Skimming jako jeden z druhů kybernetické kriminality[1]

JUDr. Štěpán Kalamár, Ph.D., JUDr. Mgr. Miroslav Petrák

Anotace: Trestná činnost související s neoprávněnými výběry peněz z bankomatů je již několik let na vzestupu. Pachatelé této trestné činnosti používají stále nové metody a postupy k překonání ochrany bankomatů. A i přes velmi dobré zabezpečení ze strany bankovních institucí není žádný klient 100% chráněn před útoky na identifikační data platební karty, včetně PINu. Jak se tyto útoky odráží v trestně právní rovině a jaká je praxe soudů? O tom pojednává tento příspěvek.

Klíčová slova: Bankomat, platební karta, identifikační údaj o platební kartě, PIN, skimming, skimovací zařízení, falešná čtečka bankovních karet, antiskimovací nástavec, termokamera, phishingová podložka, trestný čin, padělání nebo pozměnění platebního prostředku.

Abstract: Crime related to unauthorized withdrawals of money from ATMs has already been on the increase for several years. The perpetrators of this crime permanently use new methods and techniques to overcome the protection of ATMs. But despite tight security measures taken by banks clients can be hardly protected absolutely from attacks on their identification data of their payment cards, PIN included. So this contribution deals with the reflection of such attacks at the criminal justice level and also the court practice.

Keywords: ATM, payment card, identification data of credit card, PIN, skimming, skimming equipment, fake bank cards reader, anti-skimming tube, thermal camera, phishing pad, crime, forgery or fraudulent alteration of a payment means.

Úvod

Bankovní krádeže uskutečňované pomocí počítače jsou u nás zatím vyjímkou. Množí se ale útoky na bankovní domy prostřednictvím bankomatů. Typický bankomat ve svých útrobách shromažďuje hotovost o hodnotě (*průměrně*) kolem jednoho milionu korun. Čas od času se tedy jak samotný bankomat**,** tak případně klienti, kteří z něj zrovna vybírají, mohou stát obětí trestné činnosti. Podle evropského úřadu ENISA dochází ročně ke ztrátám v objemu kolem 12 mld. korun a trestná činnost tohoto typu zažívá prudký nárůst[2].

[1] Příspěvek byl zpracován v rámci Projektu vědeckovýzkumného úkolu č. 4/4, „Informační bezpečnost a kybernetická kriminalita v organizaci“, který je součástí Integrovaného výzkumného úkolu na léta 2010-2015, realizovaný Fakultou bezpečnostního managementu Policejní akademie České republiky v Praze.

[2] Viz. http://cs.wikipedia.org/wiki/Bankomaty,_platební_karty_a_trestná_činnost

Evropská unie pro zajištění vysoké a účinné bezpečnosti sítí a informací ve Společenství a vytvoření kultury bezpečnosti sítí a informací v zájmu občanů, spotřebitelů, podniků a organizací veřejného sektoru v Evropské unii (dále jen „EU“) a pro zajištění řádného fungování vnitřního trhu zřídila nařízením Evropského parlamentu a Rady (ES) ze dne 10. března 2004, č. 460/2004[3], „**Evropskou agenturu pro bezpečnost sítí a informací“** (*European Network and Information Security Agency*). Tato agentura (také známá pod zkratkou „**ENISA**“) je nápomocna Komisi Evropského parlamentu a členským státům, a proto spolupracuje s průmyslem, aby mu pomáhala splňovat požadavky bezpečnosti sítí a informací, včetně požadavků stanovených současnými a budoucími právními předpisy Společenství, například směrnicí 2002/21/ES[4], a zajišťovala tím řádné fungování vnitřního trhu.

Cíli a úkoly agentury nejsou dotčeny pravomoci členských států v oblasti bezpečnosti sítí a informací, které nespadají do oblasti působnosti Smlouvy o ES, jako pravomoci uvedené v hlavě V a VI Smlouvy o Evropské unii, a v každém případě činnosti týkající se veřejné bezpečnosti, obrany, státní bezpečnosti (včetně hospodářského blahobytu státu, souvisí-li taková činnost s otázkami státní bezpečnosti) a činnosti státu v trestněprávní oblasti.

