KPMG

Глобальне дослідження з питань шахрайства у банківській сфері

Багатостороння загроза шахрайства: чи готові банки гідно протистояти виклику?

2019

kpmg.ua

Зміст

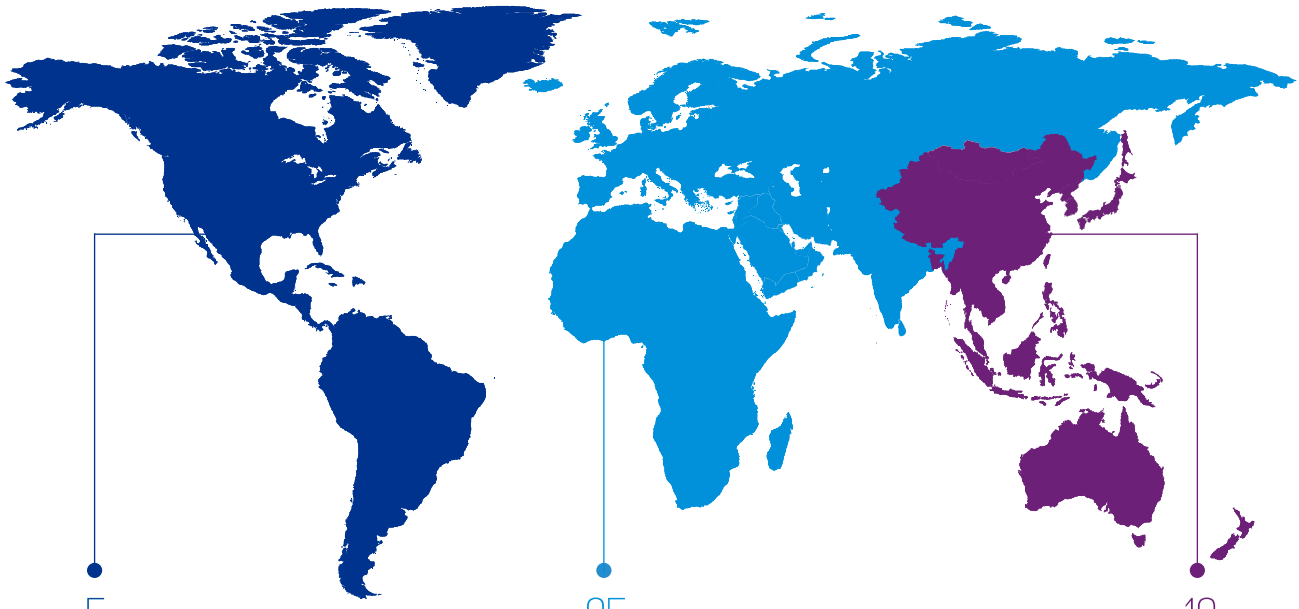
Передмова

KPMG має честь представити результати нашого першого глобального дослідження з питань шахрайства у банківській сфері (далі – «дослідження»). Дослідження було проведене з метою отримати глобальну картину того, яким чином банки протидіють внутрішнім та зовнішнім загрозам шахрайства.

Дослідження торкається питань ризиків шахрайства у банківській сфері, містить розслідування та опитування професіоналів з питань безпеки щодо трендів у типологіях шахрайства, викликів, з якими стикалися банки при мінімізації внутрішніх та зовнішніх загроз у період 2016—2018 рр., безпеки у цифрову еру, а також способів, у які банки структурують свої робочі групи та розподіляють ресурси задля оптимізації своїх зусиль у сфері управління ризиками.

Глобальне дослідження KPMG у банківській сфері було проведене у період листопад 2018 року — лютий 2019 року у 43 роздрібних банках, 13 з яких розташовані у країнах Азіатсько-Тихоокеанського регіону, 5 — в Америці і 25 — у Європі, на Середньому Сході та в Африці (EMA). 18 з цих банків мали дохід понад 10 млрд дол. США, а 31 банк мав понад 10 000 співробітників у різних країнах світу.

Висловлюємо подяку респондентам, що погодилися взяти участь у дослідженні. Представляємо результати, а також наші власні глобальні та регіональні інсайти, якими поділилися фахівці фірми-учасника KPMG.



За даними нашого дослідження, збитки від шахрайства збільшуються швидшими темпами, аніж витрати на управління ризиками. Необхідно терміново провести новий аналіз трендів

Девід Хікс

Провідний партнер глобальної практики Форензік KPMG International

Ключові спостереження

Понад половина респондентів повідомили про збільшення як кількості випадків зовнішнього шахрайства, так і розмірів спричинених ними збитків. У період 2015—2018 рр. розширилася типологія шахрайських дій, які наразі включають крадіжку персональних даних та встановлення контролю за рахунками жертв, кібератаки, шахрайство з безкартковими операціями та схеми з авторизацією пуш-платежів. У цьому звіті ми називаємо такі платежі, авторизовані клієнтами, протиправними схемами.

— Переважна більшість респондентів з усіх країн заявила, що загальна та середня величина втрат і кількість виявлених випадків внутрішнього шахрайства з боку працівників залишилися незмінними або зменшилися. Однак ця інформація може не відображати реальної картини витрат унаслідок внутрішнього шахрайства. Велика кількість зовнішніх шахрайських дій ініціюються певними особами, що працюють у банку.

— Понад половина респондентів відшкодовують менше 25% збитків від шахрайства, що свідчить про те, що ключем до вирішення проблеми є запобігання шахрайству. Банки інвестують у нові технології запобігання шахрайству, включно з машинним навчанням, повідомленнями про шахрайство в режимі реального часу, розпізнаванням голосу, обличчя та відбитків пальців (біометричні дані) та формуванням профілів взаємодії клієнтів з їхніми пристроями та засобами інтернет-банкінгу (поведінкові біометричні дані).

— Банки-респонденти з усіх регіонів заявили, що найбільшим викликом вважають кібератаки. Шахраї отримують дані клієнтів із застосуванням хакерських технологій, засобів соціального інжинірингу, у Dark Web та кримінальних мережах після порушень безпеки даних, що перебувають поза межами контролю банків.

— Однак, клієнти вважають, що відповідальність за запобігання шахрайським атакам їхніх рахунків із застосуванням соціального інжинірингу несуть банки. Приклади методів соціального інжинірингу наведені у Додатку 1.

— За результатами дослідження було встановлено, що банки помічають тенденцію до поширення застосування протиправних схем в усьому світі. Приклади протиправних схем наведені у Додатку 2. Шахраї маніпулюють і примушують клієнтів здійснювати платежі на їхню користь, оминаючи банківські засоби контролю. Велика Британія ухвалила Кодекс про модель потенційного відшкодування збитків від протиправних схем у формі авторизованого пуш-платежу для забезпечення відшкодування коштів клієнтам у певних випадках та забезпечення розробки регуляторами та урядами надійного рішення для жертв протиправних схем.

— Клієнти — ключ до запобігання та виявлення шахрайських дій на їхніх рахунках і зокрема до зменшення збитків від протиправних схем.

— Необхідно докласти додаткових зусиль у сфері навчання клієнтів з питань запобігання шахрайству та протиправним схемам.

— З огляду на те, що банки в усьому світі готуються відкрити двері третім сторонам, зокрема надати їм доступ до даних своїх клієнтів, відкритий банкінг (open banking) кваліфікується банками як серйозний, пов'язаний з шахрайством, виклик.

— Постає питання щодо ступеня надійності засобів контролю третіх сторін. Разом з тим відкритий банкінг надає додаткову можливість отримати більше даних про клієнта, що можуть використовуватися для запобігання та виявлення шахрайства та відшкодування збитків, завданих шахрайськими атаками.

< 25% Понад половина респондентів відшкодовують менше чверті збитків від шахрайських дій

> 50% Понад половина респондентів з різних країн повідомили про збільшення суми збитків від шахрайства

> 60% Понад 60% респондентів з різних країн повідомили про збільшення випадків шахрайства

Типології

- Безкарткові операції («CNP»)
- Соціальний інжиніринг
- Протиправні схеми
- Кібер-/онлайн шахрайство

Безпека у цифровому світі

- Зростання кількості товарів, що доставляються через цифрові канали
- Правила, машинне навчання, штучний інтелект та робототехніка
- Великий обсяг фальшивих підтверджень

Інвестиції/витрати

- Комплексні операційні моделі
- Неефективні процеси
- Навчання клієнтів
- «Тут і тепер» на противагу прогнозуванню нових трендів

Модель управління ризиком шахрайства

- Відсутність моделі управління ризиками шахрайства та процедури єдиної процедури оцінки ризику шахрайства
- Невиявлення шахрайства впливає на управлінську інформацію та інвестиційні рішення
- Оптимізація технології в розрізі кількості персоналу
- Фінансові злочини у відокремлених підрозділах

Тематика дослідження

Тренди еволюції шахрайства

Зовнішнє шахрайство

За даними дослідження, у 2018 році 61% респондентів повідомили про зростання загальної кількості випадків зовнішнього шахрайства, а 59% заявили про збільшення сум шахрайських операцій.

