Aj keď sú zmieňované rizikové faktory typické pre menších obchodníkov s obmedzenými zdrojmi na dodržiavanie opatrení, v určitých situáciách sa obeťami podobných útokov stávajú aj giganti s počtami zákazníkov pohybujúcich sa v stovkách tisícov. Medzi typické príklady patrí útok na leteckú spoločnosť *British Airways* z leta 2018, v rámci ktorého útočníci získali prístup k osobným a platobným informáciám viac ako 500 000 zákazníkov. Bezpečnostná bariéra systémov *British Airways* bola prelomená práve prostredníctvom využitia nedostatku partnerskej tretej strany, konkrétne spoločnosti *Swissport* poskytujúcej služby spojené s prepravou batožiny. Útočníci mali k dispozícii prístupové informácie jedného z účtov spojeného práve zo *Swissport*, pričom daný účet v dobe útoku nemal aktivovanú dvojfaktorovú autentifikáciu. Britský Úrad pre ochranu osobných údajov (*Information Commissioner's Office – ICO*) následne v októbri 2020 leteckej spoločnosti uložil pokutu vo výške 20 miliónov eur namiesto plánovaných 183 miliónov eur vzhľadom na finančné komplikácie spôsobené globálnou pandémiou. Presnú škodu spôsobenú zákazníkom *British Airways* je problematické vyčísliť, keďže pri útokoch podobných rozmerov páchatelia sami nevyužívajú odcudzené informácie. Dané informácie sa následne predávajú na *dark webe*, pričom kupujúci po ich kúpe pristupujú ku klonovaniu kariet, nákupom na internete alebo výberom hotovosti z bankomatu, relatívne častým je aj ich ďalší predaj na sekundárnom trhu.[26] Fyzické platby klonovanou kartou sa vyskytujú mimoriadne zriedkavo, resp. takmer vôbec, keďže predmetný sfalšovaný platobný prostriedok vyzerá vo svojej základnej forme ako biela karta bez akéhokoľvek označenia alebo grafického dizajnu banky. Väčšina aspoň minimálne informovaného personálu obsluhujúceho platobný terminál sfalšovaný prostriedok okamžite rozpozná a odmietne realizovať platbu. V kontexte vyššie zmieňovaného sekundárneho trhu nie je výnimkou ani existencia obchodníkov so stránkami prístupných z bežného internetu, pričom vo väčšine prípadov ide o podvody, kedy prevádzkovateľ stránky po získaní platby (najčastejšie) v kryptomene objednané údaje nezašle.

V rámci širšej definície do sféry *cardingu* spadá aj (vo voľnom preklade) bankový podvod (z anglického originálu *bank,* resp. *bank log fraud*), ktorého primárnym elementom je získanie prístupových informácií k bankovému účtu bez využitia informácií prináležiacich k platobnej karte. Rovnako ako v prípade vyššie uvedeného *skimmingu*, aj informácie o bankovom účte sú relatívne ľahko dostupné pre obchodníkov operujúcich primárne na *dark webe.* Tie sa najčastejšie získavajú kombináciou sociálneho inžinierstva a *phishingu,* konkrétnejšie napríklad prostredníctvom účelovo vytvorených stránok pripomínajúcich internetové bankovníctvo alebo iné finančné inštitúcie spadajúce do FinTech sektora. Nemenej rozšírenými sú aj priame telefonáty, v rámci ktorých sa útočník vydáva za zamestnanca banky alebo polície a „informuje" obeť o údajnom hroziacom nebezpečenstve, technologickej aktualizácii, jedinečnej možnosti zhodnotiť svoje finančné prostriedky atď., pričom od obete následne vyžaduje citlivé prístupové informácie. Medzi sofistikovanejšie metódy patria hackerské útoky na databázy bankových informácií online obchodníkov, prípadne využitie vyššie zmieňovaného *spywaru* alebo *keyloggerov*. Vzhľadom na komplexnejší charakter danej trestnej činnosti disponuje zložitejšou formou aj samotný výber

[25] FINREPORT. *Spotrebiteľská organizácia varuje pred sťahovaním aplikácie Temu.* [online]. 2024. [cit. 5.októbra 2024]. Dostupné na internete: https://www.finreport.sk/fintech/spotrebitelska-organizacia-varuje-pred-stahovanim-aplikacie-temu/.

