УДК 343.98
DOI https://doi.org/10.32837/pyuv.v0i1.741

І. О. Коваленко
orcid.org/0000-0001-9522-5971
адвокат,
аспірант кафедри криміналістики та домедичної підготовки
Дніпропетровського державного університету внутрішніх справ

ОБСТАВИНИ, ЩО ПІДЛЯГАЮТЬ ВСТАНОВЛЕННЮ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Постановка проблеми. Сфера здійснення безготівкових розрахунків є невід'ємною частиною економіки України. Розвиток і вдосконалення банківських електронних платежів відіграли важливу роль у банківській справі: дали змогу знизити операційні банківські витрати, розширити сегмент активних клієнтів, підвищити їхню лояльність. Але також гостро стоїть проблема інформаційної та фінансової безпеки клієнтів, що користуються дистанційними видами банківського обслуговування, зокрема під час роботи з банківськими електронними платежами. Перед більшістю країн, в яких активно розвиваються операції з використанням онлайн-банкінгу, виникають різні види загроз шахрайства, не є винятком і Україна.

Безсумнівно, користуватися безготівковим розрахунком за допомогою онлайн-банкінгу набагато зручніше, ніж готівкою. Не доводиться носити з собою грошові суми, а в тих випадках, якщо їх не вистачає під час розрахунку за покупку, знову ж на допомогу приходить банківська карта, на яку можливо отримати кредит миттєво за допомогою смартфона і додатку банку. Однак всі ці зручності та переваги злочинці використовують у своїх корисливих цілях і, отримавши верифікаційні дані злочинним шляхом, можуть здійснювати різні операції, розраховуючись за їх вчинення чужим майном, тобто грошовими коштами, які їм не належать.

Аналіз останніх досліджень і публікацій. Проблематикою розслідування шахрайства у сфері банківських електронних платежів займалися багато вчених та науковців, таких як С.С. Чернявський, В.І. Отряхина, К.В. Суркова, А І. Анапольська, С.В. Васюков, О.В. Журавльова, А.А. Сандрачук, А.Ф. Волобуєв, Н.В. Павлова, В.Ю. Голубовський, Є.П. Фірсов, С.М. Астапкина, В.М. Єгошин, В.В. Колесников, О.І. Луценко, О.С. Овчинський, Р.С. Сатуєв, Г.М. Спірін, В.О. Фінагеєв та інші.

Як влучно зазначає А.І. Анапольська, в сучасних умовах у банківській системі здійснюється безліч банківських афер, серед яких найбільш розповсюдженими є шахрайства, здійснювані у сфері функціонування банківських електронних платежів. Виявлення та розслідування таких злочинів є одним із пріоритетних завдань, що стоять перед правоохоронними органами. Важливе значення у вирішенні цього питання належить налагодженій взаємодії правоохоронних органів із банківськими установами [1].

С.В. Васюков наголошує, що перебудова платіжної системи гостро потребує зміни принципів організації безготівкових розрахунків, використання нових форм і способів здійснення платежів, а також вирішення питань, пов'язаних із забезпеченням кримінологічної безпеки учасників платіжних систем, які є сторонами здійснення електронних платежів, з використанням яких відбувається більшість грошових розрахунків. Як відомо, чітко організована система безготівкових розрахунків має велике економічне значення і низку переваг перед розрахунками з використанням готівки, водночас активна криміналізація зазначеної сфери в останні роки вимагає прийняття адекватних заходів реагування на криміногенну обстановку, а саме на шахрайство у сфері використання банківських електронних платежів [2]. Тому в цьому дослідженні ми детально проаналізуємо обставини, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів.

Мета дослідження. Метою статті є визначення і характеристика обставин, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів.

Виклад основного матеріалу. З настанням всесвітньої пандемії COVID-19 грошові відносини громадян усіх країн зазнали докорінних змін. Зважаючи на те, що уряди багатьох країн час від часу в непередбачуваний момент запроваджують карантинні обмеження, такі як заборона роботи розважальних закладів, навчальних закладів, закладів харчування, крамниць, людство фактично адаптувалося працювати онлайн, проводити навчальний процес у вигляді онлайн-конференцій; служби доставки їжі в один момент витіснили ресторанний бізнес, практично всі магазини вимушено змінили концепцію роботи, віддавши перевагу торгівлі через сайти і соціальні мережі. Ця

ситуація миттєво примусила і, як наслідок, мимоволі суттєво збільшила довіру суспільства до інтернет-банкінгу, сайтів онлайн-оплати послуг і товарів, збільшивши лояльність суспільства до сфери використання банківських електронних платежів, зробивши її частиною нормальних грошових відносин. Таким чином, пропорційно зростанню онлайн-транзакцій збільшується і шахрайство у сфері банківських електронних платежів.