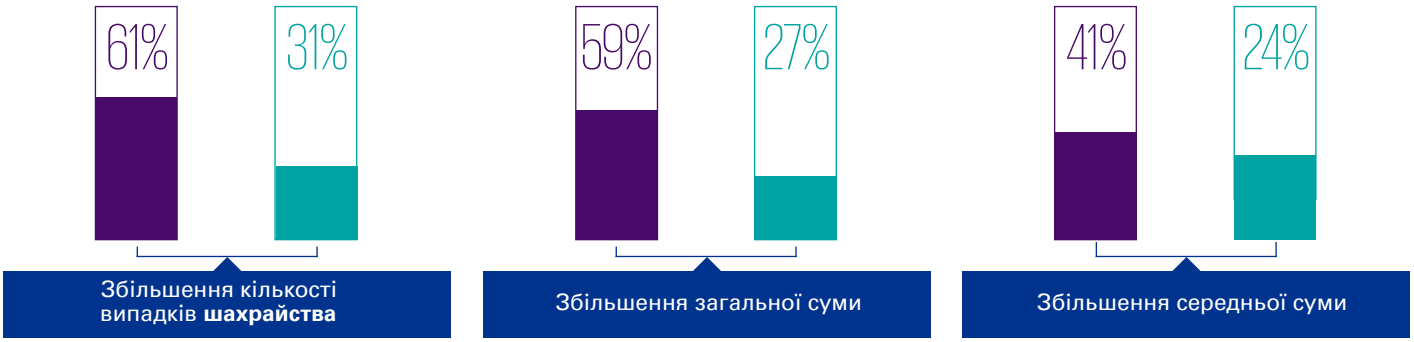
У більшості випадків респонденти вважали, що середня сума кожної шахрайської операції не змінилася (21%) або зменшилася (38%). Це можна пояснити великою кількістю шахрайських операцій з картками, сума яких була незначною. Нова типологія шахрайських операцій, що виникли у 2015—2018 рр., включає крадіжку персональних даних та використання номера картки для шахрайства/шахрайство від імені принципала, кібератаки, шахрайство з безкартковими операціями та протиправні схеми.

Внутрішнє шахрайство (з боку працівників)

Водночас найбільша частка респондентів заявила, що загальна вартість, середня вартість та кількість випадків внутрішнього шахрайства у 2017 і 2018 роках лишилися незмінними або скоротилися. Однак ця інформація може не відображати повну картину впливу внутрішнього шахрайства на фінансову установу, оскільки, як показує наш досвід, велика кількість зовнішніх атак є результатом співпраці досвідчених злочинців з внутрішніми джерелами, які детально знають банківські системи, процеси та засоби контролю (а також недоліки та слабкі місця систем контролю).

Потенційна шкода від шахрайства з боку інсайдерів може бути не меншою, якщо не більшою, за шкоду від зовнішнього шахрайства, враховуючи спроможність працівників використовувати слабкі місця засобів контролю з метою привласнення найбільші цінних активів банку. Банкам краще й надалі діяти на випередження з метою виявлення шахрайства з боку інсайдерів.

Ці статистичні дані ґрунтуються на виявлених випадках шахрайства. Як показує наш досвід, методи виявлення шахрайства стають дедалі досконалішими, однак певні елементи шахрайства поки що не піддаються контролю; до того ж, їх узагалі може бути важко виявити.



Відшкодування збитків від шахрайства

Понад половина респондентів повідомила, що частка відшкодованих збитків від шахрайства склала менше 25% від усіх збитків. Цей низький показник демонструє, яке значення мають прогнозування і запобігання шахрайству.

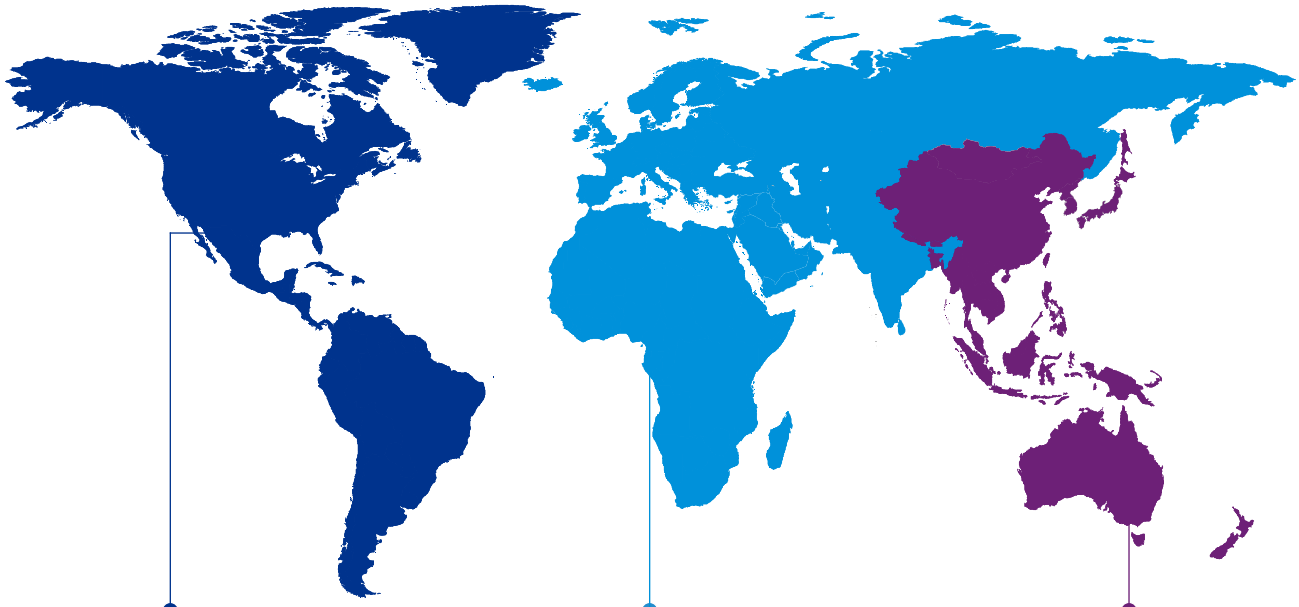
Тренди типології шахрайства за регіонами у 2017-2018 рр., згідно з найпоширенішими відповідями учасників

Типологія шахрайства	Америка	ЕМА	Азіатсько-Тихоокеанський регіон
Протиправні схеми	△ **Збільшення**	△ **Збільшення**	△ **Збільшення**
Безкарткові операції	△ **Збільшення**	△ **Збільшення**	△ **Збільшення**
Кібернетичне/онлайн шахрайство	△ **Збільшення**	△ **Збільшення**	△ **Збільшення**
Крадіжка ПД/шахрайство від імені принципала	△ **Збільшення**	△ **Збільшення**	△ **Збільшення**
Внутрішнє шахрайство	△ **Збільшення**	△ **Збільшення**	● **Без змін**
Крадіжка даних	△ **Збільшення**	● **Без змін**	△ **Збільшення**
Шахрайство з іпотечною заявою	● **Без змін**	△ **Збільшення**	△ **Збільшення**
Шахрайство у торгових точках	● **Без змін**	● **Без змін**	● **Без змін**
Підробка фінансової звітності	● **Без змін**	● **Без змін**	● **Без змін**
Шахрайство в трейдингу	● **Без змін**	● **Без змін**	● **Без змін**

Джерело: Глобальне дослідження з питань шахрайства у банківській сфері, KPMG International 2019

Виклики, що постають перед банками сьогодні

Дослідження мало на меті знайти відповідь на запитання, якими є найбільші виклики, що постають перед фінансовими установами у зв'язку з ризиками шахрайства. Наведена нижче діаграма відображає 5 найпопулярніших варіантів відповіді з 7 можливих варіантів у розрізі регіонів.



Америка

1. Кібернетичні атаки та порушення безпеки даних
2. Підвищення швидкості платежів
3. Відкритий банкінг (рівно третина)
4. Нові цифрові канали (рівно третина)
5. Віртуальні валюти (рівно третина)

EMA

1. Кібернетичні атаки та порушення безпеки даних
2. Підвищення швидкості платежів
3. Нові цифрові канали
4. Директива ЄС про платіжні послуги на внутрішньому ринку 2 (PSD2)/ відкритий банкінг
5. Соціальний інжиніринг

Азіатсько-Тихоокеанський регіон

1. Кібернетичні атаки та порушення безпеки даних
2. Соціальний інжиніринг
3. Підвищення швидкості платежів
4. Нові цифрові канали
5. Відкритий банкінг

Більш детальний аналіз цих викликів поданий у наступних розділах.

1. Кібернетичні атаки та порушення безпеки даних

2.Соціальний інжиніринг

3. Нові цифрові канали і підвищення швидкості платежів

4. Відкритий банкінг

Джерело: Глобальне дослідження з питань шахрайства у банківській сфері, KPMG International 2019

Ризик кібершахрайства є найбільшим викликом для фінансових установ у всіх трьох регіонах.

Фактично 5 найбільших ризиків шахрайства в усіх трьох регіонах пов'язують із цифровими трансформаціями, що відбуваються в світі. Щоб мінімізувати в майбутньому ризики шахрайства, фінансові установи мають комплексно змінити свій підхід до них. За великим рахунком, фінансовим установам необхідно зрозуміти цифрову трансформацію, що швидко відбувається навколо нас, оцінити нові ризики шахрайства, що з'являються внаслідок цих швидких змін, і розробити принципи управління ризиками шахрайства, що будуть спроможні ефективно і результативно мінімізувати ці ризики, забезпечуючи стабільні результати. Гадаю, що ані наявні «сейфи», ані інші дорогі в обслуговуванні рішення, що наразі використовуються фінансовими установами, враховуючи їхню значну фрагментарність і недосконалість, не можуть ефективно захистити від ризиків шахрайства, що постійно трансформуються. Системи управління ризиками шахрайства нового покоління повинні бути спроможні працювати в умовах постійної цифрової трансформації, виявляти нові, досі невідомі ризики шахрайських дій, використовувати переваги технологій та зменшувати витрати на забезпечення дотримання законодавства

Лем Чін Кок

Провідний партнер практики форензік, країни Азіатсько-Тихоокеанського регіону, KPMG у Сінгапурі

1. Кібернетичні атаки та порушення безпеки даних

Найбільшим викликом респонденти з різних країн визнали кібератаки та випадки витоку даних. За останні кілька років вони дізналися з преси про численні порушення безпеки важливих даних, приклади яких наведені на малюнку, поданому нижче.

