На № 2719/0411-06-1
23.08.2013
№ 03/08/ДСФМУ-2013

Голові Державної служби
фінансового моніторингу
України Гуржію С. Г.

Копія: Заступник Голови
Національного банку України
О. О. Ткаченко

Шановний Сергію Григоровичу!

Бажаємо успіхів в Вашій професійній діяльності та щиро дякуємо за співпрацю з членами платіжних систем в сфері протидії та попередження платіжних злочинів.

Надаємо консолідовані відповіді на питання для підготовки типологічного дослідження на тему «Типологічні схеми легалізації (відмивання) доходів, пов'язаних із злочинами у сфері кіберзлочинності».

1. Які, на вашу думку, найбільші ризики та загрози для фінансової системи України несе кіберзлочинність?

Основним об'єктом, на який спрямовані кіберзлочини, є економічна безпека держави, тому що платіжні інструменти забезпечують безпосередній (в т.ч. он-лайн) доступ до банківських рахунків, а недовіра громадян до надійності фінансової системи та національної грошової одиниці в результаті кіберзлочинів є дуже небезпечним фактором для української економіки. Кіберзлочинність гальмує розвиток безготівкових розрахунків та є додатковим чинником нелегальної економічної діяльності (сіра, чорна економіка) завдяки сприянню використанню готівки. Таким чином кіберзлочинність заважає використанню Урядом України механізмів покращення фінансового стану країни, наповненню державного бюджету та виконання Урядом та Президентом Україні Програми соціально-економічного розвитку країни.

2. Які головні чинники (у тому числі особливості українського законодавства), на вашу думку, сприяють поширенню кіберзлочинності в Україні?

- декларативність організаційних засад боротьби з кіберзлочинністю, в т.ч., відсутність спеціалізованого підрозділу в структурі Головного слідчого управління та ДНДЕКЦ МВС України, відсутність ефективної координації діяльності між різними департаментами та управліннями кримінальної міліції, кримінальної міліції, ГСУ та Генпрокуратури.
- не відповідність окремих положень українського кримінального законодавства міжнародним зобов'язанням України, наприклад, ст.200, 231, 361 Кримінального кодексу України мають відповідати Амстердамському Договору ЄС в частині криміналізації діянь та уніфікації відповідальності за їх здійснення.
- не узгодженість окремих положень нормативно-правових актів Національного банку України, Закону України "Про платіжні системи та переказ грошей в Україні, Закону України "Про електронний цифровий підпис", наприклад, щодо неналежних переказів та договірного списання, ЕП та ЕЦП.
- відсутність керівних роз'яснень Вищого спеціалізованого суду України з розгляду цивільних та кримінальних справ, як в частині узагальнення судової практики, так і формування стандартизованого підходу до розгляду справ щодо кіберзлочинів.
- відсутність скоординованої діяльності Державної судової адміністрації, Академії підвищення кваліфікації Генпрокуратури та Національної Академії внутрішніх справ в частині спільного підвищення кваліфікації фахівців за напрямком боротьби з кіберзлочинністю.
- Відсутність оверсайту з боку Національного банку України (або іншої наглядової інстанції) за компаніями, які надають послуги з розробки програмних комплексів для дистанційного-банківського обслуговування. За наявності в Україні реєстру програмного забезпечення для систем ДБО сертифікованого НБУ (за його дорученням), можливо було б уникнути поточних проблем, пов'язаних із використання значною кількістю банків однотипного "проблемного" програмного забезпечення.
- Відсутність стимулювання та/або оверсайту з боку Національного банку України за використанням українськими банками платіжних інструментів, технологічні особливості яких (наприклад, магнітна смуга платіжної картки) сприяють тому, що до кібер-злочинності долучається молоде покоління українців (переважно студенти).

3. Надайте, будь ласка, інформацію (короткий опис) найбільш типових видів кіберзлочинів у банківській сфері України.

1) Банкоматне шахрайство:
1.1) скіммінг – копіювання інформації з магнітної смуги ПК та отримання ПІН-коду до неї
1.2) використання «білого пластику» для зняття готівки в банкоматах
1.3) Transaction Reversal Fraud - втручання в роботу банкомату при здійсненні операцій видачі готівки, яке залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником.
1.4) Cash Trapping - заклеювання диспенсеру для привласнення зловмисником готівки, яка була списана з карткового рахунку законного Держателя картки.

