

Оперативна Политика за Сигурност на Данните (DSOP)

Раздел 1	Въведение в DSOP и Стандарти за Защита	3
Раздел 2	Програма за Съответствие с PCI DSS (Важно Периодично Утвърждаване на Вашите Системи)	3
Действие 1:	Участие в Програмата за Съответствие на American Express по настоящата Политика	4
Действие 2:	Разбиране на Вашето Ниво на Търговец/Доставчик на Услуги и Изискванията за Документацията за Утвърждаване	4
Действие 3:	Попълване на Документацията за Утвърждаване, която трябва да изпратите на American Express	7
Действие 4:	Изпращане на Документацията за Утвърждаване до American Express	9
Раздел 3	Задължения за Управление на Инциденти с Данни	10
Раздел 4	Задължения за Обезщетение за Инцидент с Данни	12
Раздел 5	Програма за Целеви Анализ (Targeted Analysis Programme, TAP) ..	14
Раздел 6	Поверителност	15
Раздел 7	Отказ	16
Раздел 8	Терминологичен речник	16
Раздел 9	Полезни уебсайтове	20

DSOP Обобщение на Промените

Икони

Важните актуализации са изброени в таблицата „Обобщение на промените“ и също така са посочени в DSOP с правоъгълен маркер за промяна. Маркерът за промяна е вертикална лента, обикновено разположена в полето от ляво, която обозначава добавен или ревизиран текст. Само съществени промени в DSOP с потенциално въздействие върху оперативните процедури на Търговеца се отбелязват с маркер за промяна, както е показано в полето от ляво.



Премахнат текст се отбелязва с икона на кошче за отпадъци, разположена в полето до мястото, където се е намирал изтритият важен текст, включително раздели, таблици, параграфи, забележки и подточки. Изтритият текст се упоменава в таблицата „Обобщение на промените“, като, за да се избегне объркване, се използва номерацията на разделите от предишните публикации.

Параграфите, оградени със сини линии, показват специфична за отделните региони информация.

Обобщение на Таблица с Промени

Важните актуализации са изброени в следната таблица и също така са посочени в DSOP с правоъгълен маркер за промяна.

Раздел/Подраздел	Описание на Промяната
Няма промени за тази версия.	

Раздел 1

Въведение в DSOP и Стандарти за Защита

Като лидер в защитата на потребителите, American Express има дългосрочен ангажимент за защита на Данните на Картодържателя и Чувствителните Данни за Удостоверяване и се грижи за тяхната сигурност.

Компрометираните данни имат отрицателно въздействие върху потребителите, Търговците, Доставчиците на Услуги и издателите на карти. Дори един инцидент може сериозно да увреди репутацията на компанията и да наруши способността ефективно да извършва търговска дейност. Разглеждането на тази заплаха чрез прилагане на оперативни политики по сигурност може да помогне за подобряване на доверието на клиентите, увеличаване на печалбата и подобряване на репутацията на компанията.

В American Express знаем, че нашите Търговци и Доставчици на Услуги (колективно **Вие**) споделят нашата загриженост и изискваме, като част от Вашите отговорности, да спазвате разпоредбите за сигурност на данните във Вашето **Споразумение** за приемане (в случая на Търговци) или обработване (в случая на Доставчици на Услуги) на Картата American Express® (всяко наричано съответно Споразумението) и настоящата Оперативна Политика за Сигурност на Данните (DSOP), която можем да изменяме периодично. Тези изисквания се отнасят за цялото Ви оборудване, системи и мрежи (и техните компоненти), върху които Криптографските Ключове, Данните на Картодържателя или Чувствителните Данни за Удостоверяване (или комбинация от тях) са съхранени, обработени или предадени.

Използваните термини с главни букви, които не получават определение тук, носят смисъла, даден им в терминологичния речник в края на настоящата политика.

Оперативна Политика за Сигурност на Данните (DSOP) представлява набор от изчерпателни изисквания на политиката, предназначени да защитават Данните за Сметката, когато тези данни се съхраняват, обработват или предават.