У взаємопов'язаному світі, коли порушення безпеки даних може стосуватися певної компанії з однієї країни, дані, що зберігалися цією компанією, часто можуть стосуватися осіб, що перебувають в інших країнах. У результаті цих витоків даних кіберзлочинці можуть отримувати великі обсяги інформації, яку можна використовувати для крадіжок персональних даних, здійснення шахрайських дій засобами соціального інжинірингу та використання протиправних схем з авторизованими пуш-платежами, де персональні дані використовуються для завоювання довіри клієнта, або ж для використання номерів карток для шахрайства

Наприклад, у 2018 році виток даних стався у великій пасажирській авіакомпанії, коли хакери отримали секретні реквізити понад 244 000 кредитних карток. За інформацію з кожної картки хакери вимагали від 9 до 50 дол. США, і оціночні збитки склали 12,2 млн дол. США[2].

«Імена, електронні адреси, паролі, номери карток соціального страхування, дати народження, номери кредитних карток, банківські дані, номери паспортів, номери телефонів, домашні адреси, номери посвідчень водія, медичні картки — усе це було захоплено примарними хакерами, що завжди залишаються в тіні, скоюючи свої злочини»[3]

Дані та записи клієнтів, що стали публічно відомими[4]

Як свідчить цей звіт, поточний процес диджиталізації банківського сектора, безумовно, створює нові ризики шахрайства. Водночас він генерує деякі дивовижні нові рішення та можливості для тих, хто відповідає за захист клієнтів і активів банків. Враховуючи взаємозв'язок між технологіями і ризиками шахрайства, банки можуть виявити бажання надати у своїх цифрових стратегіях пріоритет запобіганню шахрайству і перешкоджанню фінансовим злочинам

Джадд Кеплейн

Керівник відділу глобального банкінгу та ринків капіталу, KPMG International

2. Соціальний інжиніринг. Детальний аналіз протиправних схем

Представники банків з країн EMA та Азіатсько-Тихоокеанського регіону, які взяли участь у дослідженні, згадали соціальний інжиніринг як один із 5 найбільших викликів.

Неправомірне використання засобів соціального інжинірингу може мати такі наслідки:

Недозволений доступ до рахунків клієнта, коли певні особи отримують персональні дані клієнтів, що використовуються для отримання доступу до їхніх банківських рахунків (використання номера картки клієнта у шахрайських цілях).

Приклади окремих методів, використовуваних шахраями для отримання даних клієнтів, наведені у Додатку 1.

Здійснення авторизованих платежів, де клієнта змушують переказати свої кошти на рахунок, що контролюється шахраєм, який вдає законного отримувача платежу. Такі дії також відомі як «протиправні схеми», «телефонне шахрайство» та «шахрайство з авторизованими пуш-платежами». У цьому звіті ми називаємо такі авторизовані клієнтами платежі «протиправними схемами».

Респонденти повідомили про збільшення випадків використання протиправних схем у кожному регіоні світу у 2018 році. Поряд із старими добрими прийомами на кшталт «нігерійських листів», шахраї вдаються до численних нових схем, включно зі встановленням романтичних стосунків з жертвою, діями від імені удаваних урядових чи податкових органів, інвестиційними схемами, лотереями, зламами ділової електронної кореспонденції, шахрайськими діями у сфері технологічної підтримки/віддаленого доступу та схемами, де зловмисники представляються жертвам їх онуками чи іншими родичами, тощо. Усі ці схеми застосовуються з однією метою: отримати доступ до даних жертви, які в подальшому використовуються для привласнення коштів жертви чи спонукання їх здійснити платіж на рахунок, контрольований шахраєм. Приклади таких протиправних схем подані у Додатку 2.

Збитки від протиправних схем зростають у геометричній прогресії.

У 2018 році Федеральне бюро розслідувань (ФБР) повідомило, що у 2013—2018 рр.[5] протиправні схеми зі зламом електронної кореспонденції завдали в глобальному масштабі збитків завбільшки у 12 млрд дол. США

Комісія з питань контролю конкуренції та прав споживачів Австралії (ACCC) повідомила, що у 2018 році збитки від протиправних схем у країні склали понад 0.5 млрд австралійських дол.[6]

Вірогідно, це лише верхівка айсберга, тому що не всі клієнти знають і не всі з них повідомляють про шахрайські дії проти них.

Жертвами протиправних схем стають різні люди. Хоча переважна більшість жертв таких схем — люди старшого покоління; іншими верствами, що стають мішенями зловмисників, також є:

— Соціально ізольовані або одинокі люди (схеми, що реалізуються шляхом встановлення романтичних стосунків)

— Особи, що мають фінансові труднощі (схеми, коли зловмисник пропонує жертві беззаставний кредит (за умови, що остання сплатить авансом комісію за відкриття кредиту, або ж зловмисник представляється жертві колектором, вимагаючи сплатити неіснуючий борг), а також інвестиційні програми під небувало високі проценти)

— Компанії (наприклад, працівник бухгалтерії отримує фейковий лист від фінансового директора, який перебуває у відпустці, з вимогою здійснити грошовий переказ

— Молоді особи, яким пропонується участь в організованих зловмисниками схемах працевлаштування, відпусток та лотерей.

Банки часто звинувачують у відсутності запобіжних заходів чи заходів виявлення протиправних схем. Обмежені можливості банків у сфері виявлення протиправних схем викликані тим, що тепер клієнти мають доступ до власних рахунків, і тому засоби контролю доступу не можуть виявляти такі схеми. Щоб протистояти ризику, який постійно зростає, сьогодні багато банків створили спеціальні групи боротьби з протиправними схемами та діють паралельно з робочими групами боротьби з шахрайством.

Існують випадки, коли банки виявляють протиправні схеми до початку обробки платежів, але клієнти настільки впевнені у законності транзакції, жертвами якої вони можуть стати, що вони категорично вимагають здійснити платіж навіть після того, як банк повідомив їм про те, що отримувач платежу — шахрай.

У більшості країн законодавство не визначає чітко особу, що несе відповідальність за відшкодування збитків, завданих протиправними схемами, і одні банки вважають, що за ці збитки відповідає клієнт, а інші банки аналізують кожний випадок окремо, щоб ухвалити рішення, чи зобов'язаний банк компенсувати клієнту завдані йому збитки.

Навіть якщо банк не несе відповідальність за дії зловмисників, емоційно напружена ситуація, коли клієнти усвідомлюють, що втратили значні кошти, вартує банківським працівникам чимало часу й зусиль.

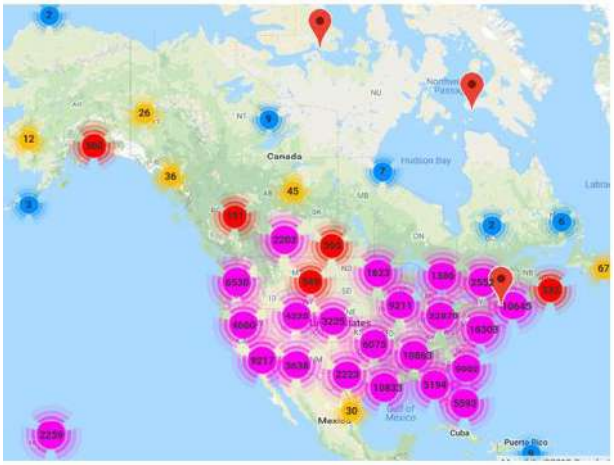
Якщо банк несе відповідальність за дії зловмисників, середній розмір збитків від протиправних схем значно вищий, ніж розмір збитків від шахрайства з платіжними картками.

Велика Британія затвердила Кодекс моделі потенційного відшкодування збитків від протиправних схем з авторизованими пуш-платежами (Кодекс), що має на меті надавати відшкодування

жертвам зловмисників у будь-якому випадку, якщо банк чи платіжна система визнані винними, а клієнт дотримувався стандартів, очікуваних від нього згідно з Кодексом[7]. Кодекс — добровільний, був розроблений з метою захисту клієнтів, а також для того, щоб регулюючі органи й уряд ухвалювали обґрунтовані рішення. Банки, що ухвалили рішення дотримуватися положень Кодексу, ще не оголошені, однак один великий роздрібний банк вже оголосив, що він відшкодує своїм клієнтам всі втрати від протиправних схем, включно з шахрайством з пуш--платежами[8]. Буде цікаво простежити, чи будуть впроваджені такі документи для банків в інших країнах.

Нижче відображені обсяги втрат від протиправних схем, заявлені жертвами та потенційними жертвами у США та Канаді у період з 1 липня 2015 р. по 22 квітня 2019 р.

Виявлено 152 595 випадків шахрайських схем



Джерело[9] на 22 квітня 2019 р.

3. Еволюція цифрових каналів та пришвидшення процесингу платежів: перехід на цифровий банкінг із скороченням часу фізичної присутності клієнтів

Респонденти з регіонів Америка та EMA визначили розвиток цифрових каналів як один з трьох найбільших викликів.

Частка продуктів і послуг, що реалізуються банками через цифрові канали, зростає. Згідно з прогнозами World Payments Report 2018, частка неготівкових операцій зросте сукупно на 12,7% до 2021 року.[1]

78% респондентів заявили, що понад чверть їхніх продуктів і послуг надається через цифрові канали. Ми стаємо свідками того, що на багатьох ринках з'являються цифрові нео- та челенджер-банки, які реалізують свої продукти виключно через цифрові канали.

