Додаток 1.2
до Пропозиції

Веб-сайт/Інтернет-магазин/інше програмне забезпечення(далі разом – сайт) Клієнта(яке використовується Клієнтом), на якому розміщується Віртуальний платіжний термінал, протягом строку дії Договору відповідатиме наступним вимогам:

- всі внутрішні посилання сторінки сайту Клієнта повинні бути робочими і здатними до адекватної обробки інформації;

- через сайт Клієнт не повинен надавати послуги «розваг для дорослих», послуги знайомств («Adult Entertainment»);

- на сайті Клієнта не повинно бути посилань або банерів підозрілих Інтернет-сайтів (наприклад, сайтів для дорослих та інших, використання яких заборонено внутрішніми документами Платіжних систем та Законодавством, або якщо така інформація вводить в оману Споживача), а також посилань банерних мереж, у яких можуть спливати банери підозрілого змісту;

- сайт Клієнта не повинен розташовуватися на безкоштовних серверах, які надають послуги хостингу, а також на серверах, не рекомендованих НПП, банком-еквайром НПП. Сайт Клієнта має розміщуватися на інфраструктурі, що забезпечує належний рівень доступності, захисту, оновлення, резервування та реагування на вразливості відповідно до характеру Послуги (НПП може встановлювати документовані технічні критерії сумісності/безпеки, але не обмежує вибір провайдера лише переліком «рекомендованих» серверів без об'єктивної підстави);

- наявність на сайті Клієнта актуальної довідкової інформації про Клієнта, його місцезнаходження, адресу для кореспонденції (адреса не може бути до запитання), а також контактних номерів телефонів, за якими Споживач може зв'язатися зі службою підтримки Клієнта;

- на сайті Клієнта має бути зазначений опис споживчих характеристик Товарів, що реалізуються через сайт (серед іншого, не має містити недоліків, що можуть стати підставою для повернення платежу за Платежем), актуальні ціни на Товари, детальний опис процедур замовлення та доставки Товарів та їх оплати з використанням Карток(їх реквізитів), опис процедур повернення коштів, надання рівноцінних Товарів, обміну Товарів і т.п. у разі відмові від Товару, наявність відгуків щодо Клієнта, його Товарів тощо.

Для перевірки відповідності сайтів Клієнта вимогам безпеки, що об'єктивно пов'язані з прийманням Платежів, НПП або залучений ним ТО має право проводити погоджені неінвазивні перевірки публічно доступного периметра та/або отримувати документальні підтвердження відповідності. Перевірки проводяться в обсязі, необхідному для оцінки платіжного ризику, без отримання доступу до внутрішніх систем, облікових записів, персональних даних, вихідного коду, секретів/ключів або інформації третіх осіб, якщо інше окремо не погоджено Клієнтом або прямо не вимагається Законодавством:

1) Попереднє сканування сайтів Клієнта здійснюється до початку приймання Платежів як неінвазивна автоматизована перевірка погодженого публічного периметра. Критерії критичності вразливостей, порядок підтвердження результатів, усунення хибнопозитивних спрацювань та повторної перевірки визначаються документованою методикою НПП. Виявлення підтвердженої критичної/високої вразливості, що безпосередньо створює неприйнятний ризик для платіжної взаємодії, може бути підставою для відкладення підключення до її усунення або застосування погодженого компенсуючого заходу;

2) Перевірок сайтів Клієнта на відповідність вимогам, що можуть здійснюється протягом всього строку дії цього Договору, а саме:

- автоматизоване сканування сайтів Клієнта на предмет вразливостей та наявності шкідливого коду;

- перевірки на відповідність стандартам PCI DSS, правилам/політикам ПС та внутрішнім стандартам безпеки Платіжного провайдера, іншим вимогам;

- моніторингу використання заборонених або потенційно ризикованих сервісів (наприклад, анонімайзерів, нелегального контенту, прихованих редиректів тощо).