2) Шахрайство в торгівельно сервісних-підприємствах:
2.1) укладання фіктивних угод торгівельного еквайрингу для обслуговування підробних платіжних карток;
2.2) викрадення реквізитів платіжних карток,
2.3) підлімітні операції без авторизації.
2.4) використання втрачених /викраденних / підроблених платіжних карток

3) Шахрайство в середовищі Інтернет:
3.1) викрадення реквізитів платіжних карток,
3.2) проведення операцій з використанням викрадених реквізитів платіжних карток.

4) Шахрайство в системах Дистанційного банківського обслуговування:
4.1) проведення несанкціонованих операцій в системах дистанційного банківського обсуговування,
4.2) відкриття рахунків та отримання готівки в результаті несанкціонованих операцій в системах ДБО.
4.3) отримання платежів від закордонних відправників через міжнародну систему SWIFT в наслідок втручання у роботу комп'ютерів ти систем ДБО клієнтів закордонних банківських установ

4. За наявності, надайте інформацію (короткий опис) щодо кіберзлочинів, які мали міжнародний характер (але водночас стосувались і банківського сектору України).

Всі чотири вищеописані види кіберзлочинів носять міжнародний характер і представлені в усіх країнах світу в тій чи іншій мірі, в залежності від поточних тенденцій шахрайства в конкретному регіоні. Крім того, всі вищеописані види злочинів носять трансграничний характер, коли початок злочину може мати місце в одній країні, а його завершення в іншій. Наприклад, копіювання картки іноземного емітента мало місце за кордоном, а зняття готівки по «Білому пластику» в Україні, і, навпаки. Такі практичні приклади існують і можуть бути наведені щодо кожного із чотирьох вищевказаних типів шахрайства.

5. Які види шахрайства зі спеціальними платіжними засобами є найпоширенішими в Україні (у разі можливості, наведіть приклади)?

Тенденції шахрайства із спеціальними платіжними засобами останніх років свідчать про те, що, незважаючи на стрімке зростання шахрайства в системах ДБО та мережі Інтернет, найпоширенішими за кількістю інцидентів в Україні залишаються шахрайства з банкоматами. Так, наприклад, кількість виявлених фактів встановлення скімінгових пристроїв за 2-ий квартал 2013р. зросла в 8 разів в порівнянні з аналогічним періодом 2012р. (Додаток 2)

6. Наскільки поширеними, на вашу думку, є кіберзлочини із використанням платіжних систем. (За наявності, вкажіть їх найпоширеніші види, надайте їх короткий опис, наведіть приклади)?
Кіберзлочини із використанням платіжних систем, у тому числі із використанням платіжних карток, доволі поширені у рамках фінансових організацій. Оскільки у фінансовій сфері кіберзлочини направлені на отримання фінансової вигоди, а платіжні системи використовуються як інструменти переводу та переведення викрадених коштів у готівкову форму. Серед найпоширеніших можна відмітити:
- випадки скіммінгу у банкоматній та торговельних мережах з подальшим використанням підроблених платіжних карток клієнтів
- отримання реквізитів платіжних карток для їх несанкціонованого використання у мережі Інтернет для купівлі товарів та оплати послуг. Отримання реквізитів платіжних карток може відбуватись як через втручання у роботу комп'ютера клієнта, так і через зломи платіжних сервісів інтернет-магазинів

- несанкціоновані переводи з систем ДБО з використанням ідентифікаційних реквізитів клієнтів. Кошти від банка-відправника до банка-отримувачі відправляються через НСМЕП
- отримання платежів від закордонних відправників через міжнародну систему SWIFT в наслідок втручання у роботу комп'ютерів ти систем ДБО клієнтів закордонних банківських установ

7. **Які зміни до законодавства України, на вашу думку, можуть сприяти зменшенню кількості випадків шахрайства зі спеціальними платіжними засобами, платіжними системами?**