В умовах зменшення кількості клієнтів, що утримують або знімають кошти з банківських рахунків завдяки доступності цифрового банкінгу та безготівкових платежів, необхідність фізичної присутності клієнтів при наданні банківських послуг зменшується. У результаті глобальний тренд закриття банківських філій поширюється.

У Великій Британії за останні 30 років закрито дві третини філій[11], у Європі — майже 6000[12], а у США — майже 9000 за останнє десятиріччя[13].

Із зменшенням кількості банківських філій та зростанням кількості користувачів цифрового банкінгу виникає необхідність у розширенні автоматизації банків з метою запобігання загрозам цифрового шахрайства, що постійно еволюціонують.

Крім того, пришвидшення процесингу платежів може нести новий виклик, оскільки банки матимуть менше часу на аналіз операцій на предмет шахрайства. Пришвидшення платежів також несе в собі ризик зменшення розміру відшкодування збитків, понесених в результаті шахрайства, оскільки проходження офшорних платежів через велику кількість рахунків здійснюватиметься за лічені секунди.

У пошуках збалансованості між заходами із запобігання ризику шахрайства та відносинами з клієнтами, як показує дослідження, банки застосовують засоби запобігання та виявлення шахрайства у режимі реального часу та встановлюють обмеження і додаткові засоби аутентифікації для операцій з високим ступенем ризику шахрайства, прагнучи зменшити його під час онлайн-платежів.

Аутентифікація псевдонімів також є ключовим моментом, зокрема у випадку операцій із стягнення платежів у режимі онлайн (pull payments), коли шахраї можуть вимагати здійснити платіж, представившись як комунальне підприємство або підприємство зв'язку. У Великій Британії на цей ризик відповіли, запровадивши вимогу підтвердження чеків отримувача платежу при запиті клієнтів на перерахування коштів.

Яка частина ваших продуктів/послуг реалізується через цифрові канали?

Джерело: Глобальне дослідження з питань шахрайства у банківській сфері, KPMG International 2019

− Скорочення кількості філій зменшує особисті контакти між банками та клієнтами, чим користуються організована злочинність та шахраї, здійснюючи транскордонні афери та добуваючи ідентифікаційні дані клієнтів через злами та фішинг з метою захоплення рахунків клієнтів у банках.

\+ Збільшення кількості цифрових операцій дозволяє отримати багатий набір даних щодо цифрової поведінки, які полегшують ідентифікацію потенційних випадків шахрайства, пов'язаного з платежами.

Наразі системи запобігання шахрайству у межах одного підприємства характеризуються надто високою розсередженістю та фрагментованістю. Фінансові установи повинні еволюціонувати у бік більш централізованих та ширших моделей управління ризиком шахрайства для того, щоб виявити шляхи досягнення синергії та підвищити ефективність

Енрік Ольсіна
Провідний партнер практики форензік, регіон Європи, Близького Сходу та Африки, KPMG в Іспанії

Банки інвестують у технології, що вдосконалюють процес виявлення шахрайства, чому ж тоді зростають збитки від шахрайства? Нижче ми розглядаємо виклики, з якими стикаються банки у процесі зменшення рівня ризику шахрайства, а також те, яким чином банки структурують свої підрозділи із запобігання шахрайству у відповідь на його загрозу.

4. Відкритий банкінг (Open Banking)

Респонденти з усіх регіонів визначили технологію відкритого банкінгу як один з 5 найбільших викликів для банків. У найближчі роки відкритий банкінг радикально змінить характер діяльності фінансових установ у глобальному масштабі, оскільки банки та фінансові установи передають інформацію про рахунки своїм клієнтам.

Клієнти матимуть змогу ділитися своїми реквізитами та операційними даними з третіми сторонами (такими, як інші банки, власники прикладних систем бюджетування, фінтех-компанії, телефонні компанії та інвестиційні платформи) через інтерфейси прикладного програмування (API).

Регуляторні органи все частіше заохочують, а в деяких країнах вимагають від банків надавати клієнтам доступ до відкритого банкінгу через розробку API.

Відкритий банкінг, ймовірно, вплине на управління ризиком шахрайства у фінансових установах у різні способи:

— Як і у випадку з усіма реформами, що зробили банкінг швидшим і зручнішим для клієнтів, існує ймовірність збільшення частки платежів, що здійснюються через цифрові канали, в результаті чого збільшиться обсяг операцій для банків при аналізі рахунків на предмет шахрайства.

— Банки сподіваються, що при використанні технологій відкритого банкінгу захист банківської інформації клієнтів здійснюватимуть треті сторони. Якщо треті сторони не зможуть забезпечити адекватний захист проти шахрайства, існує ймовірність того, що клієнти покладатимуть провину за це на банк, а не на прикладні системи бюджетування.

— Відкритий доступ до банківської інформації у фінансових установах створить можливість шахраям, що одержали такий доступ, зібрати більш чутливі дані щодо клієнтів, зокрема отримати більш цілісну картину щодо стану рахунків клієнтів та взяти на приціл рахунки з більш високими залишками коштів у різних банках.

— З іншого боку, більша прозорість інформації щодо рахунків клієнтів при обміні між банками дає можливість більш надійно ідентифікувати особу, виявляти рахунки-«прокладки» або фальшиві рахунки на більш ранньому етапі, а також ефективніше відстежувати грошові потоки за шахрайськими оборудками.

Як банкам підготуватися?

Безпека даних. Банківські записи містять чутливу, конфіденційну клієнтську інформацію, що вимагає найсуворішого дотримання стандартів безпеки даних. Банки повинні забезпечити наявність надійних засобів контролю безпеки даних у API, а також ретельну перевірку сторонніх розробників до того, як останні отримають доступ до клієнтської інформації та будуть акредитовані як провайдери послуг.

Цифрова ідентифікація. Відкритий банкінг великою мірою ґрунтується на інтегрованих засобах цифрової ідентифікації. Створення консолідованого цілісного онлайн-профілю користувача-фізичної особи, організації або електронного пристрою дасть можливість зробити процес аутентифікації безпечним та органічним.

Управління доступом. Банки потребують можливості надання клієнтам доступу до своїх даних з дотриманням належного рівня безпеки та конфіденційності. Це вимагатиме створення системи управління наданням (і скасуванням) прав доступу з використанням обмежень і заходів безпеки. Подібно до користування обліковими записами при доступі до соціальних медіа, надання клієнтам доступу до банківських рахунків вимагає наявності стандартизованих або адаптованих протоколів управління доступом для обміну та використання даних із сторонніми провайдерами послуг.

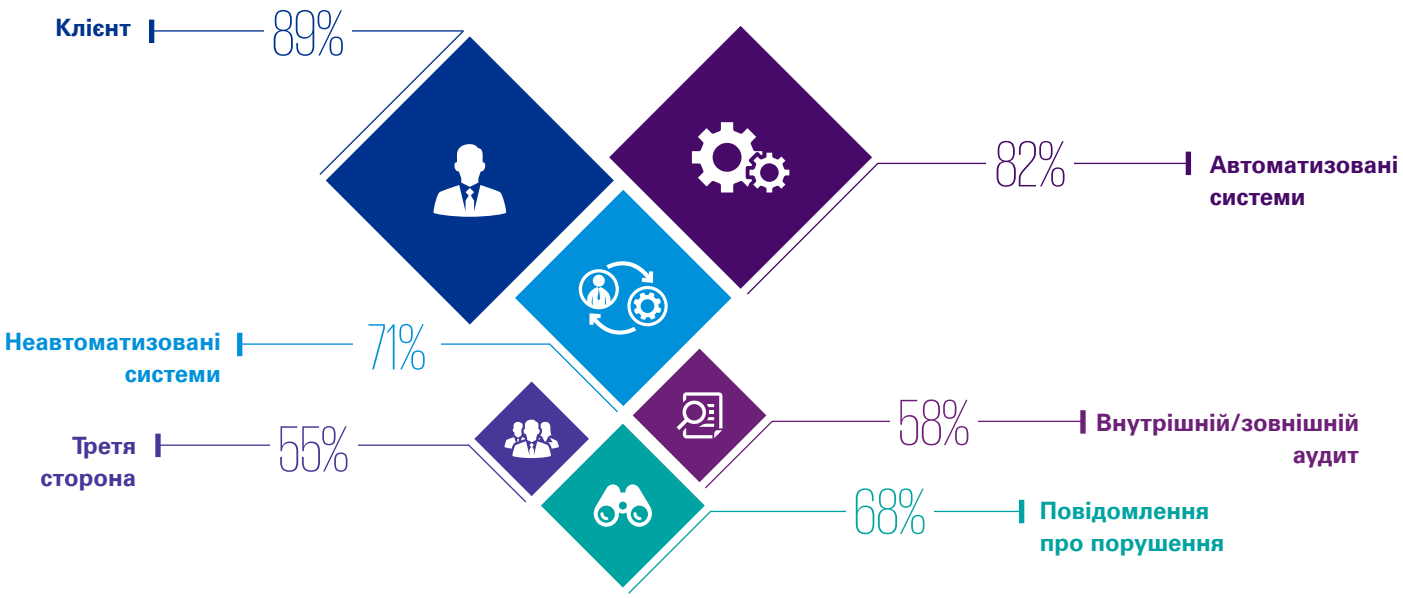
Поширення відкритого банкінгу в світі за роками:

Можливо зробити більше для того, щоб клієнти усвідомили нові виклики

Клієнти грають основну роль у запобіганні та виявленні протиправних схем, зокрема у випадках, коли платіж виконується клієнтом. Під час опитування більшість респондентів заявили про те, що джерелом викриття шахрайських дій, ідентифікованих у 2018 році, були саме клієнти.