[26] BBC. *British Airways fined £20m over data breach* [online]. 2020. [cit. 5.októbra 2024]. Dostupné na internete: https://www.bbc.com/news/technology-54568784.

peňazí z napadnutého účtu. Medzi najrozšírenejšie varianty patria napr. využitie spolupracovníkov, ktorým sú za percentuálny podiel na ich bankové účty (prípadne FinTechové aplikácie, ako sú PayPal, CashApp atď.) zasielané odcudzené finančné prostriedky, nákup drahých predmetov alebo darčekových kariet následne predávaných za hotovosť, výnimkou nie je ani nákup kryptomien a ich *de facto* okamžitý predaj za „čisté“ peniaze. Bankový podvod býva nezriedka kombinovaný aj s vyššie uvedeným klonovaním platobných kariet. Ide napr. o prípady, keď útočník získa kompletný prístup k bankovému účtu a následne pristúpi ku klonovaniu kariet s ním spojených na účel čo najrýchlejšieho výberu hotovosti.

Prelomenie bezpečnostnej bariéry v danom prípade vyžaduje pokročilejšie technologické znalosti rôznych procesov vedúcich k verifikácii identity páchateľov, ktorých analýza siaha nad rámec tohto článku. Uvedená zvýšená komplexnosť je pozorovateľná aj v dostupných štatistikách, podľa ktorých jednoduchšia forma trestnej činnosti využívajúca platobné karty (zväčša pri internetových platbách) stále predstavuje najatraktívnejší variant. Podľa najnovšieho spoločného reportu Európskej centrálnej banky a Európskeho orgánu pre bankovníctvo objem platieb s využitím kariet časovom rozmedzí od polovice roka 2022 do polovice roka 2023 dosiahol hodnotu takmer 22 miliónov, pričom u priamych prevodov medzi bankovými účtami daná metrika za rovnaké obdobie dosiahla menej než 5 miliónov. [27]

Záver

Sumarizujúc vyššie uvedený text možno zhrnúť, že tak, ako v mnohých iných oblastiach, aj v oblasti platobných kariet sa v súčasnosti pripravujú priam radikálne technologické zmeny, ktoré zmenia spôsoby, akými platíme za tovary a služby v online prostredí. Takéto platby majú výrazne vzrastajúci trend, pričom za posledné tri roky sa ich počet strojnásobil. Tomu zodpovedá aj určitý nárast počtu trestne stíhaných osôb za trestný čin neoprávneného vyrobenia a používania platobného prostriedku podľa § 219 Trestného zákona, pretože v roku 2021 bol ich počet 624, v roku 2022 – 717 a v roku 2023 – 766.[28]

V praxi boli zaznamenané konkrétne prípady zneužitia najmä platobných kariet, telefonického bankovníctva, tankovacej, resp. palivovej karty, Premia kariet k revolvingovým úverom a mnohých iných.

Základnými právnymi normami upravujúcimi predmetnú problematiku sú rámcové rozhodnutie 2001/413/SVV o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov, Trestný zákon a zákon č. 492/2009 Z. z. o platobných službách v znení neskorších predpisov.

V súčasnosti najsofistikovanejším spôsobom spáchania trestného činu neoprávneného vyrobenia a používania platobného prostriedku podľa § 219 Trestného zákona je zbieranie informácií na karte na účel neoprávnenej výroby platobného prostriedku, ide o tzv. *skimming,* keď páchateľ do bankomatu (alebo iného zariadenia, pri ktorom sa sníma čip karty) neoprávnene nainštaluje zariadenie umožňujúce kopírovanie údajov z karty (meno a priezvisko držiteľa karty, číslo karty, čas exspirácie a bezpečnostný kód CVC – *card verification code*) a zachytenie PIN kódu pomocou falošnej klávesnice alebo jeho nasnímania bankomatovou kamerou, pričom zneužitie platobnej karty je možné iba vtedy, ak sa podarí

[27] ECB. *Report on Payment Fraud* [online]. 2024. [cit. 5.októbra 2024]. Dostupné na internete: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf.
[28] Štatistické ročenky GP SR za roky 2021 – 2023.

získať PIN kód a údaje o platobnej karte. K ďalším formám zneužitia platobných prostriedkov patria *shimming, carding a spywar*, ktoré sú takisto obsahom tohto príspevku.

Literatúra

KLIMEK, Libor. Boj proti podvodom a falšovaniu bezhotovostných platobných prostriedkov na úrovni Európskej únie. In: *Justičná revue*. 2016. roč. 68, 2016, č. 1.