American Express изисква от всички Търговци и Доставчици на Услуги да отговарят на Стандарта за Сигурност на Данните на Индустрията за Разплащане с Платежни Карти (PCI DSS). Като част от тези изисквания, Вие трябва, и също така трябва да накарате Вашите Обхванати Страни, да:

- съхраняват Данните на Картодържателя само с цел улесняване на Трансакциите с Карти American Express в съответствие с и съгласно изискванията на настоящото Споразумение.
- отговарят на актуалната версия на Стандарта за Сигурност на Данните на Индустрията за Разплащане с Платежни Карти (Payment Card Industry Data Security Standard, PCI DSS) и други изисквания на Съвета за Стандарти за Сигурност на Индустрията за Разплащане с Платежни Карти (Payment Card Industry Security Standards Council, PCI SSC), приложими за Вашето обработване, съхраняване или предаване на Криптографски Ключове, Данни на Картодържателя или Чувствителни Данни за Удостоверяване не по-късно от датата на влизане в сила на версията на въпросното приложимо изискване.
- да се уверите, че при внедряването или подмяната на технология за обработване, съхраняване или предаване на данни се използват продукти, одобрени от PCI.

Вие трябва да защитавате всички Записи за плащания с American Express и Кредитните записи, съхранявани съгласно Споразумението, в съответствие с настоящите разпоредби за сигурността на данните; Вие трябва да използвате тези записи само за целите на Споразумението и да им осигурявате съответната защита. Вие носите финансова и друга отговорност пред American Express за осигуряване спазването от страна на Вашите Обхванати Страни на настоящите разпоредби за сигурност на данните (освен за демонстриране на съответствието на Вашите Обхванати страни с тази политика съгласно [Раздел 2, „Програма за Съответствие с PCI DSS \(Важно Периодично Утвърждаване на Вашите Системи\)“](#), освен ако не е предвидено друго в този раздел). Подробности относно стандартите на PCI и как да бъде постигнато съответствие с изискванията им може да бъдат намерени на www.pcisecuritystandards.org.

Раздел 2

Програма за Съответствие с PCI DSS (Важно Периодично Утвърждаване на Вашите Системи)

Трябва да предприемате следните действия за утвърждаване по Стандарта PCI DSS ежегодно и на всеки 90 дни, както е описано по-долу, на състоянието на оборудването, системите и/или мрежите си (и техните компоненти) и

тези на Вашите Франчайзополучатели, върху които се съхраняват, обработват или предават Данни на Картодържателя или Чувствителни Данни за Удостоверяване.

За завършване на утвърждаването са необходими четири действия:

- [Действие 1](#): Участие в PCI Програмата за съответствие на American Express по настоящата Политика.
- [Действие 2](#): Разбиране на Вашето Ниво на Търговец/Доставчик на Услуги и Изискванията за Документацията за Утвърждаване.
- [Действие 3](#): Попълване на Документацията за Утвърждаване, която трябва да изпратите на American Express.
- [Действие 4](#): Изпращане на Документацията за Утвърждаване до American Express в рамките на предвидените срокове.

Действие 1: Участие в Програмата за Съответствие на American Express по настоящата Политика

Търговци Ниво 1, Търговци Ниво 2 и всички Доставчици на услуги, както са описани по-долу, трябва да участват в Програмата по настоящата политика. American Express може да изиска, по наша преценка, конкретни Търговци Ниво 3 и Ниво 4 да участват в Програмата по настоящата политика.

Търговците и Доставчиците на услуги, които са длъжни да участват в Програмата, трябва да се запишат в [Портала](#), предоставен от избрания от American Express Програмен Администратор, в рамките на предвидените срокове.

- Вие трябва да приемете всички разумни условия, свързани с използването на Портала.
- Вие трябва да определите и предоставите точна информация за поне един контакт за сигурност на данните в рамките на Портала. Задължителната информация включва:
 - пълно име
 - адрес на електронна поща
 - телефонен номер
 - физически пощенски адрес
- Трябва да предоставите актуализирана или нова информация за връзка с посочения контакт за сигурност на данните в рамките на Портала в случай на промяна на информацията.
- Трябва да се уверите, че Вашите системи са актуализирани и позволяват комуникации по обслужването от съответния домейн на Портала.