Podle této agentury v Evropě hrozivým způsobem narůstají počty útoků a krádeží souvisejících s bankomaty. Jejich počet meziročně stoupl o 149 % a ročně tak dochází ke ztrátám zhruba 12 miliard korun. Podle ENISA je hlavní příčinou růst počtu bankomatů a stále chytřejší metody zlodějů.[5]

Není proto divu, že dne 5. října 2011 se v německém Frankfurtu konal vůbec první „**evropský summit o bezpečnosti elektronických plateb**“. Sešli se na něm vedoucí pracovníci členských bank Visa, představitelé obchodníků, dodavatelé technologií, zástupci orgánů činných v trestním řízení, regulátorů a státních úřadů z celé Evropy. Summit řešil otázky důvěry a bezpečnosti v novém světě digitálních a mobilních plateb. Na tomto evropském summitu o bezpečnosti elektronických plateb byl deklarován mezinárodní zájem o zamezení skimovaní platebních karet [„*V polovině července 2011 si celosvětové vyšetřování Europolu připsalo rozbití organizované skupiny podezřelé z držení naskimovaných údajích o více než 15 000 debetních a kreditních karet. Tato skupina se sídlem v Bulharsku je podezřelá z defraudování cca 50 mil. EUR od držitelů karet v Evropě (cca 1,25 mld. Kč.*“[6]].

[3] Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:CS:NOT [cit. 2012-02-17]

[4] Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:CS:HTML

[5] Dostupné na: http://byznys.lidovky.cz/kradeze-bankomatu-jsou-v-evrope-obrovskym-hitem-fuw-/moje-penize.asp?c=A090908_105029_moje-penize_mel [cit. 2012-02-17]

[6] TOMÁŠEK, František. Zadržení mezinárodního gangu podvodníků s kartami. *Cardmag*: *magazín nejen o kartách*. 2011, roč. 2011, č. 4, s. 33. Dostupné z: http://cardmag.cardzone.cz/aktual/pages/cze/archiv.html

Ponechme stranou způsoby, jimiž se pachatelé snaží dostat k cizím penězům, jako jsou krádeže celých bankomatů, které nejsou zabudované do zdi, za pomoci hrubé síly, krádeže platebních karet, kdy tzv. kapsáři vedle platební karty v peněženkách mnohdy nalezají i napsaný PIN kód (na papírku anebo i přímo na platební kartě), nebo loupežné přepadení klienta banky po výběru hotovosti z bankomatu. Příspěvek je zaměřen na způsoby neoprávněného zjišťování identifikačních údajů platebních karet, včetně PIN kódu.

Obecně se dá říci, že trestné činnosti související s neoprávněnými výběry peněz z bankomatů se dopouštějí převážně cizinci. Zaměřují se spíše na zahraniční banky a zahraniční klienty bank, kteří navštěvují Prahu, Brno, popř. i další velká města. K instalaci přistupují převážně z pátku na sobotu v časných ranních hodinách, kdy spoléhají na to, že blokaci platební karty lze provést nejdříve až v první pracovní den. Orientují se spíše do centra města, kde je velký pohyb turistů. Pro tyto pachatele není podstatné, zda je bankomat venku na ulici nebo uvnitř v uzvařeném prostoru. Držitel platební karty má sice dojem, že v uzvařeném prostoru je nejvíce chráněn a nikdo nepovolaný se do blízkosti bankomatu nemůže dostat a nadto je tento prostor ještě střežen kamerami. Opak je ovšem pravdou**.** Pachatelům této trestné činnosti vůbec nevadí, že je sleduje bezpečnostní kamera, protože po instalaci skimovacího zařízení se již pro toto zařízení nevrací. Nemají potřebu skimovací zařízení odinstalovat, aby si mohli přečíst načtená data, jak tomu bylo dříve. Dnes je toto zařízení v on-line provozu a sejmutá data skimovací zařízení odešle dalšímu příjemci v sms zprávě, který bezprostředně poté může jakoukoliv peněžní transakci nerušeně a bez rizika provést.