Враховуючи цей факт, а також виявлений під час опитування низький рівень відшкодування збитків від шахрайства (понад половина опитуваних заявила про те, що рівень відшкодування становить менше 25%), банки можуть зробити більше для того, щоб навчити клієнтів, як запобігати та виявляти випадки шахрайства.

Як банки ідентифікують шахрайські дії?



Методи шахраїв стають усе витонченішими. Для озброєння клієнтів навичками, необхідними для того, щоб не стати жертвою шахраїв, банки повинні навчити клієнтів:

- своєчасно перевіряти стан їхніх рахунків;
- робити зворотний пошук google-зображень, що використовуються зловмисниками на сайтах знайомств;
- розпізнавати фішингові повідомлення, що надходять електронною поштою, текстові/SMS-повідомлення та телефонні дзвінки;
- часто змінювати паролі;
- ігнорувати спливаючі вікна;
- розпізнавати електронний спам через орфографічні помилки, відсутність надійної інформації про вебсайт, підозрілі посилання та адреси електронної пошти, інші, ніж в організації, від імені якої нібито надійшло повідомлення;
- у разі невпевненості спитати товариша або члена родини;
- пам'ятати, що представник реальної організації ніколи не запитуватиме у вас ваші паролі, а також не заперечуватиме, якщо ви попросите завершити дзвінок та перетелефонувати на номер з вашого клієнтського файла;
- стерегтися спуфінгової атаки на автоматичний визначник номера (Caller ID spoofing), коли шахраї намагаються імітувати номер установи, за яку вони себе видають. Технологія Caller ID spoofing застосовувалася, наприклад, коли шахраї видавали себе за друзів або членів родини потерпілого, що перебувають на місці нещасного випадку, заявляючи, що останній залишиться помирати, якщо їм не перерахують гроші.[14]
- пам'ятати, що за надто вигідною пропозицією можуть стояти шахраї.

Крім того, робота з клієнтами в цьому напрямку повинна охоплювати користувачів як цифрових, так і нецифрових каналів, зокрема, літніх людей або інші вразливі категорії, яким бракує відповідних технічних знань.

Джерело: Глобальне дослідження з питань шахрайства у банківській сфері, KPMG International 2019

Операційна модель управління ризиком шахрайства

Скільки коштує управління ризиком шахрайства і наскільки воно ефективне?

Під час дослідження ми формулювали запитання таким чином, щоб мати змогу зрозуміти, яким чином банки структурують свою діяльність з управління ризиком шахрайства з метою оптимізації розподілу ресурсів, а також інформування тих, хто ухвалює рішення щодо інвестицій на рівні корпоративного управління, персоналу, процесів і технологій.

Хоча діяльність з управління ризиком шахрайства є обліково-витратною, 52% опитаних банків не відстежують, у скільки саме вона загалом їм обходиться. Це надає їй другорядного значення серед здійснюваних банком операцій і применшує значимість в очах ради директорів і комітетів з управління ризиками, які ухвалюють ключові рішення щодо бюджету, розподілу ресурсів та інвестицій.

Під час обговорення за ефективність роботи підрозділів з протидії запобігання шахрайству, ми отримали різноманітні відповіді щодо відповідальності посадових осіб за ефективне запобігання шахрайським діям, їх виявлення та реагування у випадках, коли виникає підозра у шахрайстві, а також щодо відшкодування збитків від шахрайства. Відповіді варіювалися в залежності від відсутності у банках офіційного аналізу до наявності скорингових карт/ключових показників ефективності, прогнозування збитків, планування/ризик-апетиту, оцінки задоволення бізнесу/клієнта, застосування методу «контрольних закупівель» і наявності ешелонованої системи захисту від шахрайства.

Ми отримали різноманітні відповіді щодо того, як фінансові установи в усьому світі структурують свої операційні моделі управління ризиком шахрайства.

Джерело: Глобальне дослідження з питань шахрайства у банківській сфері, KPMG International 2019

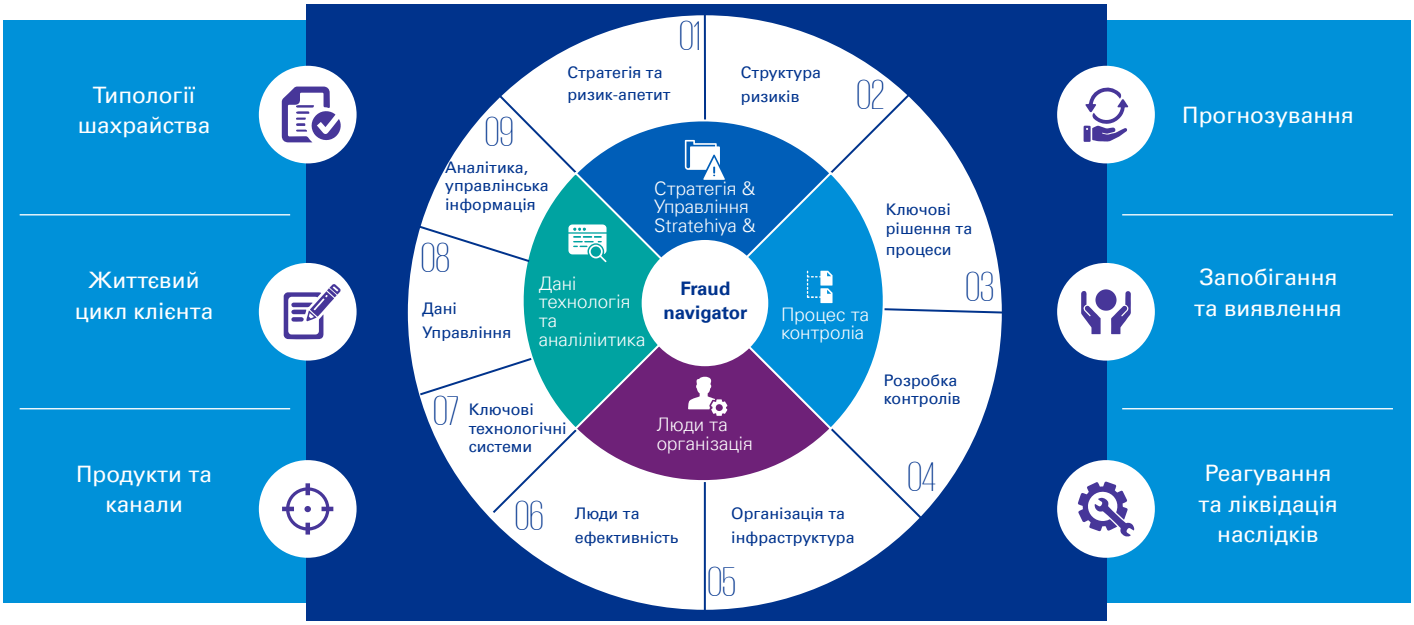
> *Відповідно до того, як удосконалюються методи й ускладнюються ризики шахрайства в результаті переходу на цифрові технології та рішення, регулюючі органи все більше очікують від фінансових установ більшої узгодженості та інтеграції підходів першої та другої ліній захисту з метою запобігання, виявлення та реагування на ризики шахрайства.*

Томас Стентон

Провідний партнер практики управління ризиками шахрайства, регіон Північної, Центральної та Південної Америки, KPMG у США

KPMG: Модель управління ризиками шахрайства (KPMG's Fraud navigator)

Добре структурована операційна модель управління ризиком шахрайства та оцінка ризиків на рівні організації є важливими чинниками, що забезпечують банкам надійність захисту, дозволяючи постійно зменшувати ризик внутрішнього та зовнішнього шахрайства у межах ризик-апетиту банку.



За результатами опитування, не всі респонденти мають документально оформлену операційну модель з управління ризиком шахрайства, проводять оцінку ризику шахрайства на рівні підприємства та створюють комітет із запобігання шахрайству:

Корпоративне управління, персонал, процеси...

ТУ під час опитування було виявлено відмінності у тому, як фінансові установи структурують операції з управління ризиком шахрайства, при цьому відповідальність за управління ризиком розподілялася таким чином:

— **69%** всіх операцій припадає на першу лінію захисту, яка управляється працівниками бізнес-підрозділів/співробітниками, що працюють безпосередньо з клієнтами (перша лінія);

— **31%** всіх операцій припадає на другу лінію захисту, побудовану на принципі групової безпеки, яка здійснює нагляд за управлінням ризиками і комплаєнс-контроль бізнес-підрозділів (друга лінія).

Структури, відповідальні за управління ризиком шахрайств, підпорядковувалися комітету із запобігання шахрайству, головному посадовцю з управління ризиками, голові служби комплаєнсу, головному юрисконсульту та службі внутрішнього аудиту.

Цікаво, що єдиної «правильної» моделі, яка використовувалася б банками глобально з метою послідовного структурування операцій з управління ризиком шахрайства, схоже, не існує.