Існують різні думки про зміст обставин, що підлягають встановленню. В.А. Образцов та інші вчені виходять із норми кримінального закону і положень кримінально-процесуального права щодо предмета доказування [3, с. 48]. Н.А. Селіванов використовує відому семичленну формулу, яку використовували ще за часів Римської імперії (що скоєно, де, коли, яким чином, ким, за допомогою кого або чого, чому), яка доповнюється і деталізується стосовно конкретних видів злочинів [4, с. 121].

Обставини, що підлягають доказуванню у кримінальному провадженні, визначені ст. 91 КПК України. Таким чином, у кримінальному провадженні підлягають доказуванню: подія кримінального правопорушення, а саме місце, час, спосіб та інші обставини вчинення шахрайства; винуватість обвинуваченого у вчиненні кримінального правопорушення, форма його вини, мотив і мета вчинення цього злочину; вид і розмір шкоди, завданої кримінальним правопорушенням, а також розмір процесуальних витрат; обставини, які впливають на ступінь тяжкості вчиненого шахрайства, характеризують особу обвинуваченого, обтяжують чи пом'якшують покарання, які виключають кримінальну відповідальність або є підставою закриття кримінального провадження; обставини, що є підставою для звільнення від кримінальної відповідальності або покарання [5]. Обставини, викладені у цій статті, являються узагальнюючими для всіх видів кримінальних проваджень, і в теорії доказів ці обставини називаються загальним предметом доказування на всіх етапах кримінального провадження. Уособлення предмета доказування у кожному окремому провадженні здійснюється, зважаючи на вимоги диспозиції статті КК України, за якою кваліфікується це правопорушення, що підлягає встановленню.

Розслідування шахрайств, вчинених із використанням електронних платежів, залишається досить складним завданням для більшості співробітників органів слідства, що зумовлено специфікою цього роду правопорушень. На практиці складнощі виникають через відсутність теоретичних методик і досвіду розслідування таких справ у співробітників правоохоронних органів. Ситуація ускладнюється також тим, що багато дрібних випадків просто не доходять до правоохоронних органів.

Злочини, скоєні у сфері використання банківських електронних платежів, характеризуються низкою специфічних ознак, таких як:

1) використання сучасних технологій для видобутку і розповсюдження платіжної інформації та персональних даних потерпілих;

2) високий професіоналізм злочинців, деякі з яких, можливо, мають спеціальну технічну освіту;

3) велика географія шахрайства та його наслідків (наприклад, заподіяння шкоди можливе банку або фізичній особі – власнику розрахункового рахунку, який знаходиться на території іншого регіону і навіть держави);

4) безперервний процес винаходу нових способів кримінальних дій із проведенням банківських електронних платежів;

5) високий ступінь організованості учасників злочинної діяльності, що істотно розширює предмет доказування у кримінальній справі й інші ознаки;

6) труднощі з узагальненням матеріалів слідчої та судової практики щодо цього виду злочину.

Під час розслідування шахрайства у сфері використання банківських електронних платежів можна виділити такі обставини, що підлягають встановленню: існування взаємозв'язку між способом вчинення цього виду правопорушення та механізмом викрадення коштів; місце вчинення злочину; ким вчинено шахрайство: одноосібно або групою осіб.

Виділяються такі обставини вчинення шахрайства з використанням електронних способів оплати:

– використання розрахункових рахунків, що належать одному із співучасників розкрадання грошових коштів;

– використання фіктивних розрахункових рахунків, що належать випадковим учасникам злочинного процесу;

– використання сервісів обміну грошових коштів;

– використання фіктивної юридичної особи, яка уклала договір з банком про обслуговування розрахунків з використанням електронних засобів платежу;

– переведення в готівку грошових коштів, що містяться на рахунку потерпілого, дані авторизації якого виявилися в руках зловмисників;

– оплата товарів через інтернет з використанням персональних даних потерпілого.