K útoku na bankovní účet poškozené osoby následně dochází mimo území státu, kde došlo k neoprávněnému získání identifikačních údajů o platební kartě**,** včetně PIN kódu, formou výběru peněz v hotovosti, popř. zaplacením zboží, služeb apod. Jedná se o jev celosvětový, viz následující příklady:

1. Tak např.: *„Policie v Novém Jižním Walesu eviduje případy, kdy cizinci zneužívají kartového platebního systému využitím skimingu. Tamní policie zatkla a obvinila pět malajsijských a srilanských státních příslušníků, podezřelých z propracovaného mezinárodního plánu skimování karet. Jejich aktivity se rozprostřely od Spojeného Království, kontinentální Evropy až po Severní Ameriku.“* [7]

2. *„Dne 7. prosince 2009 kolem deváté hodiny ráno oznamoval na linku 158 zaměstnanec kartového centra České spořitelny, a. s., že na bankomatu jejich peněžního ústavu umístěném ve vestibulu stanice metra Vysočanská v Praze 9 bylo prokazatelně umístěno skimovací zařízení. Všimla si ho žena, která se zde chystala provést výběr hotovosti. Na bankomatu se jí zdálo něco podezřelého, proto okamžitě informovala kartové centrum České spořitelny, a. s. Jejich*

[7] Dostupné na: http://cardmag.cardzone.cz/aktual/pages/cze/0_bezpecnost.html

pracovník podezření na místě potvrdil. Zjistil, že bankomat byl skutečně narušen nepovolanou osobou. Opodál si přitom všiml dvou mladých mužů, kteří v okamžiku, kdy byli zpozorováni, zařízení z bankomatu odinstalovali, schovali pod oděv a začali z místa rychle odcházet. Po jejich zadržení bylo zjištěno, že se jednalo o dva rumunsky hovořící muže ve věku 28 a 29 let.“ [8]

3. *Na policii se obrátili zástupci pobočky peněžního ústavu v Praze 4, podle nichž někdo na jejich bankomat naistanoval dne 19. dubna 2010 skimovací zařízení. Pachatel či pachatelé tak získali údaje z platebních karet několika klientů banky a na padělané karty pak o několik dní později vybírali peníze z bankomatů v Austrálii.*[9]

4. *Dva cizinci z Bulharska ve věku 29 a 32 let přibližně v prvních čtrnácti lednových dnech 2012 instalovali čtecí zařízení na tři bankomaty v oblasti Černého Mostu. Princip nelegálního počínání cizinců byl vždy stejný. Pirátské zařízení pokaždé na bankomat nainstalovali pouze na několik hodin. Přitom se zdržovali nedaleko a zařízení si hlídali*.[10]

Zvýšený počet těchto případů zaznamenávají kriminalisté Odboru hospodářské kriminality Krajského ředitelství policie hl. m. Prahy od **července roku 2009**. Od té doby jich stále přibývá. Jen za listopad jich bylo zaznamenáno kolem třiceti, což znamená prozatím naprosto enormní nárůst.[11]

Sběr dat z platební karty

Jedním ze způsobů, jak pachatelé zjišťují PIN[12] kód při běžném použití bankomatu**,** je sběr dat z platební karty, tzv. skiming[13] (z angl. data skimming – sbírání dat). K tomu se používá tzv. skimmovací zařízení, které je schopno PIN zjistit např. při dotazu na zůstatek v bankomatu. Pachatelé skimmovací zařízení instalují přímo do otvoru pro kartu

Skimming = v současnosti jeden z nejčastějších způsobů zneužití platebních karet. Podvodníci na určitou dobu umístí na bankomat speciální čtecí zařízení, které kopíruje data z magnetického proužku karty. Většinou tuto čtečku doprovází miniaturní kamera pro snímání PINů. Získané informace umožní podvodníkům vyrobit padělek karty.

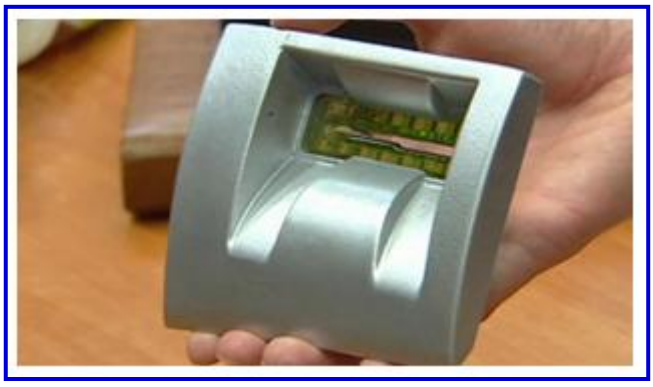
[8] Dostupné na: http://www.policie.cz/clanek/skimovacich-zarizeni-pribyva.aspx
[9] Dostupné na: http://www.novinky.cz/krimi/199671-policie-zadrzela-muze-ktery-u-bankomatu-kopiroval-karty.html
[10] Dostupné na: http://www.regiony24.cz/14-145220-prazsti-policiste-zadrzeli-dva-cizince--na-bankomaty-montovali-skimovaci-zarizeni
[11] Dostupné na: http://www.policie.cz/clanek/skimovacich-zarizeni-pribyva.aspx
[12] PIN je akronym z anglického personal identification number (osobní identifikační číslo). Jde o identifikátor, jímž se lze autorizovat např. u platebních karet, mobilního telefonu atd. Nejčastěji je tvořeno čtyřmi čísly, které se musí zadat při zapnutí předmětu. PUK (z angl. personal unlocking key) je pak tzv. osobní odblokovací kód, který slouží při nadlimitním zadání PINu.
[13] Dostupné http://finance.idnes.cz/ani-antiskimmovaci-zarizeni-vase-karty-stoprocentne-neochrani-hrozba-trva-1bu-/bank.aspx?c=A071121_164225_fi_osobni_fib