У зв'язку з цим, Клієнт гарантує, що:

- сайти Клієнта не будуть блокувати доступ інструментам автоматичного сканування Платіжного провайдера (в т.ч. але не виключно за допомогою CAPTCHA, обмеження геолокації або IP);

- сайти Клієнта будуть цілодобово доступними для перевірки Платіжного провайдера (в т.ч. у нічний час, вихідні та святкові дні);

- на вимогу НПП ним буде надається технічна інформація (наприклад, User-Agent або список IP-адрес) для включення у whitelist системи захисту сайтів Клієнта.

У разі невиконання Клієнтом, визначених обов'язків за цим пунктом Договору, НПП має право призупинити виконання обов'язків за Договором.

За платіжними операціями держателів, що здійснюються з використанням Картки(для надсилання коштів НПП), Клієнт зобов'язується:

- дотримуватися вимог установчих документів/правил ПС (VISA, Mastercard, НПС «Український платіжний простір та/або інших ПС за допомогою яких виконуються платіжні операції за цим Договором), а також їх програм, що стосуються випадків невідповідності вимогам певних стандартів, що діють в ПС та розміщені на офіційних веб-сайтах ПС;

- не допускати порушення правил ПС, що може мати наслідком негативний вплив на репутацію ПС, їх торговельних марок, продуктів та послуг, функціонування систем або діяльність їх учасників;

- дотримуватися вимог ПС, що стосуються платформи електронної комерції (маркетплейс);

- забезпечувати(в частині, що може застосовуватися до Клієнта) виконання вимог ПС щодо захисту інформації, пов'язаної з рахунками та/або інформацією про транзакції;

- забезпечити (в частині, що може застосовуватися до Клієнта) виконання програм ПС з моніторингу ризику, пов'язаного з якістю даних, у тому числі, зміна власного найменування, тощо, з метою оминути Програми ПС з питань моніторингу суперечливих питань (VDMP), Програми ПС з питань моніторингу випадків шахрайства (VFMP), чи Програму ПС із захисту бренда (Global Brand Protection Program);

- не здійснювати(не допускати здійснення) незаконні чи заборонені ПС та чинним законодавством України операції, у тому числі, що стосуються дитячої порнографії, каліцтва, насильства, незаконних азартних ігор, порушення прав інтелектуальної власності, контрабанди сигарет, потенційно оманливих практик маркетингу, незаконних посвідчувальних документів про особу державного зразка, тощо;

- не допускати дій, що свідчать про перешкоджання використанню або упереджене ставлення до Карток карткової ПС;

- прямо чи опосередковано не вимагати від будь-якого власника Картки здійснення додаткової доплати або будь-яких одноразових зборів у зв'язку з проведенням транзакції/платіжної операції;

- не вимагати здійснення мінімальної або максимальної суми транзакції/платіжної операції при використанні Карток карткової ПС;

- не встановлювати, як умову прийому Картки, щоб власник такої Картки відмовився від права оскаржувати транзакцію/платіжну операцію;

- не розголошувати даних про законного держателя Кратки особам, які не мають на це законного права або повноважень, і не дозволяти їм використовувати за призначенням Картку;

- не копіювати, не зберігати, не журналювати та не передавати реквізити Картки понад обсяг, прямо необхідний і погоджений для відповідної платіжної інтеграції; не допускати зберігання чутливих автентифікаційних даних після авторизації. Якщо архітектура інтеграції передбачає отримання або обробку Клієнтом даних Картки, така обробка допускається лише в погодженому обсязі та за умови виконання застосовних вимог PCI DSS/правил ПС і вимог захисту інформації. У разі моделі, за якою дані Картки вводяться безпосередньо в середовищі НПП/еквайра, Клієнт не повинен технічно отримувати повні реквізити Картки;

- не установлювати різні ціни на ті самі Товари в разі здійснення розрахунку за них у безготівковій формі порівняно з розрахунком готівковими коштами;

- не здійснювати будь-яку діяльність, яка згідно правил ПС може зашкодити фінансовій стабільності та/або репутації відповідної. ПС Перевіряти відповідність суми зазначеної в чеку реєстратора розрахункових операцій/ товарному чеку та суми;

