**Правила формування показників,**

**що подаються у файлі F5X “Дані про збитки через незаконні дії/шахрайські операції з використанням електронних платіжних засобів”**

Файл подають банки, що надають послуги з емісії платіжних інструментів та/або здійснення еквайрингу платіжних інструментів, небанківські надавачі платіжних послуг, авторизовані для надання послуги з емісії платіжних інструментів та/або здійснення еквайрингу платіжних інструментів (далі – постачальники звітності).

У файлі подається інформація щодо кількості випадків та суми збитків через незаконні дії/шахрайські операції з використанням електронних платіжних засобів (платіжні картки та їх реквізити, токенізовані картки).

**Незаконна дія/шахрайська операція з використанням електронних платіжних засобів** (далі – шахрайська операція) – це операція з використанням електронного платіжного засобу, що ініційована:

- третіми особами без згоди клієнта

- клієнтом самостійно за для оплати певної послуги/продукту та нездійснення шахраями обіцяного або на сайтах, що були створені шахраями

- клієнтом під психологічним впливом/тиском шахраїв,

в результаті чого було зазнано збитків однією із сторін: держателем електронного платіжного засобу, банком, оператором поштового зв’язку, небанківською фінансовою установою, торговцем.

До файла не включаються:

сумнівні операції, по яким не було підтверджено факту шахрайства (в тому числі коли клієнт прийняв рішення відмовитись від подальшого розслідування з певних причин);

спірні операції, які не відносяться до шахрайських операцій з використанням електронних платіжних засобів (в тому числі не включаються операції, проведені клієнтом через банкомат, ПТКС, торговельний термінал тощо, в результаті яких відбувся технічний збій, кошти були повернуті автоматично на картковий рахунок клієнта або повернені постачальником звітності за рахунок виявлених надлишків у пристроях);

операції по яким триває розслідування і не було прийнято кінцеве рішення щодо того, хто зазнає збитків (клієнт, торговець чи постачальник звітності).

Постачальник звітності розглядає всі звернення клієнта подані будь-яким каналом, фіксує всі випадки шахрайства з використанням електронного платіжного засобу, за результатом проведеного розслідуванням приймає рішення хто має зазнати збитків (клієнт, торговець чи постачальник звітності) та в подальшому відображає інформацію про збитки від шахрайських операцій у звітності за відповідний звітний період, коли розслідування було фактично завершено.

Сума шахрайської операції, здійсненої в іноземній валюті з використанням електронних платіжних засобів, емітованих до рахунків, відкритих в іноземній валюті, надається у перерахунку за офіційним курсом гривні до іноземних валют, установленим Національним банком України на дату відображення операцій за рахунком.

Для шахрайських операцій, здійснених в іноземній валюті з використанням електронних платіжних засобів, емітованих до рахунків відкритих в національній валюті, зазначається фактична сума операції, відображена за рахунком.

Інформація щодо кількості випадків та сум збитків через незаконні дії/шахрайські операції з використанням електронних платіжних засобів, подається постачальниками звітності відповідно до наступних правил:

1. якщо збитків зазнає постачальник звітності – тоді збитки у звітному файлі повинен подавати той постачальник звітності, який фактично їх зазнав як еквайр або як емітент електронного платіжного засобу, з використанням якого було проведено шахрайську операцію. Відповідно постачальник звітності, якому стало відомо про факт здійснення шахрайської операції, але він не відшкодовував клієнту втрати (це зробив інший постачальник звітності) – дані шахрайські операції не подає до файлу.

*Приклад:* клієнт звернувся до банку-емітента картки та повідомив про шахрайство в мережі Інтернет з його платіжною карткою. Банк-емітент у ході розслідування з’ясував, що еквайром сайту, де проводилась шахрайська операція є інший банк (банк-еквайр). Банк-емітент здійснив запит (в тому числі з використанням порядку подання диспутів платіжних систем) до банку-еквайра, який надав інформацію, що зі сторони банка-еквайра операція була правомірною. Банк-емітент вирішує повернути кошти клієнту – відповідно банк-емітент має відобразити дану шахрайську операцію як власні збитки у файлі, а банк-еквайр дану операцію не зазначає при подачі звітного файла;

1. якщо відбулась шахрайська операція з використанням електронного платіжного засобу, клієнт звернувся до постачальника звітності та було прийнято рішення про невідшкодування збитків клієнту – дану шахрайську операцію потрібно відобразити як збитки клієнта тому постачальнику звітності, який є емітентом електронного платіжного засобу. Еквайр не повинен відображати дану операцію при подачі звітного файла;
2. якщо збитки клієнта по шахрайській операції з використанням електронного платіжного засобу відшкодував торговець, де була здійснена така операція (магазин, сайт і т.д.), тоді збитки відображаються у файлі як збитки торговців та подаються тим постачальником звітності, який здійснює обслуговування даного торговця відповідно до договору. Банк-емітент в такому разі не відображає дану операцію при подачі звітного файла;
3. у випадку відображення шахрайських операцій з використанням електронного платіжного засобу, емітованого банками-нерезидентами, що були проведені на території України – збитки клієнта подає той постачальник звітності, який виступив еквайром по операції та зазнав збитків за відшкодування коштів клієнту. У разі, якщо еквайр чи торговець не відшкодовував клієнту збитки, то дана операція не подається у звітному файлі.