v bankomatu. Běžný uživatel si jej vůbec nevšimne. Při jeho použití zpravidla nedochází k fyzickému odcizení platební karty, poškozený se o vzniklé újmě nedozví okamžitě.

Skimmovací zařízení je v převážné většině případů tvořeno z části, která dokáže přečíst magnetickou kartu při jejím vložení do bankomatu, a z části (např. minikamera či upravená klávesnice), která sejme PIN kód zadaný uživatelem bankomatu (viz obr. č. 1). Čísla 3 a 4 na obrázku značí umístění skimovací zařízení. Pachatelé se při své činnosti zaměřují výhradně na určité typy bankomatů, na které lze skimovací zařízení nainstalovat. Jedná se o jakousi část, popř. sestavu elektronického zařízení (např. minikamera či upravená klávesnice), které se stane součástí bankomatu a které sejme identifikační údaje karty včetně PIN kódu. Dokáže tedy po vložení platební karty do bankomatu přečíst jeho magnetickou část a odeslat SMS zprávu o údajích z karty a PINu.

Obr. č. 1 Umístění skenovacího zařízení do otvoru pro kartu[14]

Skimovací zařízení jsou stále dokonalejší, takže nemusí být laickým pohledem rozpoznatelná. Na obr. 2 a 3 je vidět skimovací zařízení nalezené u rumunsky hovořících mladíků.



Obr. č. 2 – Falešná čtečka bankovních karet - nástavec na otvor bankomatu pro vložení karty, stejné barvy jako bankomat[15].

[14] Dostupné na. http://www.policie.cz/clanek/podezrele-bankomaty.aspx

Obr. č. 3 – **D**etail elektronického skimmovacího zařízení pro čtení magnetické pásku platební karty[16]

Mnohé české banky právě kvůli tomuto typu útoků začaly inistalovat ochranná zařízení (FDI - Fraudulent Device Inhibitor) pro štěrbinu na vkládání karty do bankomatu (viz obr. č. 4).

Obr. č. 4 - Antiskimovací nástavec zelené bary, které brání skimovaní karet[17]

Antiskimovací nástavce zelené barvy na štěrbinu, do které klient vkládá kartu při výběru z bankomatu. Česká spořitelna, a. s., začala ve velkém instalovat antiskenovací zařízení již od roku 2004 jako reakci na růst tohoto typu podvodu.[18]

Ačkoli banky stále zvyšují ochranu bankomatů před útoky podvodníků na data z karet a tedy i peníze, nový případ potvrzuje, že každá ochrana je překonatelná.

Česká spořitelna, a. s., na podzim roku 2009 zaznamenala útok na bankomat, který měl nainstalované zařízení zabraňující zkopírování údajů z platební karty, takzvané **antiskimovací zařízení**. Podvodníkům se podařilo získat data karet

---

[15] Dostupné na: http://www.ceskatelevize.cz/ct24/domaci/152665-policie-sleduje-dalsi-skimovaci-gang-v-praze/

[16] Dostupné na: http://www.policie.cz/clanek/skimovacich-zarizeni-pribyva.aspx

[17] Dostupné na: http://finance.idnes.cz/ani-antiskimmovaci-zarizeni-vase-karty-stoprocentne-neochrani-hrozba-trva-1bu-/bank.aspx?c=A071121_164225_fi_osobni_fib

[18] Dostupné na: http://www.rozhlas.cz/radiozurnal/publ_izurnal/_zprava/111782?print=1

a posléze i peníze více než desítky klientů. Peníze podvodníci vybírali v Polsku.[19] Při zběžném pohledu to nebylo patrné. Kamerka byla nad klávesnici a čtečka údajů z karty byla na původním antiskimovacím nástavci, ale byla z podobného materiálu a ve stejné barvě.