Під час опитування виявлено розбіжності в тому, хто визначає ризик-апетит у банках щодо ризику шахрайства:

✱ **52%** Рада директорів/Комітет з управління ризиками ✱ **29%** First line ✱ **5%** Second line

Джерело: KPMG Fraud navigator 2019

…і технології

Перед фінансовими установами постає серйозний виклик — зробити так, щоб їхні методи захисту випереджали методи шахраїв. Банки дедалі більше шукають можливості для вдосконалення своїх систем за рахунок посилення моніторингу трансакцій із залученням технологій машинного навчання/штучного інтелекту та біометричного управління доступом. Більшість респондентів, що взяли участь в опитуванні, інвестували у наведені нижче методи прогнозування, запобігання та виявлення спроб шахрайства:

— подвійна або багатофакторна аутентифікація з метою перевірки ідентичності клієнта (вимоги до користувачів надати дані, наприклад, пароль, з використанням інших факторів, наприклад, текстового повідомлення/SMS-коду або відбитків пальців);

— 70% опитаних банків мають технологічні рішення, що дозволяють скорингову оцінку ризиків та ухвалення рішень у режимі реального часу;

— 67% використовують фізичну біометрію (ідентифікація за голосом і відбитками пальців, технологія розпізнавання облич). Зазначимо, що сьогодні кіберзлочинцями створено ринок цифрових відбитків пальців, і мали місце випадки, коли шахраї записували та відтворювали голоси клієнтів, використовуючи нові технології[15];

— 63% використовують комбінацію правил та машинного навчання, вбудовану у їхні технології з метою забезпечити виявлення шахрайських дій.

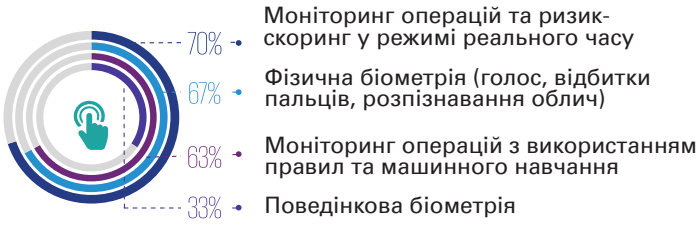
Респонденти повідомили про інвестиції у поведінкову біометрію, технології негативних оглядів медіа, аналіз мереж та аутентифікацію через Google.

Незважаючи на інвестування у нові технології, 51% опитаних банків повідомили про значну кількість хибнопозитивних результатів від їхніх технологічних рішень, які шкодять ефективності процесу виявлення шахрайських дій.

Неефективні системи впливають на інформацію щодо управління ризиком шахрайства : може, причини ризиків, що їх зазнають банки, лежать на поверхні? Неякісно складена звітність також може негативно вплинути на здатність ради директорів і комітетів з управління ризиками правильно розподіляти ресурси та ухвалювати рішення про інвестиції, при цьому шахрайство при інвестуванні, як показує опитування, мало чим відрізняється від фінансового злочину.

Крім того, з огляду на розмір та складність банківських операцій та процесів реалізація змін може потребувати часу. Зі свого боку, шахраї можуть діяти дуже оперативно. Оскільки шахрайства, такі, як використання протиправних схем і крадіжка персональних даних/соціальна інженерія з метою незаконного отримання доступу до банківських рахунків клієнтів, набирають обертів, а організована злочинність обмінюється знаннями через свої мережі в різних юрисдикціях для того, щоб обійти засоби виявлення шахрайських дій, які застосовуються банками. Останні визнають необхідність постійно відточувати свої знання та навички з управління ризиками шахрайства.

Частка респондентів, що інвестували у нижченаведену технологію



На думку учасників опитування, подальше удосконалення шляхів виявлення шахрайства потребує інвестування у нові технології упродовж наступних трьох років, зокрема такі:

— технологія моніторингу операцій з використанням машинного навчання (штучний інтелект)/робототехніки;

— інноваційне програмне забезпечення у сфері фінтеху/регтеху, що забезпечує автоматизацію надання фінансових послуг, зокрема за принципом «Знай свого клієнта»;

— біометрія та більш активне використання даних, отриманих з відкритих джерел і соціальних медіа.

Зрештою, для банків й надалі існує можливість оптимізувати свою операційну модель на рівні корпоративного управління, персоналу, процесів і технологій, зокрема зосередившись на:

— досягненні балансу між кадровою укомплектованістю та технологічними змінами;

— оптимізації розміщення ресурсів шляхом їхнього планування, незважаючи на невизначеність щодо часу фінансування;

— посиленні систем виявлення шахрайських дій, зокрема зменшенні кількості хибнопозитивних результатів через цикл зворотного зв'язку з метою вдосконалення алгоритмів та наборів правил.

Для досягнення результатів та оптимізації роботи своєї операційної моделі управління ризиками на рівні корпоративного управління, персоналу, процесів і технологій банки не повинні при плануванні покладатися виключно на нові технології.

Джерело: Глобальне дослідження з питань шахрайства у банківській сфері, KPMG International 2019

Як щодо того, щоб об’єднати функції управління ризиком шахрайства та комплаєнсу у сфері протидії фінансовим злочинам?

В усьому світі у разі неповідомлення про можливе відмивання коштів або іншого такого невиконання вимог щодо контролю з метою боротьби з фінансовими злочинами передбачено значні штрафи, які впливають на інвестиційні рішення банків, в результаті чого останні приділяють боротьбі з фінансовими злочинами більшу увагу, ніж шахрайству.

Як показують результати опитування, понад 50% респондентів в усьому світі планують більше інвестувати у діяльність з контролю за виконанням вимог міжнародних фінансових установ щодо боротьби з фінансовими злочинами (боротьба з відмиванням грошей та фінансуванням тероризму (AML CTF), хабарництвом і корупцією (ABC), а також вимог щодо контролю за дотриманням санкцій), ніж в управління ризиком шахрайства.

За результатами нашого огляду, 43% респондентів вели інтегровану звітність, 40% мали інтегровані структури корпоративного управління, 38% — інтегровані системи та 35% — інтегровані штатні обов’язки у зв’язку з управлінням ризиком шахрайства та комплаєнсом у сфері протидії фінансовим злочинам.

Для 43% інтеграція між функціями управління ризиком шахрайства та комплаєнсу у сфері протидії фінансовим злочинам була відсутня.

У таблиці нижче наведені наші міркування щодо використання неінтегрованих та інтегрованих моделей комплаєнсу щодо шахрайства та фінансових злочинів.

Ймовірні переваги об’єднання двох функцій

Інтегровані команди з управління ризиком шахрайства та протидії фінансовим злочинам з огляду на персонал та процеси

- Діяльність, пов’язана з протидією фінансовим злочинам, наприклад, комплаєнс за принципом «Знай свого клієнта» та повідомлення про підозрілі операції, також має відношення до ризику шахрайства. Наявність єдиної команди з єдиною стратегією створює можливість більш високого рівня взаємодії при розслідуванні однієї й тієї ж атаки/інциденту, наприклад, надходжень від злочину (шахрайства) через рахунки-«прокладки», про які банк має повідомити регулятора з питань протидії фінансовим злочинам.
- Наявність персоналу з різним набором ролей та ідей дає переваги інтегрованим командам.
- Уникнення дублювання зусиль або втрати комунікації у зв’язку з інцидентами впливає як на діяльність з управління ризиком шахрайства, так і на запобігання фінансовим злочинам.
- Напрями боротьби з фінансовими злочинами й управління ризиком шахрайства отримують спільні вигоди від інвестування.

Інтегровані команди з управління ризиком шахрайства та протидії фінансовим злочинам з точки зору технології

- Об’єднання екстрених розслідувань інцидентів з динамічним профайлінгом клієнтів за обома напрямками.
- Економія витрат за рахунок використання однієї й тієї ж технічної платформи з різними модулями та користувацькими інтерфейсами.

Ймовірні причини окремого сприйняття шахрайства та фінансових злочинів

Відокремлені команди з управління ризиком шахрайства та протидії фінансовим злочинам

- Ймовірно, що головним чинником окремого сприйняття шахрайства та фінансових злочинів є розбіжності у регуляторних вимогах, які передбачають значні штрафи у випадку неінформування регулюючих органів про підозрілі операції, а також штрафи й тюремні строки за хабарництво/корупцію у деяких країнах, зокрема у регуляторних документах Комісії США з цінних паперів і фондових бірж (SEC) та Міністерства юстиції США. Водночас такі покарання за неповідомлення про випадки шахрайства не передбачені.
- Укорінена організаційна культура («Ми завжди так робили»).

Окремі системи управління ризиком шахрайства та протидії фінансовим злочинам

- Можливість відібрати «найкращі наявні» системи управління ризиком шахрайства та запобігання фінансовим злочинам, потенційно разом з наявністю третьої системи, здатної вести розслідування в обох напрямках.
- Потенційний брак знань щодо належних рішень, за допомогою яких можна управляти обома ризиками.

Висновок

У контексті змін глобального банківського ландшафту — скорочення кількості банківських філій, збільшення обсягів цифрових платежів та обробки платежів за лічені секунди — шахраї демонструють винахідливість, знаходячи нові способи привласнення коштів банків та їхніх клієнтів.

Якою має бути реакція банків?

Як показують результати нашого дослідження, центр уваги шахраїв переміщується з незаконного отримання доступу до рахунків на протиправні схеми, в яких клієнти використовуються як слабка ланка. Банкам необхідно зробити більше у справі обізнаності та захисту своїх клієнтів.

Результати нашого дослідження ще раз підтверджують, що потенційна шкода від шахрайства всередині банку може бути такою ж самою, якщо не більшою, ніж від зовнішнього шахрайства, враховуючи здатність працівників банку скористатися слабкими місцями контролю з метою атаки на найбільш цінні активи банку. Банкам слід й надалі діяти на випередження з метою виявлення до виявлення випадків внутрішнього шахрайства.

У контексті того, що все більше країн впроваджують технології відкритого банкінгу, банки повинні розширити свої можливості щодо аналізу великих даних у середовищі відкритого банкінгу та краще орієнтуватися в інтерфейсах прикладного програмування (API)

Методи як внутрішнього, так і зовнішнього шахрайства стають чимдалі досконалішими. Для банків зростає потреба забезпечити операційну ефективність і результативність цифрових систем і засобів контролю ризиків шахрайства, а також підвищити кваліфікацію персоналу щодо прогнозування, запобігання та виявлення шахрайських дій. Неефективні системи впливають на інформацію щодо управління ризиком шахрайства: можливо, причини ризиків, що їх зазнають банки, лежать на поверхні? Неякісно складена звітність також може негативно вплинути на здатність ради директорів і комітетів з управління ризиками правильно розподіляти ресурси та ухвалювати рішення про інвестиції, при цьому шахрайство при інвестуванні, як показує опитування, мало чим відрізняється від фінансового злочину.