KLIMEK, Libor. Falšovanie bezhotovostných platobných prostriedkov v teórii a praxi. In: SZABOVÁ, Eva, Karin VRTÍKOVÁ a Ivana MOKRÁ. (eds.): *Tradičné a netradičné prístupy v trestnom práve. Zborník príspevkov z konferencie „Trnavské právnické dni 2024: Tradičné a netradičné v práve“*. Trnava: Typi, 2024. ISBN 978-80-568-0661-6.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání Plzeň: Aleš Čeněk, 2022.

ŠÁMAL Pavel a kol. *Trestní zákonník II. § 140 až 421. Komentář*. 1. vydání. Praha: C. H. Beck, 2010.

ŠÁMAL, Pavel, František PÚRY a Stanislav RIZMAN,*Trestní zákon – Komentář*. 5. vydání. Praha: C. H. Beck, 2003.

Štatistické ročenky GP SR za roky 2021 – 2023.

Elektronické dokumenty:

FinReport. *mBank po platbách prsteňom prináša aj platobné náramky* [online]. 2024. [cit. 25.októbra 2024]. Dostupné na internete: https://www.interez.sk/na-slovensko-prichadza-novy-typ-platby-znama-banka-svojim-klientom-poskytne-novinku/.

JAMNICKÝ, Martin. *Odhalili malvér, ktorý kradol údaje z platobných kariet.* [online]. 2024. [cit. 27. októbra 2024]. Dostupné na internete: https://uzitocna.pravda.sk/peniaze/clanok/721684/.

MARCIČIAK, Maroš. *Veľké zmeny pri platení cez internet. Bude bezpečnejšie, ale komplikovanejšie* [online]. 2024. [cit. 29. októbra 2024]. Dostupné na internete:https://www.techbyte.sk/2024/09/slovaci-zvyknut-platobne-karty-zmeny/.

ECB. *Report on Payment Fraud* [online]. 2024. [cit. 5. októbra 2024]. Dostupné na internete: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf.

FBI. *Skimming* [online]. 2024. [cit. 5. októbra 2024]. Dostupné na internete: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and scams/skimming.

FICO. *Card Skimming and Other Fraud Types Continue to Grow – US Dat* [online]. 2023. [cit. 5. októbra.2024]. Dostupné na internete: https://www.fico.com/blogs/us-card-skimming-grew-nearly-5x-2022-new-fico-data-shows.

FINREPORT. *Spotrebiteľská organizácia varuje pred sťahovaním aplikácie Temu*, [online]. 2024. [cit. 5. októbra 2024]. Dostupné na internete: https://www.finreport.sk/fintech/spotrebitelska-organizacia-varuje-pred-stahovanim-aplikacie-temu/.

HUMAN. *What is Digital Skimming?* [online]. 2023. [cit. 5. októbra 2024]. Dostupné na internete: https://www.humansecurity.com/learn/topics/what-is-digital-skimming.

INSIKT GROUP. *Annual Payment Fraud Intelligence Report: 2022* [online]. 2022. [cit. 5. októbra 2024]. Dostupné na internete: https://www.recordedfuture.com/research/annual-payment-fraud-intelligence-report-2022.

Keywords: means of payment, payment card, illegal production, possession, theft, fraud, skimming

Summary

In the scientific article in question, its authors focus attention on the current phenomenon of means of payment with an emphasis on payment cards. In connection with them, they describe the basic legislation, namely 2001/413/JHA Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, the Criminal Code and Act No. 492/2009 Coll. on payment services as amended. They also analyse specific ways of committing criminal offences related to means of payment in the Slovak Republic and abroad. Thus, they focus on the repressive but also the preventive aspects of the given issue.

doc. et. doc. JUDr. Ján Šanta, PhD., LL.M., MBA, MSc.
Generálna prokuratúra SR Bratislava
Právnická fakulta Trnavskej univerzity v Trnave
e-mail: jan.santa@genpro.gov.sk

Mgr. Ivo Šanta, LL.M, MBA, MSc.
finančný analytik a poradca
e-mail: ivosanta1997@gmail.com

JUDr. Matúš Husák
advokát
Advokátska kancelária Trlinská 541/66
Šenkvice
e-mail:husak.advokat@gmail.com

Recenzent: pplk. doc. JUDr. Veronika Marková, PhD.