Pachatelé, kteří se této trestné činnosti dopouštějí**,** se zaměřují spíše na zahraniční banky a zahraniční klienty bank, kteří navštěvují naši metropoli. Orientují se přitom spíše do centra města a na turisticky atraktivní místa. Prozatím si vybírali výhradně bankomaty, které jsou umístěny přímo u peněžních ústavů, ať už venku na ulici, anebo vevnitř v uzavřeném prostoru. Tato místa jsou totiž pro toho, kdo si jde vybrat hotovost, nejvíce důvěryhodná. Spoléhá na to, že jsou zde nainstalovány kamery a kromě držitele platební karty se za uzavřené dveře nikdo nepovolaný nedostane. Opak je ale pravdou. Pachateli nevadí, že je sledován kamerou. Ke své činnosti si dokonce vyhradí dostatek časového prostoru. Instalace zařízení mu trvá i dvacet minut. V uzavřených prostorách má navíc na „práci" klid. Pro skimovací zařízení, jako tomu bylo dříve, se zpět nevrací. Nepotřebuje si totiž odnést data na nosiči. Skimovací zařízení je naopak on-line pošle dalšímu příjemci, který může peněžní transakci k výběru hotovosti nerušeně provést. Zařízení pachatelé instalují výhradně z pátku na sobotu v časných ranních hodinách. Zaměřují se přitom na zahraniční banky a spoléhají, že zablokování karty zahraničním turistou lze provést až v pracovní dny. K výběru hotovosti tak získají dostatek času.

Poté, co dobře sehraná skupina zjistí PIN kód, odčerpá peníze z účtu zpravidla mimo území České republiky (např. zaplacením zboží, úhradou hotelové služby atp.**).**

Pachatelé skimmovací zařízení instalují přímo do otvoru pro kartu v bankomatu. Běžný uživatel si jej nevšimne.

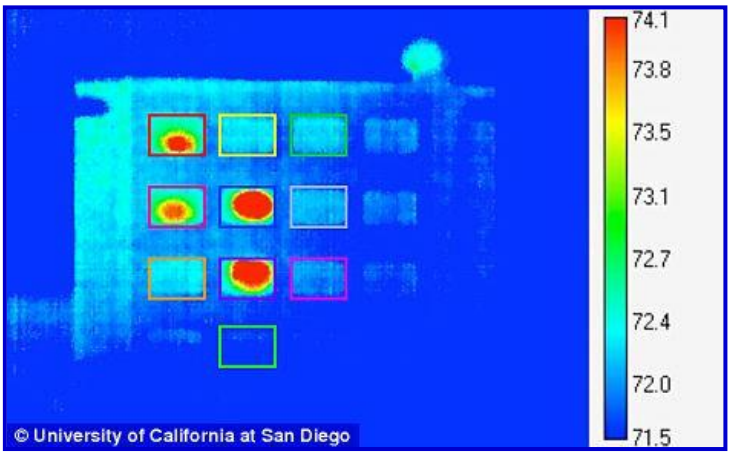
Dalším způsobem, jak neoprávněně zjistit PIN kód, je použití speciální fólie (*podložky*), viz obr. č. 5, která se umístí na klávesnici, popřípadě za použití klasickou miniaturní (*mikro*) kamery nebo termokamery.

Útočník vloží na klávesnici, kde se zadává PIN „fake" (*podvodnou*) klávesnici, která zaznamenává vaše stisky, ale zároveň promačkává na reálnou, skutečnou klávesnici. Provedení bývá dokonalé a k nerozeznání ani při podrobnějším prozkoumání.

[19] Dostupné na: http://byznys.lidovky.cz/podvodnici-obesli-novou-ochranu-bankomatu-ceske-sporitelny-pr0-/moje-penize.asp?c=A091126_162730_ln_domov_kim

Obr. č. 5 - Phishingová podložka[20]

Velmi efektní je i použití termokamery. Při zadávání PINu zůstává na klávesnici zbytkové teplo z doteku prstu, toto teplo je měřitelné až do 40 sekund po doteku! Přijde-li útočník do půl minuty po výběru z bankomatu, tak pomocí termokamery sejme termo otisk a zná váš pin. ***Podle chladnutí lze rozeznat i pořadí stisku kláves*** (viz obr. č. 6).