1. **Встановлення відповідальності за злочини в сфері підробки та використання підроблених платіжних карток** випливає з міжнародних зобов'язань України в т.ч. має відповідати Амстердамському Договору ЄС в частині криміналізації діянь та уніфікації відповідальності за їх здійснення. В Європі відсутні країни, в яких підробка та/або використання підроблених платіжних карток карається штрафом.
Рентабельність такого «бізнесу», як і відсутність належного покарання сприяє масовому туризму до України міжнародних злочинних угруповань і призводе як до суттєвих проблем в середині країни (протягом 2013 року більше 50 осіб, затриманих під час встановлення в банкомати обладнання для підробки платіжних карток було відпущено судами з причини того, що ст.200 ККУ не є "тяжкою" статтею), а й до погіршення міжнародного іміджу України.
В зв'язку із вищезазначеним доцільно внести до Верховної Ради України законопроект щодо ст.200 КК, виклавши її в такій редакції:

Стаття 200. Незаконні дії з платіжними інструментами

1. Підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а також придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ чи платіжних карток, електронних грошей або їх використання чи збут - караються позбавленням волі на строк від трьох до п'яти років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або службовою особою чи працівником, яким відомості про платіжні інструменти стали відомі по службі чи роботі, - караються позбавленням волі на строк від чотирьох до восьми років з

позбавленням права обіймати певні посади чи займатися певною діяльністю на строк від одного до трьох років або без такого.

3. Дії передбачені частиною першою або другою цієї статті, вчинені організованою групою, - караються позбавленням волі на строк від шести до десяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк від одного до трьох років або без такого.

2. Щодо порядку дій банка отримувача та банка платника при неналежному переказі із використанням систем ДБО з рахунку неналежного платника, доцільно внести до Інструкції про безготівкові розрахунки в Україні в національній валюті, норми вже передбачені Законом України "Про платіжні системи та переказ коштів в Україні" - про договірне списання та неналежні перекази та доповнити розділ "Розрахунки за допомогою систем дистанційного обслуговування" відповідним поєднанням механізму договірного списання та відкладальной умови (надходження на рахунок неналежного отримувача неналежного переказу з рахунку неналежного платника). Це дозволить відповідно до положень Закону України "Про платіжні системи та переказ коштів в Україні" своєчасно та без залучення судових процедур повертати суми неналежних переказів на банківські рахунки осіб з яких вони були неправомірно списані.

Щодо програмно-технічних засобів безпеки систем ДБО, доцільно внести до інструкції про безготівкові розрахунки в Україні в національній валюті, вимоги про те, що має проводитись двоканальна аутентифікація та обов'язкове online-інформування клієнтів про кожну проведену операцію, за аналогією з вимогами до інформування, передбаченими до операцій з платіжними картками. Також доцільним є внесення до нормативно-правового акту НБУ про оверсайт процедури контролю діяльності постачальників програмного забезпечення для систем ДБО.

Щодо керівних роз'яснень Вищого спеціалізованого суду України з розгляду цивільних та кримінальних справ, відносно стандартизованого підходу до розгляду справ щодо використання підроблених карток у банкоматній мережі України. Додаток 1

8. Чи траплялись у ваші практиці випадки викрадення персональних даних клієнтів вашого банку, що спричиняло скоєння кіберзлочину(ів) (за можливості, наведіть приклади)?

Мова іде про інсайдерство, а саме зловживання службовим становищем шляхом копіювання та подальшого неправомірного використання внутрішніх баз даних про клієнтів для проведення будь-яких фінансових операцій або інших дії від імені клієнтів, направлених на зміну стану їх майнових прав. Такі випадки траплялися в банківській системі України.

9. Яким чином банками здійснюється перевірка та виявлення фінансових операцій, що можуть бути пов'язані з кіберзлочинністю (надайте, будь ласка, короткий опис відповідного порядку)?