**Особливості формування показника**

**AF5001 “Кількість випадків та сума збитків через незаконні дії/шахрайські операції з використанням електронного платіжного засобу”.**

**Опис параметрів.**

За показником відображається кількість випадків та сума збитків через незаконні дії/шахрайські операції, що були здійснені з використанням електронних платіжних засобів (платіжні картки та їх реквізити, токенізовані картки).

**Параметр D060** – код платіжної системи, у якій була здійснена шахрайська операція з використанням електронного платіжного засобу (довідник D060).

**Параметр Z350** – код емітента електронного платіжного засобу (довідник Z350).

**Параметр Z241** – код власника мережі, де була здійснена шахрайська операція з використанням електронного платіжного засобу (довідник Z241).

**Параметр K045 –** код території здійснення операції (довідник К045).

**Параметр Z130 –** код типу незаконної дії/шахрайської операції з використанням електронного платіжного засобу (довідник Z130).

Дані надаються у розрізі:

за підробленими електронними платіжними засобами (Z130=01) – шахрайські операції проведені з використанням підроблених електронних платіжних засобів (в т.ч. “білий пластик”);

за втраченими/викраденими електронними платіжними засобами (Z130=02) – шахрайські операції, що були проведені з використанням втрачених або викрадених електронних платіжних засобів;

за скомпрометованим електронним платіжним засобом (без пред'явлення) (Z130=03) – шахрайські операції проведені шахраями без пред’явлення електронного платіжного засобу із зазначенням реквізитів, що стали відомі шахраям внаслідок:

- введення реквізитів електронного платіжного засобу клієнтом на підробленому/незахищеному сайті;

- після переходу за фішинговими повідомленнями;

- компрометації касиром даних платіжної картки під час розрахунку клієнтом у торговельно-сервісній мережі та подальше використання їх для проведення операцій в мережі Інтернет або операції з введенням реквізитів картки вручну на терміналі без застосування картки;

- заволодіння шахраями доступу до баз даних з реквізитами електронних платіжних засобів клієнтів, паролів/кодів доступу до Інтернет-банкінгу тощо;

соціальна інженерія (Z130=06), до даного типу відносяться:

- шахрайські операції, які були здійсненні після контакту з шахраями (дзвінок, смс-повідомлення, e-mail тощо), в ході комунікації шахраї використовуючи психологічні маніпуляції, залякування, погрози, неправдиві історії спонукали клієнта провести операції та/або надати дані електронного платіжного засобу, одноразові паролі тощо, що призвело до проведення шахрайських операцій із використанням електронного платіжного засобу клієнта та/або створення шахраями токенізованої картки з подальшим проведенням операцій;

- операції з використанням електронних платіжних засобів або реквізитів, що проведені клієнтом самостійно за для оплати певної послуги/продукту або операції переказу коштів на користь осіб, які виявились шахраями і не надали обіцяну клієнту послугу/товар;

- шахрайські операції проведені родичами/близькими особами клієнта внаслідок тимчасового заволодіння електронним платіжним засобом, телефоном, інтернет-банкінгом клієнта або даними, що дозволили провести шахрайську операцію без відома клієнта. Випадки, коли клієнт в процесі розслідування з’ясував обставини здійснення таких операцій і відмовився від подальшого розслідування/повернення коштів, не включаються до файлу.

інші (Z130=09) – шахрайські операції з використанням електронних платіжних засобів (в тому числі за реквізитами картки та за токенізованими картками) проведені з використанням інших схем незаконних дій, в тому числі здійснення шахрайських операцій клієнтом з використанням власних електронних платіжних засобів, внаслідок чого постачальником звітності були понесені збитки.

**Параметр Z140 –** код суб`єкта, який зазнав збитків (довідник Z140).

Дані надаються у розрізі:

банки (Z140=1) – збитки від шахрайських операцій з використанням електронних платіжних засобів, яких зазнав банк в результаті прийнятого рішення щодо повернення коштів клієнтам;

держателі електронного платіжного засобу (Z140=2) – збитки клієнта від шахрайських операцій, про які стало відомо постачальнику звітності після звернення клієнта будь-яким чином (заява, телефонний режим, скарга і т.д.) та було прийнято рішення постачальником звітності не відшкодовувати збитки клієнту;

торговці (Z140=3) – збитки від шахрайських операцій з використанням електронних платіжних засобів, яких зазнав торговець в результаті прийнятого рішення щодо повернення коштів клієнту;

оператори поштового зв’язку (Z140=4) – збитки від шахрайських операцій з використанням електронних платіжних засобів, яких зазнав оператор поштового зв’язку в результаті прийнятого рішення щодо повернення коштів клієнту;

небанківські фінансові установи (Z140=5) – збитки від шахрайських операцій з використанням електронних платіжних засобів, яких зазнала небанківська фінансова установа в результаті прийнятого рішення щодо повернення коштів клієнту.

**Параметр Z270** – код виду пристрою, де була здійснена шахрайська операція (довідник Z270).

**Метрика T070 –** сума збитків від незаконних дій/шахрайських операцій з використанням електронних платіжних засобів.

**Метрика T080 –** кількість незаконних дій/шахрайських операцій з використанням електронних платіжних засобів.