Obr. č. 6 - Sejmutí obrazu termokamerou[21]

Zvýšený počet těchto případů zaznamenávají kriminalisté Odboru hospodářské kriminality Krajského ředitelství policie hl. m. Prahy od července roku 2009. Od té doby jich stále přibývá. Jen za listopad roku 2009 jich bylo zaznamenáno kolem třiceti, což znamenalo enormní nárůst.

Pro úplnost je nutné ještě uvést jeden ze starších útoků na bankomaty pomocí tzv**. *libanonské smyčky***[22] (viz obr. č. 7). Tento útok spočívá ve zhotovení poměrně

[20] Dostupné na: http://www.kdosiodjinud.cz/bezpecnost-bank-cast-1-bankomaty.a201.html
[21] Dostupné na: http://www.kdosiodjinud.cz/bezpecnost-bank-cast-1-bankomaty.a201.html
[22] *J. Krhovják, M. Kumpošt, V. Matyáš. Útoky na platební systémy. Zpravodaj ÚVT MU. ISSN 1212-0901, 2007, roč. XVIII, č. 1, s. 10-17.* Dostupné na: http://www.ics.muni.cz/bulletin/articles/562.html

jednoduchého přípravku, který je upraven pomocí pásky z videokazety tak, aby při vložení platební karty do štěrbiny bankomatu kartu zachytila a nenechala jí propadnout do systému. Tento přípravek se poté umístí na otvor bankomatu určený pro vkládání platebních karet. Celý trik pak spočívá v tom, že když přípavek kartu zadrží (nepropadne do systému) a proto ji nelze ani vysunout ven, tak k oběti přistoupí útočník a poradí jí opětovné vložení PINu, který odpozoruje. Jakmile oběť odejde problém s platební kartou reklamovat, vytáhne útočník kartu z bankomatu a s pomocí odpozorovaného PINu odcizí z účtu peníze, které je schopen bankomat vydat na jeden výběr, ještě před zablokováním karty.

Obr. č. 7 - Přípravek na zadržení platební karty - tzv. „libanonská smyčka“[23]

Trestněprávní ochrana

Nelegální opatřování PIN kódu lze postihnout jako trestný čin „*Neoprávněné opatření, padělání a pozměnění platebního prostředku“* podle ustanovení § 234 trestního zákoníku. *Základní* skutková podstata tohoto trestného činu spočívá v jednání pachatele, který „*sobě nebo jinému bez souhlasu oprávněného držitele* ***opatří, zpřístupní, přijme*** *nebo* ***přechovává*** *platební prostředek jiného, zejména* ***nepřenosnou platební kartu*** *identifikovatelnou podle jména nebo čísla …“.*

Přísněji trestný (ačkoliv jde opět o základní skutkovou podstatu) pak bude ten, kdo sobě ***opatří, zpřístupní, přijme*** *nebo* ***přechovává*** *<u>již **padělaný platební prostředek**</u>.*

Dalšími okolnostmi, které jsou zákonnými (obligatorními) znaky skutkové podstaty tohoto trestného činu a které umožňují použití trestněprávní kvalifikace s vyšší trestní sazbou, jsou:

- ***padělání nebo pozměnění platebního prostředku*** *v úmyslu použít jej jako pravý nebo* ***použití padělaného nebo pozměněného platebního prostředku*** *jako pravého nebo platného,*

[23] Dostupné na: http://finance.idnes.cz/ani-antiskimmovaci-zarizeni-vase-karty-stoprocentne-neochrani-hrozba-trva-1bu-/bank.aspx?c=A071121_164225_fi_osobni_fib

- *spáchání tohoto činu (podle odstavců 1, 2 a 3) v postavení* ***člena organizované skupiny*** *nebo spách****ání*** *takov****ého*** *čin****u ve značném rozsahu****,*
- *spáchání výše uvedeného činu jako* ***člen organizované skupiny působící ve více státech*** *nebo spáchání takového činu* ***ve velkém rozsahu***.

Kontakty:

JUDr. Štěpán Kalamár, Ph.D.

tajemník fakulty bezpečnostně právní,
Policejní akademie České republiky v Praze
e-mail: kalamar@polac.cz

JUDr. Mgr. Miroslav Petrák

Okresní státní zastupitelství v Jindřichově Hradci
e-mail: mpetrak@osz.jhr.justice.cz