У відповідності до вимог Закону України "Про платіжні системи та переказ грошей в Україні"
Банки приймають участь в міжбанківському обігу (Exchange-online: опис на ema.com.ua) та використанні наступної інформації:
- про неправомірне або не передбачене законами України, правилами, договорами використання фізичними й юридичними особами платіжних інструментів та платіжних систем, ПТКС, АТМ, платіжних терміналів, обладнання, програмного забезпечення, придатного для компроментації ключової інформації, засобів доступу до банківських рахунків, підробки платіжних карток, електронних грошей, неправомірні дії у сфері надання позик, кредитів в т.ч. шахрайство з фінансовими ресурсами, фіктивне підприємництво, незаконні дії з застосуванням платіжних систем, засобів доступу до банківських рахунків, електронних грошей тощо;
- історії авторизації, моніторинг інформації в сфері застосування банківських рахунків для розрахункових, кредитних операцій та переказів, результати аналізу інформації, які сприяють належній ідентифікації платників, отримувачів, суб'єктів правовідносин банківського вкладу (включаючи правовідносини позики, кредитування і розрахунків з використанням документів на переказ та спеціальних платіжних засобів),
- фото /відео інформації тощо.

Аналіз та використання підрозділами банку зазначеної інформації проводиться з метою:
- попередження збитків і мінімізація ризиків банківської системи в сфері функціонування в Україні платіжних систем;

- належна ідентифікація платників, отримувачів - суб'єктів правовідносин банківського рахунку (включаючи правовідносини позики, кредитування і розрахунків з використанням документів на переказ та спеціальних платіжних засобів), що є передумовою запобігання та протидії легалізації доходів, одержаних зазначеними особами в результаті неналежних переказів, переказів здійснених неналежними платниками;

	платіжних карток	банкоматів	платіжних терміналів	Роздрібне кредитування
Українські банки всього:	30 345 238	36 864	172 308	100%
Українські банки (69), користувачі Exchange-online	28 613 943	34 518	158 520	90%+
Користувачі Exchange-online - платіжні агрегатори : PayU, Portmone, Liqpay, Ipay, UPC, EasyPay				

10. Які ознаки (критерії), на вашу думку, можуть використовуватись банком для виявлення фінансових операцій, пов'язаних з кіберзлочинністю?

Індикатори можливого відмивання коштів, які можуть стати підставою для внутрішнього фінансового моніторингу

– використання для банківських операцій Ір-Адрес й імен користувачів за якими попередній платіжний моніторинг виявив причетність до неправомірних операцій;
– незвичайні умови або складність операції: висока частота грошових переказів протягом невеликого періоду часу, велика кількість різноманітних джерел походження коштів і платіжних методів (інструментів);
– відсутність явного взаємозв'язку між операцією й характером діяльності клієнта юридичної особи;
– відсутність точної інформації про підприємницьку діяльність клієнта або використання клієнтом виключно системи Інтернет платежів;

– поведінка особи не відповідає характеру чиненої операції або не заслуговує довіри;
– особі потрібна допомога в заповненні документів для виконання банківської операції або воно не може їх заповнити;
– особа не інформована про характер діяльності юридичної особи, яку він представляє;
– особа не може пояснити необхідність надання тієї або іншої банківської послуги;
– особа вимагає надзвичайно високі ліміти (особливо для трансграничних операцій), які не відповідають обороту особи, його попередній фінансовій поведінці або профілю клієнтів, до яких відноситься цей клієнт;
– особа вимагає видати йому дві й більш банківських карток, що не відповідає природі діяльності особи або її обороту або моніторинг платіжних операції виявив явне використання таких карток різними особами (власником рахунку та іншою особою);
– особа не має інформацію про справжніх власників юридичної особи, яку представляє, місці знаходження або не має у своєму розпорядженні контактні дані;
– особа не може вказати партнерів юридичної особи й/або сферу її діяльності;
– особа прагне відкрити рахунок у філії банку в одному районі/місті, у те час як адреса й місцезнаходження представника або юридичної особи — в іншому місці, і не надане зрозумілого пояснення цьому факту;
– внесення коштів на рахунок особи/компанії, у якої низький рівень оборотів або не було нікого значного росту оборотів;
– міжнародні перекази на ім'я особи не відповідають профілю клієнта (не було раніше, з "екзотичної" країни, з країни, з якої в останній час надходять перекази в рамках шахрайських схем);
– міжнародні перекази з подальшими переказами по Україні в короткий проміжок часу або зняттям готівки (в касі, в АТМ) ;
– операція не відповідає попереднім операціям клієнта;
– постійні операції на суму нижче граничного для запобігання декларування джерела походження; велика сума переказів/ операцій;
– видаткові операції по рахунку з підключеною системою Інтернет платежів здійснюються переважно у формі зняття готівки;
– кошти вносяться переважно в готівковій формі або інструментами, схожими на готівку (наприклад, наперед оплачені картки, ЕГ); сума нижче граничного значення;