Слідчий задля неупередженого, швидкого і повного розслідування кримінального провадження повинен встановити такі моменти [6, с. 27]:

1) матеріальні та електронні сліди злочину. До матеріальних слідів відносяться: сліди рук, ніг, інструментів злому як відображення зовнішнього фізичного впливу на кібернетичні системи, пристрої

та мережеве обладнання; сліди тонерів, барвників, різних витратних матеріалів, що використовуються в електронних пристроях; диски, пристрої зберігання інформації, пристрої для віддаленого зняття даних та інформації, будь-якого вигляду документи та роздруківки, так звані сліди-предмети [7, с. 112]. До електронних слідів злочину у сфері банківських електронних платежів належать: носій інформації, окремий або інтегрований у цифрову систему, що являє собою місцезнаходження; цифровий код, що має вигляд звукового, текстового або графічного запису; обов'язкове звертання уваги на дотримання технології під час виявлення, фіксації та вилучення слідів, а також залучення фахівців, що володіють технічними, науковими та іншими специфічними навичками, використання новітніх програм та пристроїв [8]. Під час визначення електронних носіїв інформації ми спираємося на дослідження М.В. Феоктистова. До зазначених об'єктів він відносить різні носії, зокрема карти пам'яті, флеш-накопичувачі, електронні ключі тощо. Ідентифікація користувача як клієнта банку, тобто уповноваженої особи на вчинення будь-яких фінансових операцій або інших юридично значущих дій, відбувається при фізичному під'єднанні цих пристроїв до комп'ютера [9];

2) місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні);

3) способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів);

4) засоби, залучені до скоєння правопорушення (технічні, такі як електронно-обчислювальна техніка, смартфони, планшети, модеми, маршрутизатори, і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації);

5) способи проникнення крізь інформаційний захист (генерація ключів і паролів, викрадення паролів, заборона доступу до облікового запису тощо).

Насамкінець слід зазначити, що ключове значення мають також обставини, що сприяли вчиненню діяння. Незважаючи на те, що ст. 24 ЗУ «Про захист персональних даних» передбачено, що суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від незаконної обробки, а також від незаконного доступу до них [10], у мережі Інтернет існують різноманітні сайти-форуми, торговельні онлайн-майданчики, де зловмисники успішно продають величезні обсяги персональних даних, здобуті злочинним шляхом, імена, адреси реєстрації, контактні дані осіб, що можуть бути використані для верифікації фіктивного клієнта банку, а також дані доступу до банківської інформації, кредитних та дебетових карток, дані доступу до онлайн-банкінгу, надають послуги створення підробних фото-ID тощо.

Висновки. Таким чином, у статті визначено низку обставин, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів. Такими обставинами є матеріальні та електронні сліди злочину, місця отримання доступу до комп'ютерних систем, способи підключення до них, засоби, що були застосовані під час вчинення шахрайства, способи автентифікації в мережу онлайн-банкінгу та обставини, що сприяли вчиненню шахрайства цього виду.

Література:

1. Анапольская А.И. Порядок взаимодействия правоохранительных органов с банковскими учреждениями при расследовании мошенничеств в сфере функционирования электронных расчетов. *Вестник Тамбовского университета. Серия: Гуманитарные науки.* 2015. Вип. 5 (145). С. 221–224.

2. Васюков С.В. Предупреждение преступлений, совершаемых в сфере проведения безналичных расчетов. Автореферат диссертации на соискание ученой степени канд. юр. наук. М. 2013. 233 с.

3. Образцов В.А. Криминалистическая характеристика преступлений: дискуссионные вопросы и пути их . Сб. науч. тр. М. ВНИИ прокуратуры, 1984. С. 7–15.

4. Селиванов Н.А. Советская криминалистика: система понятий. М. Юрид. лит. 1982. 152 с.

5. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. Офіційний сайт ВР України. URL: http://zakon4.rada.gov.ua/laws/show/4651-17 (дата звернення 20.04.2021).