- виконувати установлені вимоги з товарно-касового обліку при оформленні операцій з використанням Картки(її реквізитів);

- не допускати дроблення однієї операції на декілька операцій з метою уникнення процедури верифікації особи Споживача;

- протягом 5 (п'яти) робочих днів, на запит НПП (в тому числі, за результатами отриманого НПП запиту банка-еквайра/банка-емітента Картки), надавати завірені копії документів, які підтверджують

факт проведення операції з використанням Карток (їх реквізитів) у торгових точках Клієнта: копії чеків, копії документів товарно-касового обліку (чеків реєстраторів розрахункових операцій, записів з товарно-касової книги та інші необхідні документи по операціях, проведених на сайтах Клієнта) у відповідь на запит НПП;

- на запит НПП (в тому числі, за результатами отриманого НПП запиту банка-еквайра/банка-емітента) надавати необхідні документи, відомості та інші дані для ідентифікації Клієнта, визначення суті його діяльності та фінансового стану, з метою виконання вимог законодавства у сфері ПВК/ФТ (з можливістю подальшої передачі до банку-еквайра/банку-емітента);

- не надавати даних про держателя Картки не уповноваженим особам;

- негайно, але не пізніше наступного робочого дня повідомити НПП про зміну профіля/виду діяльності Клієнта;

- відповідати за надання недостовірної інформації про види своєї діяльності. Клієнту заборонено обмежувати права держателів Карток на оскарження операцій з оплати Товарів за допомогою Карток (їх реквізитів) шляхом прохання або вимоги до держателів відмовитись від прав на оскарження операцій;

- внести зміни до сайту(-ів) Клієнта з метою усунення порушень цього Договору та/або правил ПС протягом 3-х операційних днів від дати отримання повідомлення від НПП(або повідомлення банку-еквайра/ПС) про виявлене порушення та необхідність його усунення (внесення змін). Клієнт зобов'язаний відмовитися від здійснення платіжної операції з використанням Картки, у разі: 1) неможливості виконання авторизації у зв'язку з технічними причинами; 2) отримання негативного коду відповіді від емітента Картки; 3) інших випадків, установлених Договором або законодавством України.

Щодо інцидентів Клієнт зобов’язується:

Без невиправданої затримки Клієнт зобов’язаний негайно після виявлення повідомляти НПП про інцидент інформаційної безпеки, кіберінцидент, несанкціонований доступ, компрометацію або підозру на компрометацію API-ключів, токенів, сертифікатів, паролів, інших автентифікаційних чи облікових даних, втрату, незаконне розкриття, зміну або знищення персональних даних, платіжної, транзакційної чи іншої інформації з обмеженим доступом, зараження шкідливим програмним забезпеченням, а також про інший інцидент у інформаційних системах, сайта або інформаційно-комунікаційній інфраструктурі Клієнта, якщо такий інцидент впливає або обґрунтовано може вплинути на інформаційну взаємодію з НПП, безпеку Платежів, достовірність переданих НПП даних або безпеку інформації НПП чи Споживачів.

Первинне повідомлення має містити наявну на момент його направлення інформацію, достатню для визначення характеру інциденту, його можливого впливу на взаємодію Сторін та вжиття першочергових заходів реагування. Відсутність повної інформації про причини, масштаб або наслідки інциденту не є підставою для затримки первинного повідомлення. Клієнт надає НПП уточнену інформацію в міру її встановлення.

Клієнт зобов’язується в межах своєї компетенції та з урахуванням вимог Законодавства співпрацювати з НПП під час локалізації та усунення наслідків такого інциденту, у тому числі щодо припинення або обмеження скомпрометованих доступів, зміни/ротації ключів, токенів, паролів та інших автентифікаційних даних, перевірки цілісності інформаційної взаємодії, звіряння Платежів та безпечного відновлення взаємодії Сторін.

Обмін інформацією про інцидент здійснюється в обсязі, необхідному для реагування на нього та виконання Сторонами своїх обов’язків за Договором і Законодавством, без розкриття інформації третіх осіб або іншої інформації з обмеженим доступом понад обсяг, для якого наявна належна правова підстава.