Власне технології недостатньо, враховуючи, що наші глобальні респонденти повідомляють про наявність хибнопозитивних результатів, які стримують ефективність процесу виявлення випадків шахрайства. Банки повинні планувати, не покладаючись виключно на нові технології, для досягнення результатів та оптимізації роботи своєї операційної моделі управління ризиками на рівні корпоративного управління, персоналу, процесів і технологій.

Методи шахраїв стають усе витонченішими, а їхні підходи можуть швидко змінюватися та адаптуватися. Банкам необхідно оперативно реагувати на нові загрози та опановувати нові підходи та технології з метою прогнозування та запобігання шахрайству.

Додаток 1

Приклади методів соціальної інженерії

Фішинг — вид атаки, під час якої зловмисник надсилає електронні листи, видаючи себе за когось іншого, з тим, щоб отримати особисту інформацію від своєї жертви. Фішинг зазвичай полягає у тому, що користувача спонукають перейти за посиланням, увівши свій пароль, після чого зловмисник має достатньо інформації для отримання доступу до облікового запису або поштової скриньки жертви. У середньому 4% цільових користувачів будь-якої фішинг-кампанії натискають на посилання. Синонім: спуфінг.

Цільовий фішинг — полягає у спробах фішинг-атаки, коли зловмисник використовує інформацію з відкритих джерел для створення електронних листів, спрямованих значною мірою на подальше заохочення жертви натиснути на посилання, що міститься у листі. Наприклад, зловмисник може дізнатися через соціальні мережі, що жертва очікує посилку, і створює фішинг-лист, який виглядає як повідомлення від служби доставки і містить інформацію про посилку та фейкове посилання для відстеження доставки.

Претекстинг — форма соціальної інженерії, за якою зловмисник фабрикує сценарій, переконливий привід для того, щоб вимагати інформацію від жертви. Як правило, зловмисники видають себе за людей, наділених певною владою, наприклад, за представників податкових органів або банків, і просять жертву надати інформацію з метою підтвердження її особи.

Бейтинг (англ. bating - заманювання) — метод психологічної атаки, що полягає у маніпулюванні жертвою через її цікавість. Зловмисник пропонує жертві певний специфічний товар (наприклад, оновлене програмне забезпечення, приз або залишений у громадському місці USB), з тим, щоб жертва підключила його до свого комп'ютера, після чого виявляється, що на комп'ютері жертви встановлено шкідливе програмне забезпечення.

Quid Pro Quo — варіант заманювання, коли зловмисник обіцяє послугу або якусь вигоду після виконання жертвою конкретної дії. Наприклад, хакер може видати себе за фахівця з IT-безпеки, пропонуючи оновлення програмного забезпечення, за умови, що жертва спочатку відключить своє антивірусне програмне забезпечення, тим самим забезпечивши безперешкодне встановлення на свій комп'ютер шкідливого програмного забезпечення.

Додаток 2

Середня сума втрачених коштів за кожним видом протиправних схем

Інвестиція	$8 648
Романтичні стосунки	$6 003
Переїзд	$3 993
Криптовалюта*	$3 147
Ремонт житла	$2 895
Нігерійські листи/обмін валют	$2 133
Злам ділової корпоративної кореспонденції	$1 717
Термінова допомога члену сім'ї/другу	$1 219
Підробка	$1 210
Подорожі/відпустка	$887
Кредит за передоплатою	$716
Благодійність	$708
Викрадення ідентифікаційних даних	$683
Оренда	$662
Працевлаштування	$598
Тоталізатор/ лотерея/ приз	$547
Фіктивний інвойс	$441
Реструктуризація кредиту/полегшення тягаря заборгованості	$388
Покупка онлайн	$365
Фіктивний чек/ платіжне доручення	$341
Фіктивна технічна підтримка	$255
Схеми з кредитними	$231
Державна субсидія	$218
Медичне обслуговування	$170
Стипендія	$155
Комунальні послуги	$106
Стягнення боргу	$98
Жовті сторінки/ Довідник	$91
Фішинг	$44
Стягнення податків	$31
Інше	$746

* Означає категорію, яку вперше було відстежено у 2018 році

Середній розмір збитків у країнах Північної і Південної Америки за видами протиправних схем.

Інвестиційні схеми — вид схеми, під час якої жертві розповідають про неймовірні можливості, часто гарантуючи їй високі прибутки, якщо вона інвестує власні кошти. З жертвою найчастіше зв'язуються телефоном або електронною поштою шахраї, стверджуючи, що вони дають вигідну інвестиційну пораду.

Романтичні стосунки — схеми з використанням сайтів знайомств спрямовані переважно на людей, які перебувають у пошуках кохання. Зловмисники створюють фіктивні профілі на веб-сайтах знайомств або у соціальних мережах, видаючи себе за потенційних партнерів для романтичних стосунків.

Джерело: BBB Scam Tracker, 2015 – грудень 2018

Додаток 2 (продовження)

Після зазвичай тривалих онлайн-залицянь шахрай просить передати йому гроші, подарунки або особисту інформацію. Зловмисники часто грають на емоційних тригерах жертв, наприклад, просять грошей на оплату «медичних рахунків для члена сім'ї» або на квиток на літак, щоб отримати можливість побачитися з жертвою.

Шахраї також можуть просити прислати їм інтимні фотографії, які вони потім використовують для шантажування жертви.

Нігерійські листи — одна з найдавніших схем, в якій на жертву виходить людина, що називає себе дуже багатим іноземцем та/або членом королівської сім'ї і просить допомогти їй у переказі коштів зі своєї країни в обмін на можливість отримати частку в операції вартістю у кілька мільйонів доларів, як і раніше, є надзвичайно поширеним та ефективним. Жертву просять сплатити податки, дати хабар державним службовцям і оплатити судові витрати, обіцяючи, що всі витрати будуть відшкодовані, щойно кошти будуть виведені за межі країни. Отримавши платіж або банківські реквізити, королівська особа зникає, часто разом з коштами з банківського рахунку жертви.

Злам ділової електронної кореспонденції — як одна з найпоширеніших протиправних схем, BEC спрямована на осіб, які мають доступ до банківських операцій компанії, і за допомогою соціальної інженерії обманним шляхом спонукає їх платити шахраям. Часто шахрай видає себе за генерального директора компанії і вимагає здійснити терміновий платіж в обхід стандартних заходів контролю. За даними Центру прийому скарг щодо інтернет-злочинів, який входить до складу ФБР, опублікованими у червні 2018 року, сума збитків, завданих BEC-схемами, становить 12 мільярдів дол. США.

Термінова допомога члену сім'ї/ другу — шахрай, який зазвичай орієнтується на людей похилого віку і користується тим, що вони недочувають, видає себе за їхнього онука чи онуку. «Онук» говорить, що він потрапив у біду і потребує грошей (наприклад, стверджуючи, що він перебуває у в'язниці або у нього виникли проблеми із законом чи борги). Жертві говорять, що вона є єдиною людиною, якій онук довіряє, і що вона не повинна нікому розповідати про це. Зловмисники використовують дані з соціальних мереж, щоб їхні історії звучали більш правдоподібно, і говорять приглушеними голосами, вдаючи, що вони плачуть.

Лотереї — випадку протиправних схем з лотереями зловмисники виходять на жертву і повідомляють їй, що вона виграла у розіграші лотереї чи призу, в яких жертва насправді ніколи не брала участь. Жертву просять сплатити комісійні за видачу або доставку подарунку чи грошей. Їй також можуть запропонувати зателефонувати за номером з високим тарифом оплати, щоб отримати приз. Часто шахраї використовують назви реальних розіграшів з тим, щоб жертва могла переконатися в їхній законності, якщо вона захоче отримати більш детальну інформацію.

Схеми у сфері технічної підтримки/дистанційного доступу — протиправні схеми у вигляді фіктивних пропозицій щодо надання технічної підтримки/отримання дистанційного доступу полягають у тому, що жертву переконують, що виникла проблема з її комп'ютером або з інтернетом, і що для вирішення проблеми необхідно встановити нове програмне забезпечення. Жертва отримує телефонний дзвінок, електронне повідомлення або pop-up повідомлення на екрані її комп'ютера, що інформує її про проблеми з підключенням до інтернету або з її комп'ютером і спрямовує її до шахрая, який нібито може усунути ці проблеми. При цьому зловмисники можуть посилатися на типові проблеми, що виникають у користувачів, наприклад, швидкість інтернету. Потім вони просять жертву надати їм дистанційний доступ, щоб «з'ясувати, в чому полягає проблема». Як тільки шахрай отримує доступ до комп'ютера жертви, він викрадає її дані, отримує доступ до її банківських рахунків і нерідко здійснює платежі собі самому.

Протиправні дії від імені удаваних державних органів— шахраї, що посилаються на державні органи, телефонують жертвам або надсилають їм листи чи електронні повідомлення, видаючи себе за представників судових чи податкових органів. У деяких випадках шахрай вимагає негайно здійснити платіж для погашення заборгованості, наприклад, простроченого штрафу за порушення правил паркування або прострочених податків. Шахрай може погрожувати тим, що несплата призведе до збільшення суми заборгованості чи терміну ув'язнення.