– внесення коштів на рахунок здійснюється третьою особою після чого негайно здійснюється зняття готівки через касу (АТМ) або переказ коштів із застосуванням системи Інтернет платежів ;
– переказ коштів з іноземних держав, у комбінації з не підтвердженими даними про одержувача, платника або джерело походження коштів;
– тривалі комерційні відносини або здійснення операції без особистої присутності клієнта;
– перекази між банківськими рахунками зв'язаних осіб;
– операції, пов'язані з великою кількістю вхідних/вихідних переказів без логічної або явної мети;
– непояснені клірингові (залікові) операції між двома чи більше особами;
– використання рахунків для одержання переказів і для їхнього подальшого переказу на адресу тих самих платників;
– трансграничні схеми: поповнення рахунку в країни А\ зняття готівки (АТМ) в країні Б;
– платіжні операції (суми, кількість) послідовно збільшується та мають місце у відношенні однієї особи або компанії, особи або компанії, чиї імена/найменування співзвучні або вони є пов'язаними особами;
– підприємство з незначним оборотом або заново створене отримує перекази на значні суми, що не відповідає профілю клієнта;

Додаток 1

Підготовлено робочою групою Асоціації з «Уніфікації кримінальної відповідальності за карткові злочини»

Проблеми кваліфікації використання підроблених карток («білого пластику») у банкоматній мережі України

Проблеми правової кваліфікації використання «білого пластику» у банкоматній мережі України лежать передусім у площині відсутності єдиного підходу у слідчих та судових органів до кваліфікації цього злочинного прояву. Звідси - неоднаковість підходів до застосування кримінального законодавства у цілому, в результаті чого порушується насамперед конституційний принцип рівності усіх, в т.ч. і перед законом і судом (ст.24 Конституції України). На практиці складається ситуація, коли за відсутності жодного роз'яснювального акту вищих органів судової влади, за тотожні склади злочинів карають по різним статтям ККУ виходячи зі свого власного розуміння слідчих та суддів суті правовідносин у цій сфері. Підтвердженням є наявність вироків, що набрали законної сили, одночасно по таким статтям ККУ:

- по ст. 200 ККУ за незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення;
- по ч.3 ст.190 ККУ за шахрайство вчинене шляхом незаконних операцій з використанням електронно- обчислювальної техніки;
- за сукупністю у варіаціях за ст. 200 ККУ та ч.3 ст.190 ККУ, а інколи й іншими суміжними статтями ККУ.

При кваліфікації використання "білого пластику" в банкоматній мережі **виключно за ст.200 ККУ** фактично охоплюється лише перша складова злочинного ланцюжку - стадія виготовлення. Друга стадія - заволодіння чужим майном залишається некараною, хоча на перший погляд диспозиція статті охоплює увесь злочин. Об'єктивна сторона злочину, передбаченого ст. 200 полягає у: 1) підробці; 2) придбанні; 3) зберіганні; 4) перевезенні; 5) пересиланні: 6) використанні чи 7) збуті підроблених документів на переказ чи платіжних карток. Склад злочину – формальний. Коментар до статті надає розширене тлумачення поняття «використання»: під використанням підроблених документів на переказ чи платіжних карток слід розуміти пред'явлення їх як справжніх з метою здійснення незаконного переказу грошових коштів, незаконного доступу до інформації щодо відповідного банківського рахунка тощо. Використанням підробленої платіжної картки слід вважати також спробу отримання з її допомогою грошових коштів через банківський автомат, здійснення з її застосуванням оплати товарів чи послуг. Якщо ж внаслідок використання підроблених предметів особа, яка їх використала, заволодіває чужими грошовими коштами, вчинене слід кваліфікувати як сукупність злочинів за відповідними частинами ст. ст. 190 і 200. Отже, маємо пряму вказівку на необхідність додаткової кваліфікації майнового злочину за окремою статтею з матеріальним складом. У коментарі не надається уточнень з приводу місця, способу заволодіння чужими грошовими коштами, тобто в цілому не до кінця враховується специфіка суспільних відносин у сфері обігу платіжних карток. Проте це також має вирішальне значення при кваліфікації і виборі того, яка саме «корислива» стаття має бути інкримінована у сукупності із ст. 200 ККУ. Більш глибоко думка проаналізована в розрізі проблем кваліфікації за ч.3 ст.190 ККУ.