Ако не успеете да предоставите или поддържате текуща информация за контакт за сигурност на данните или да способствате комуникация по електронна поща, това няма да повлияе на нашите права за оценяване на таксите.

Действие 2: Разбиране на Вашето Ниво на Търговец/Доставчик на Услуги и Изискванията за Документацията за Утвърждаване

Има четири Нива на Търговец, които важат за Търговците, и две Нива, които важат за Доставчиците на Услуги, базирани на Вашия обем транзакции с карта American Express.

- За Търговците, това е обемът, предоставен от техните Предприятия, който достига до най-високото ниво на American Express за сметка на Търговец.*
- За Доставчиците на Услуги, това е сумата от обемите, предоставена от Доставчика на Услуги и Доставчика на Услуги за Юридически лица, на когото предоставяте услуги.

Трансакциите с инициирани от купувача плащания (Buyer Initiated Payments, BIP) не са включени в обема на Трансакциите с Карта American Express при определянето на Нивото на Търговец и изискванията за утвърждаване. Ще попаднете в едно от Нивата на Търговец, посочени в [Таблица А-1: Нива на Търговци и Доставчици на Услуги](#).

* За Франчайзодатели, това включва обем от Предприятията на техните Франчайзополучатели. Франчайзодателите, които възлагат на своите Франчайзополучатели да използват определена система „Място на Продажба“ (Point of Sale, POS) или Доставчик на Услуги, също трябва да предоставят Документация за утвърждаване на засегнатите Франчайзополучатели.

Таблица А-1: Нива на Търговци и Доставчици на Услуги

Ниво на Търговец	Трансакции с American Express Годишно
Търговец Ниво 1	2,5 милиона Трансакции с Карта American Express или повече на година; или Търговец, когото American Express иначе поставя на Ниво 1 по своя преценка.
Търговец Ниво 2	50 000 до по-малко от 2,5 милиона Трансакции с Карта American Express годишно.
Търговец Ниво 3	10 000 до по-малко от 50 000 Трансакции с Карта American Express годишно.
Търговец Ниво 4	По-малко от 10 000 Трансакции с Карта American Express годишно.
Ниво на Доставчик на Услуги	Трансакции с American Express Годишно
Доставчик на Услуги Ниво 1	2,5 милиона Трансакции с Карта American Express или повече на година; или Доставчик на Услуги, когото American Express поставя на Ниво 1 по друг начин.
Доставчик на Услуги Ниво 2	по-малко от 2,5 милиона Трансакции с карта American Express годишно; или всеки Доставчик на услуги, който не е поставен на Ниво 1 от American Express.

Изисквания за Утвърждаване на Документация към Търговеца

Търговците (които не са Доставчици на Услуги) разполагат с четири възможни категории Нива на Търговец. След определяне на Нивото на търговеца от [Таблица А-1: Нива на Търговци и Доставчици на Услуги](#) (по-горе), вижте [Таблица А-2: Документация за Утвърждаване на Търговец](#), за да определите изискванията за документацията за утвърждаване.

Таблица А-2: Документация за Утвърждаване на Търговец

Ниво на Търговец/ Трансакции с American Express Годишно	Доклад за съответствие Удостоверява не на съответствие (ROC AOC)	Въпросник за самооценка Удостоверяване на съответствие (SAQ AOC) и Тримесечно Сканиране за Уязвимост (Scan) на външната мрежа	Програма за Подобряване на Технологиите за Сигурност (STEP) Удостоверяван е за отговарящи на критериите Търговци
Ниво 1/ 2,5 милиона или повече	Задължителен	Неприложимо	По избор с одобрение от American Express (замества ROC)
Ниво 2/ 50 000 до по-малко от 2,5 милиона	По избор	SAQ AOC задължителен (освен когато се подава ROC AOC); задължително сканиране с определени видове SAQ	По избор с одобрение от American Express* (замества SAQ и сканиране на мрежата или ROC)
Ниво 3**/ 10 000 до по-малко от 50 000	По избор	SAQ AOC по избор (задължително, ако се изисква от American Express); задължително сканиране с определени видове SAQ	По избор с одобрение от American Express* (замества SAQ и сканиране на мрежата или ROC)
Ниво 4**/ по-малко от 10 000	По избор	SAQ AOC по избор (задължително, ако се изисква от American Express); задължително сканиране с определени видове SAQ	По избор с одобрение от American Express* (замества SAQ и сканиране на мрежата или ROC)