6. Рекомендації щодо особливостей досудового розслідування та процесуального керівництва у кримінальних провадженнях про злочини, вчинені з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (2017) URL: https://www.gp.gov.ua/userfiles/metodichka_Kiber_11_07_17.doc (дата звернення 20.04.2021)

7. Салтевський М.В. Криміналістика. Підручник: У 2-х ч. Ч.1. Х.: КонСУМ, Основа, 1999. 416 с.

8. Авдєєва Г.К., Стороженко С. Електронні сліди : поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2017. Вип. 1(77). С. 169–176. URL: https://journal.lduvs.lg.ua/index.php/journal/article/view/341 (дата звернення 20.04.2021)

9. Феоктистов М.В. Неправомерный оборот средств платежей (ст. 187 УК РФ). *Законность.* 2016. Вип. 1 (975). С. 45–48

10. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 34. URL: http://zakon5.rada.gov.ua/laws/show/2297-17 (дата звернення 20.04.2021)

Анотація

Коваленко І. О. **Обставини, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів.** – Стаття.

У статті визначено перелік обставин, що підлягають встановленню під час розслідування шахрайства у сфері банківських електронних платежів, та наведено їх характеристику. 2020 рік став точкою неповернення для всього людства, реальне життя буквально в один момент перетворилося на віртуальне,

що потягнуло за собою перехід усіх сфер спілкування, співробітництва, торгівлі у світ інформаційних технологій та комп'ютерних систем. Відтепер грошові кошти виглядають як програмний код і все більше віддаляються від свого попереднього фізичного вигляду у формі купюр. Передбачувано, що кібер-шахраї одразу скористаються такою ситуацією і в найбільш різноманітні способи намагатимуться заволодіти коштами як звичайних громадян – фізичних осіб, так і юридичних осіб, їх персональними даними. Це правопорушення зазвичай кваліфікується за ч. 3 ст. 190 Кримінального кодексу України. Аналіз останніх досліджень видатних науковців показує, що виявлення та розслідування злочинів у сфері банківських електронних платежів має стати одним із пріоритетних завдань для правоохоронних органів усіх країн. Особливу увагу стосовно цього питання слід приділити налагодженій взаємодії правоохоронних органів з банківськими установами. Було досліджено різні погляди про зміст обставин, що підлягають встановленню у розрізі специфіки кібер-шахрайства. У статті наведено характеристику таким обставинам, що підлягають встановленню, як матеріальні та електронні сліди злочину, наведено їх детальні приклади, місця отримання доступу до комп'ютерних систем, перераховано способи підключення до них, зазначено засоби, що були використані під час здійснення шахрайства, способи авторизації та верифікації шахраїв у мережу онлайн-банкінгу та обставини, що сприяли вчиненню шахрайства у сфері банківських електронних платежів.

Ключові слова: шахрайство, онлайн-банкінг, автентифікація, персональні дані, кардінг.

Summary

Kovalenko I. O. **Circumstances to be established during the investigation of fraud in the use of electronic bank payments.** – Article.

This article identifies a list of circumstances to be established during the investigation of fraud in the field of electronic bank payments, and provides a description of them. 2020 became a turning point for all mankind, real life literally at one point became virtual, which led to the transition of all spheres of communication, cooperation, trade in the world of information technology and computer systems. From now on, money looks like program code and is increasingly moving away from its previous physical form of banknotes. It is assumed that cyber-fraudsters will immediately take advantage of this situation, and in a variety of ways will try to seize the funds of both ordinary citizens – individuals and legal entities, their personal data. This offense, as a rule, in most cases qualifies under Part 3 of Art. 190 of the Criminal code of Ukraine. An analysis of recent research by prominent scholars shows that the detection and investigation of crimes in the field of electronic bank payments should be one of the priorities for law enforcement agencies in all countries. Particular attention should be paid to the well-established interaction of law enforcement agencies with banking institutions. Different views were explored on the content of the circumstances to be established in terms of the specifics of cyber fraud. The article describes the circumstances to be established – material and electronic traces of the crime, provides detailed examples, places of access to computer systems, lists the methods of connection to them, indicates the means used in fraud, methods of authorization and verification of fraudsters in the online banking network, and the circumstances that contributed to the commission of fraud in the field of electronic bank payments.

Key words: fraud, online banking, authentication, personal data, carding.