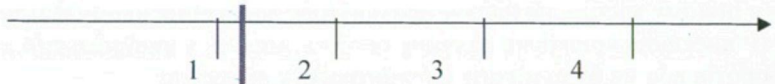
Крім цього, при кваліфікації виключно за цією статтею з'являється недолік ще й процесуального характеру – неможливість взяття під варту злочинців, особа та місцезнаходження яких не викликають у правоохоронних органів жодних сумнівів, в силу того, що стаття 200 ККУ не є тяжкою, або принаймні статтею із санкцією у вигляді позбавлення волі. Згідно з ст.155 КПКУ: «Взяття під варту як запобіжний захід

застосовується в справах про злочини, за які законом передбачено покарання у вигляді позбавлення волі на строк понад три роки. У виняткових випадках цей запобіжний захід може бути застосовано в справах про злочини, за які законом передбачено покарання у вигляді позбавлення волі і на строк не більше трьох років».

Проблема «збитків та спрямованості умислу», що виникає **при кваліфікації** використання підроблених карток в банкоматній мережі **за ч.3 ст.190 ККУ**. Для того, щоб глибоко розкрити цю проблему, розглянемо суб'єктивні сторони двох схожих складів злочинів, які лише на перший погляд відрізняються між собою тільки факультативною обставиною – місцем вчинення:

1) *Використання підроблених карток в банкоматній мережі для протиправного заволодіння готівковими коштами.*

Умисел зловмисника спрямований в даному випадку на таємне заволодіння **чужими** грошовими коштами (для нього нецікаво кому саме юридично належить право власності на них), що були поміщені банком-еквайєром у конкретний банкомат, з якого відбувається їх протиправне вилучення. Спробуємо схематично зобразити хронологію злочину та послідовність подальших розрахунків між основними **суб'єктами** цих правовідносин для визначення того, хто понесе реальний збиток на момент події злочину:



1 – момент шахрайської операції: зловмисник вставляє підроблену картку у кардрідер банкомату, та вилучає з нього чужі грошові кошти, фактично поміщені у банкомат банком-еквайєром,що обслуговує цю банкоматну мережу. В момент здійснення операції з видачі готівки банкоматом сума коштів, якими володіє банк-еквайер зменшуться, і.кошти списуються з його рахунків,. В цей момент злочин вже є закінченим, і **реальний збиток** на момент злочину несе **банк-еквайер.**

2 - **банк – еквайер** відправляє інформацію про здійснені розрахунки у платіжну організацію відповідної платіжної системи (**ПС**);

3 – **ПС** проводить кліринг, на основі результатів якого зарахує кошти **банку-єквайеру** та списує їх з рахунків **банку-емітенту**, клієнтом якого є законний держатель підробленої картки.

4 – **банк – емітент** списує кошти з рахунку свого **клієнта – законного держателя картки**.

2) *Використання підроблених карток в торгівельній мережі для розрахунку ними за отримані товари чи послуги, надані підприємством торгівлі чи сервісу (ТСП).*

Умисел зловмисника спрямований на заволодіння конкретними товарами чи на отримання конкретних послуг, з тим, щоб розраховуватися за них не власним коштом, а за рахунок держателів підроблених карток шляхом введення в оману касира чи іншої матеріально-відповідальної особи, яка проводить розрахунок. Така особа має пересвідчитися в тому, що картка належить її законному держателю, зокрема шляхом співставлення підписів на самій картці та чеку, проте оскільки ці операції відбуваються з введенням ПІН-коду, що апріорі (без урахування нових технологій кардерів з отримання доступу і до цієї інформації) вважається відомим лише законному держателю, автентичність особи зазвичай не викликає сумніву і шахрай легко розраховується чужими грошима. Зобразимо хронологію злочину та послідовність подальших розрахунків між основними **суб'єктами** цих правовідносин аналогічно першій ситуації:

1 – момент шахрайської операції: здійснення зловмисником оплати товарів чи послуг у торгівельній мережі безготівковим шляхом, *формально* - за рахунок коштів законного держателя картки. *Фактично* – на момент операції кошти списуються з рахунків банку-еквайеру, що обслуговує термінальну мережу торгівельно-сервісного підприємства (**ТСП**), в якому відбулася транзакція, на рахунок цього ТСП. В цей момент злочин вже є закінченим, і **реальний збиток** на момент злочину понесе **банк-єквайер.**

2 - **банк – єквайер** відправляє інформацію про здійснені розрахунки у платіжну організацію відповідної платіжної системи (**ПС**);

3 – **ПС** проводить кліринг, на основі результатів якого зарахувує кошти **банку-єквайеру** та списує їх з рахунків **банку-емітенту**, клієнтом якого є законний держатель підробленої картки.

4 – **банк – емітент** списує кошти з рахунку свого **клієнта – законного держателя картки**.

Правовідносини, що підпадають в обох схемах під нумерацією 2-4, за своєю суттю аналогічні *цивільним* (ст. 1191 ЦКУ) та *господарським* (ст. 228 ГКУ) правовідносинам з регресного відшкодування збитків. Вони мають місце вже після події злочину, і до встановлення потерпілої особи, що реально понесла збитки на момент злочину, відношення не мають. Позов про відшкодування таких збитків може бути подано в порядку цивільного судочинства. Недоцільність перенесення моменту закінчення

злочину на стадію 4, як це відбувається при кваліфікації за відсутності єдиної позиції з цього питання, пояснюється ще двома аспектами. По перше, злочини проти власності є злочинами з матеріальним складом, які вважаються закінченими з моменту настання зазначених у законі суспільно небезпечних наслідків - тобто з того моменту, коли винна особа вилучила майно і мала реальну можливість розпоряджатися чи користуватися ним, а це відбулося на стадії 1. (див. Постанова Пленуму ВСУ №10 від 06.11.2009 «Про судову практику у справах про злочини проти власності»). По друге, навіть якщо спробувати вважати злочин закінченим на стадії 4, і за потерпілу особу приймати клієнта банку-емітенту, який зазвичай одразу ж повідомить про неправомірне списання свій банк і також вимагатиме в нього відшкодування (тобто банк-емітент буде договірним представником потерпілої особи), при порушенні кримінальної справи виникне питання підтвердження наявності реальних збитків з боку банку-емітенту. В тих випадках, коли банк-емітент знаходиться за межами території України і всі подібного роду збитки в нього застраховані, отримання такого підтвердження не видається можливим. Як наслідок, за відсутності повного складу злочину кримінальна справа не може бути порушена, хоча подія злочину безумовно мала місце.

Тепер проаналізуємо **наявність обов'язкових ознак шахрайства** у складі двох описаних вище злочинів. При випадку з ТСП, відбувається введення в оману касира чи іншої матеріально-відповідальної особи, яка проводить розрахунок за товару чи послуги з використанням підробленої картки в процесі якого використовується ЕОМ (тобто POS-термінал). У випадку з АТМ, введення в оману чи заволодіння довірою на момент злочину відбуватися не може, оскільки незрозуміло, як можна ввести в оману машину, яка позбавлена свідомості та інтелекту. Аргументом не на користь такого підходу може бути те, що здавалося б, після відправлення авторизаційного запиту на здійснення транзакції (тобто надання дозволу на видачу готівки з боку банку-емітенту), у ланцюжку з'являється елемент свідомості у вигляді живої людини, що приймає остаточне рішення з приводу видачі банкоматом готівки, проте це не зовсім так. З технічної точки зору робота фронтальної системи банку-емітенту налагоджена таким чином, що на іншому боці каналу зв'язку цю інформацію також обробляє машина, і в разі відсутності у переданому повідомленні певних кодів, що за законами моніторингу прямо вказують на потенційне шахрайство, повідомлення з дозволом на видачу готівки формується автоматично, і у зворотному напрямку по цим же каналам зв'язку передається на АТМ, з якого пішов запит. А оскільки більшість

шахраїв знають як «правильно» знімати кошти, щоб взагалі не потрапити в поле зору відділів моніторингу банків, то переважна більшість таких операцій відсікає участь живої особи на момент здійснення транзакції. Тобто заволодіння довірою чи введення в оману, які є обов'язковою ознакою шахрайства у складі злочину - відсутні.