* **Забележка:** PCI екипът на American Express ще разгледа искането и съответствието с условията и ще потвърди, ако отговаряте на изискванията за Програмата STEP. Моля, свържете се с Вашия мениджър на клиенти и/или пишете на AXPPCIComplianceProgram@aexp.com, за да проверите дали отговаряте на изискванията.

** С цел избягване на съмнения, Търговците Ниво 3 и Ниво 4 не трябва да представят Документация за утвърждаване, освен ако такава не се изисква по преценка на American Express, но въпреки това трябва да спазват всички други разпоредби на настоящата Оперативна Политика за Сигурност на Данните и подлежат на отговорност съгласно тях.

American Express си запазва правото да проверява пълнотата, точността и целесъобразността на Вашата Документация за утвърждаване по Стандарта PCI. American Express може да изиска от Вас да предоставите допълнителни поддържащи документи за оценка в подкрепа на тази цел. Освен това American Express има право да изиска от Вас да ангажирате одобрен от Съвета за Стандарти за Сигурност на PCI Квалифициран Оценител по Сигурността (QSA) или Съдебен Експерт от Индустрията за Разплащане с Платежни Карти (PFI).

Изисквания за Документацията за Утвърждаване към Доставчика на Услуги

Доставчиците на Услуги (които не са Търговци) имат две възможни категории Нива. След определяне на Нивото на Доставчика на Услуги от [Таблица А-1: Нива на Търговци и Доставчици на Услуги](#) (по-горе), вижте [Таблица А-3: Документация за Утвърждаване на Доставчик на Услуги](#), за да определите изискванията за документацията за утвърждаване.

Доставчиците на Услуги не отговарят на критериите за участие в STEP.

Таблица А-3: Документация за Утвърждаване на Доставчик на Услуги

Ниво	Документация за Утвърждаване	Изискване
1	Годишен Доклад за Съответствие Удостоверяване на Съответствие (ROC AOC)	Задължителен
2	Годишен Въпросник за Самооценка SAQ Г (Доставчици на Услуги) и Сканиране на Мрежата на Тримесечие или Годишен Доклад за Съответствие Удостоверяване на Съответствие (ROC AOC), ако се предпочита	Задължителен

Препоръчва се Доставчиците на Услуги да спазват и Допълнителното Утвърждаване на PCI за Определени Юридически лица.

Програма за Подобряване на Технологиите за Сигурност (STEP)

Търговците, които спазват Стандарта PCI DSS, могат по преценка на American Express да изпълнят изискванията на STEP (Security Technology Enhancement Programme) на American Express, ако внедряват определени допълнителни технологии за сигурност в своите среди за обработка на Карти. STEP се прилага само ако Търговецът не е имал Инцидент с Данни през предходните 12 месеца и ако 75% от всички Трансакции с карти на Търговеца се извършват чрез използването на комбинация от следните подобрени опции за сигурност:

- **Стандарт EMV, EMV Безконтактни карти или Дигитален портфейл** – на активно Устройство с Активиран Чип, притежаващо валидно и актуално одобрение/сертифициране от EMVCo (www.emvco.com) и в състояние да обработва съвместими Трансакции с Чип Карти по Спецификацията на American Express за разплащане с карти с вграден микрочип (AEIPS). (Търговците от САЩ трябва да включват Безконтактни карти)
- **Криптиране от Точка до Точка (P2PE)** – съобщено на обработващия лични данни на Търговеца чрез одобрена от PCI SSC или одобрена от QSA система за Криптиране от Точка до Точка
- **Токенизирани** – приложените решения за токенизация трябва да:
 - отговарят на спецификациите на EMVCo,
 - бъдат осигурени, обработени, съхранени, пренесени и изцяло управлявани от доставчик на услуги за трети страни, съответстващ на изискванията на PCI, и
 - Токенът не може да бъде обърнат, за да разкрие на Търговеца немаскирани Основни номера на сметки (PANs).