Додаток 3

Джерела

2013 Target: 110 million. Based on figure quoted in report by The Huffington Post, «Target Hacked: Retailer Confirms 'Unauthorised Access' Of Credit Card Data» (19 December 2013). Available at https://www.huffpost.com/entry/target-hacked-customer-credit-card-data-accessed_n_4471672

2013 Yahoo: 3 billion. Based on figure quoted in report by The New York Times, «All 3 Billion Yahoo Accounts Were Affected by 2013 Attach» (Nicole Perlroth, 3 October 2017). Available at: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

2014 Yahoo: 500 million. Based on figure quoted in report by The Washington Post, «Yahoo confirms data breach affecting at least 500 million accounts» (Hayley Tsukayama, Craig Timberg & Brian Fung, 22 September 2016). Available at: https://www.washingtonpost.com/news/the-switch/wp/2016/09/22/report-yahoo-to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts/

2014 Ebay: 145 Million. Based on figure quoted in report by The Washington Post, «eBay asks 145 million users to change passwords after data breach» (Andrea Peterson, 21 May 2014). Available at: https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/

2016 Adult Friend Finder: 412 million. Based on figure quoted in report by The Verge, «Over 300 million AdultFriendFinder accounts have been exposed in massive breach» (Andrew Liptak, 13 November 2016). Available at: https://www.theverge.com/2016/11/13/13615750/412-million-adultfriendfinder-accounts-exposed-breach

September 2017 Equifax: 148 million American Consumers. Based on figure produced by U.S. House of Representatives Committee on Oversight and Government Reform, The Equifax Data Breach Report (December 2018) p2. Available at: https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

August 2018 Chinese Huazhu Hotels Group: 500 million records. Based on figures quoted in report by China Daily, «Huazhu Hotels Group investigates alleged info leak» (29 August Adata (including name and mobile numbers), 130 million check-in records (including name and address) and 240 million hotel stay records (including credit card numbers and check in and out dates).

September 2018 Facebook: 50 million accounts. Based on figures quoted in report by The Guardian, «Facebook says nearly 50m users compromised in huge security breach» (Julia Carrie Wong, 29 September 2018). Available at: https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

2018 Marriott International: 500 million records. Based on figures quoted in report by The New York Times, «Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing» (David E. Sanger et al, 11 December 2018). Available at: https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

The Daily Mail, «Russian hackers made £9.4m from British Airways data breach with customers' credit card details put on sale for as little as £6.94, experts say» (Sami Quadri, 14 November 2018). Credit card details available for sale were from customers through Europe and from Mexico, Brazil and China including others. Available at: https://www.dailymail.co.uk/news/article-6387001/Russian-hackers-9-4m-British-Airways-data-breach.html

Wired, «The Wired Guide to Data Breaches» (Lily Hay Newman, 12 July 2018). Available at: https://www.wired.com/story/wired-guide-to-data-breaches/

FBI Public Service Announcement, «Business E-Mail Compromise: The 12 Billion Dollar Scam» (12 July 2018). Report states that 78,617 incidents of business e-mail compromise scams occurred between October 2013 and May 2018 resulting in global losses of US$12,536,948,299. Business e-mail compromise scams are defined as «when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorised transfers of funds». Available at: https://www.ic3.gov/media/2018/180712.aspx

Australian Competition and Consumer Commission, Targeting Scams Report (May 2019). $489 billion in losses reported to the ACCC from over 378,000 scam reports. Available at https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2018

Authorised Push Payment Scams Steering Group 28 February 2019 Press release, and attached copy of the Code. The Code states that the customer may not be refunded if the customer «ignored effective warnings», «did not take appropriate actions» or where the behaved in a way that was «grossly negligent». The Code comes into force on 28 May 2019, signatories have not yet been announced. Available at: https://appcrmsteeringgroup.uk/app-scams-steering-g

[1] Faster payments, Cyber and data breaches, Payment Services Directive 2/ Open banking, Virtual currencies,
Evolving digital channels, Social engineering, Criminal use of artificial intelligence.

[2] The Daily Mail, «Russian hackers made £9.4m from British Airways data breach with customers' credit card details put on sale for as little as £6.94, experts say» (Sami Quadri, 14 November 2018). Credit card details available for sale were from customers through Europe and from Mexico, Brazil and China including others. Available at: https://www.dailymail.co.uk/news/article-6387001/Russian-hackers-9-4m-British-Airways-data-breach.html

[3] Wired, «The Wired Guide to Data Breaches» (Lily Hay Newman, 12 July 2018). Available at: https://www.wired.com/story/wired-guide-to-data-breaches/

[4] 2013 Target: 110 million. Based on figure quoted in report by The Huffington Post, «Target Hacked: Retailer Confirms 'Unauthorised Access' Of Credit Card Data» (19 December 2013). Available at https://www.huffpost.com/entry/target-hacked-customer-credit-card-data-accessed_n_4471672

2013 Yahoo: 3 billion. Based on figure quoted in report by The New York Times, «All 3 Billion Yahoo Accounts Were Affected by 2013 Attach» (Nicole Perlroth, 3 October 2017). Available at: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

2014 Yahoo: 500 million. Based on figure quoted in report by The Washington Post, «Yahoo confirms data breach affecting at least 500 million accounts» (Hayley Tsukayama, Craig Timberg & Brian Fung, 22 September 2016). Available at: https://www.washingtonpost.com/news/the-switch/wp/2016/09/22/report-yahoo-to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts/

2014 Ebay: 145 Million. Based on figure quoted in report by The Washington Post, «eBay asks 145 million users to change passwords after data breach» (Andrea Peterson, 21 May 2014). Available at: https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/

2016 Adult Friend Finder: 412 million. Based on figure quoted in report by The Verge, «Over 300 million AdultFriendFinder accounts have been exposed in massive breach» (Andrew Liptak, 13 November 2016). Available at: https://www.theverge.com/2016/11/13/13615750/412-million-adultfriendfinder-accounts-exposed-breach

September 2017 Equifax: 148 million American Consumers. Based on figure produced by U.S. House of Representatives Committee on Oversight and Government Reform, The Equifax Data Breach Report (December 2018) p2. Available at: https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

August 2018 Chinese Huazhu Hotels Group: 500 million records. Based on figures quoted in report by China Daily, «Huazhu Hotels Group investigates alleged info leak» (29 August 2018). Available at: http://www.chinadaily.com.cn/a/201808/29/WS5b86473da310add14f38871b.html. Unauthorized access to Huazhu Hotels Group 123 million pieces of registration data (including name and mobile numbers), 130 million check-in records (including name and address) and 240 million hotel stay records (including credit card numbers and check in and out dates).

September 2018 Facebook: 50 million accounts. Based on figures quoted in report by The Guardian, «Facebook says nearly 50m users compromised in huge security breach» (Julia Carrie Wong, 29 September 2018). Available at: https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

2018 Marriott International: 500 million records. Based on figures quoted in report by The New York Times, «Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing» (David E. Sanger et al, 11 December 2018). Available at: https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

[5] FBI Public Service Announcement, «Business E-Mail Compromise: The 12 Billion Dollar Scam» (12 July 2018). Report states that 78,617 incidents of business e-mail compromise scams occurred between October 2013 and May 2018 resulting in global losses of US$12,536,948,299. Business e-mail compromise scams are defined as «when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorised transfers of funds». Available at: https://www.ic3.gov/media/2018/180712.aspx

[6] Australian Competition and Consumer Commission, Targeting Scams Report (May 2019). $489 billion in losses reported to the ACCC from over 378,000 scam reports. Available at https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2018

[7] Authorised Push Payment Scams Steering Group 28 February 2019 Press release, and attached copy of the Code. The Code states that the customer may not be refunded if the customer «ignored effective warnings», «did not take appropriate actions» or where the behaved in a way that was «grossly negligent». The Code comes into force on 28 May 2019, signatories have not yet been announced. Available at: https://appcrmsteeringgroup.uk/app-scams-steering-group-agrees-voluntary-code/.

[8] The Independent, «TSB becomes first bank to offer 'refund guarantee' to all fraud victims» (Ben Chapman, 16 April 2019). Available at: https://www.independent.co.uk/news/business/news/tsb-bank-fraud-guarantee-refund-scams-a8870781.html

[9] BBB Scam Tracker, reporting US and Canadian victim and potential victim accounts from 1 July 2015 to 22 April 2019. Available at: https://www.bbb.org/scamtracker/us/

[10] World Payments Report 2018, p6. Available at https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf

[11] The Financial Times, «UK has lost two-thirds of bank branches in 30 years» (Emma Agyemang, 16 November 2018). Available at: https://www.msn.com/en-gb/money/news/uk-has-lost-two-thirds-of-bank-branches-in-30-years/ar-BBPL1Z7

[12] The European Banking Federation, 2018 Facts & Figures (11 September 2018). Available at: https://www.ebf.eu/ebf-media-centre/banking-in-europe-ebf-publishes-2018-facts-figures/)

[13] The Wall Street Journal, «Thousands of Bank Branches are Closing, Just Not at These Banks» (Allison Prang, 15 June 2018). Available at: https://www.wsj.com/articles/the-bank-branch-is-dyingjust-not-at-these-banks-1529055000

[14] CNBC.com, «You think it's your friend calling, but it's actually this growing phone scam» (Annie Nova, 12 June 2018). Available at: https://www.cnbc.com/2018/06/12/you-think-its-your-friend-calling-but-its-actually-this-growing-phone-scam.html

[15] https://www.zdnet.com/article/cybercrime-market-selling-full-digital-fingerprints-of-over-60000-users/

kpmg.ua

KPMG та логотип KPMG є зареєстрованими торговими марками або товарними марками асоціації KPMG International.