Отже, у цьому випадку, ЕОМ (тобто банкомат) виступає лише способом отримання доступу до грошей, а не пристроєм, з використанням якого вводиться в оману фактичний розпорядник грошових коштів, як це відбувається при розрахунках у торгівельній мережі за підробними картками. Одразу постає питання, як же інакше тоді кваліфікувати ці дії. Тут слід звернутися до **п.17 Постанови Пленуму ВСУ №10 від 06.11.2009 «**Про судову практику у справах про злочини проти власності»: «Якщо обман або зловживання довірою були лише *способом отримання доступу* до майна, а саме вилучення майна відбувалося таємно чи відкрито, то склад шахрайства відсутній. Такі дії слід кваліфікувати відповідно як **крадіжку**, грабіж або розбій». Оскільки вилучення майна відбувається таємно і для законного держателя картки (безпосереднього власника), і для банку-еквайеру (титульного власника), і для банку-емітенту, і навіть для перехожих,- наявність усіх обов'язкових ознак крадіжки вказує на необхідність кваліфікації використання «білого пластику» в банкоматній мережі **за ст. 185** ККУ. До речі, саме так схему боротьби з підробними картками застосовують у близьких нам правових системах, зокрема в Росії.

Висновок. Якщо розглядати використання «білого пластику» в банкоматній мережі як крадіжку за ст.185 ККУ, знімається одразу ряд проблем:

- витримуються правила кваліфікації та закони юридичної логіки з урахуванням специфіки правовідносин у сфері обігу платіжних карток;
- вирішується проблема спрямованості умислу та необхідності підтвердження збитків, і як наслідок, проблема неможливості порушення кримінальних справ та недоведеності їх до кінця при встановленому факті наявності події злочину;
- при кваліфікації в сукупності зі ст. 200 ККУ охоплюється увесь склад злочину;
- у виняткових випадках ст. 185 ККУ дає змогу правоохоронним органам застосувати тримання під вартою як запобіжний захід.

Сценарій вирішення проблеми

Реалізація забезпечення однакового застосування норм права при вирішенні справ відповідної судової юрисдикції, запобігання

виникненню судових помилок відбувається шляхом узагальнення практики застосування судами норм матеріального і процесуального права. Історично в Україні таке узагальнення здійснював Пленум Верховного Суду України та формалізував його у вигляді постанов. Серед них і Постанова Пленуму ВСУ № 10 від 6 листопада 2009 року «Про судову практику у справах про злочини проти власності», яка теоретично (зокрема в частині п.17) може застосовуватися при кваліфікації судами використання «білого пластику» в банкоматній мережі, проте прямо не вказує на це. Програма мінімум - внести зміни в існуючу Постанову № 10 з роз'ясненнями з приводу застосування ст. 185 та ч.3 ст.190 та прописуванням конкретних випадків протиправних діянь з урахуванням специфіки правовідносин у сфері обігу платіжних карток на кожну з двох статей.

Питання, що можуть виникнути в ході реалізації**:** Відповідно до п.1 перехідних положень Закону України «Про судоустрій і статус суддів» від 07.07.2010, з 1 листопада 2010 року розпочинає свою діяльність Вищий спеціалізований суд України з розгляду цивільних і кримінальних справ. Згідно зі ст. 36 Закону, відтепер саме його Пленуму належать повноваження з узагальнення судової практики та прийняття роз'яснювальних постанов. Проте ні в перехідних положеннях, ні в самому Законі не прописано можливість внесення ним змін в розрізі аналогічних повноважень в акт іншого органу судової влади, який у вертикальній ієрархії посідає вище місце.

З глибокою повагою,
Директор Олександр Карпов