За Търговците, отговарящи на изискванията на STEP, важат облекчени изисквания във връзка с Документацията за Утвърждаване на PCI, както е описано по-подробно в [Действие 3: „Попълване на Документацията за Утвърждаване, която трябва да изпратите на American Express“](#) по-долу.

Действие 3: Попълване на Документацията за Утвърждаване, която трябва да изпратите на American Express

Следните документи са необходими за различните нива на Търговци и Доставчици на Услуги, както са изброени в [Таблица А-2: Документация за Утвърждаване на Търговец](#) и [Таблица А-3: Документация за Утвърждаване на Доставчик на Услуги](#) по-горе.

Трябва да осигурите Удостоверяване на Съответствие (AOC) за приложимия вид оценяване. AOC е декларация за Вашия статус на съответствие и като такава трябва да бъде подписана и датирана от съответното мениджърско ниво във Вашата организация.

Освен AOC American Express може да изиска от Вас да предоставите копие от пълната оценка и, по Ваша преценка, допълнителни поддържащи документи, които показват съответствие с изискванията на PCI DSS. Тази Документация за Утвърждаване се попълва на Ваши разноски.

Доклад за Съответствие Удостоверяване на Съответствие (ROC AOC) - (Годишно изискване) – Докладът за Съответствие документираща резултатите от подробен преглед на място на Вашето оборудване, системи и мрежи (и техните компоненти), където Данните на Картодържателя или Чувствителните Данни за Удостоверяване (или и двете) се съхраняват, обработват или предават. Има два варианта: един за Търговците и друг, за Доставчиците на Услуги. Докладът за Съответствие трябва да бъде изготвен от:

- от QSA, или
- Вътрешен оценител по сигурността (ISA) и сертифициран от Вашия главен изпълнителен директор, главен финансов директор, главен служител по сигурността на информацията или възложител

ROC AOC трябва да бъде подписано и датирано от QSA или ISA и оторизираното ниво на мениджмънт във Вашата организация и предоставено на American Express най-малко веднъж годишно.

Въпросник за Самооценка Удостоверяване на Съответствие (SAQ AOC) - (Годишно изискване) – Въпросниците за Самооценка позволяват самостоятелна проверка на оборудването, системите и мрежите (и техните компоненти), върху които Данните на Картодържателя или Чувствителните Данни за Удостоверяване (или и двете) се съхраняват, обработват или предават. Има различни версии на SAQ. Вие ще изберете една или повече в зависимост от Вашата Среда за Данни на Картодържателя.

SAQ може да бъде попълнен от служител във Вашата Компания, който е квалифициран да отговаря на въпроси точно и пълно, като Вие може да ангажирате QSA, който да предостави помощ. SAQ AOC трябва да бъде подписано и датирано от оторизираното ниво на мениджмънт във Вашата организация и предоставено на American Express най-малко веднъж годишно.

Резюме на Одобрен Доставчик на Сканиране за Сканиране за уязвимост на външните мрежи (ASV Scan) - (Изискване на 90 дни) – Външното сканиране за уязвимост е дистанционен тест, който помага да бъдат открити потенциални слабости, уязвимости и грешни конфигурации на свързани с интернет елементи от Вашата Среда за Данни на Картодържателя (напр. уебсайтове, приложения, мрежови сървъри, сървъри за електронна поща, публични домейни или хостове).

ASV Scan трябва да се изготви от Одобрен Доставчик на Сканиране (Approved Scanning Vendor, ASV).

Ако се изисква от SAQ, Докладът за Сканиране от Одобрен Доставчик на Сканиране Удостоверяване на Съответствие на Сканирането (AOSC) или резюме, съдържащо броя на сканираните цели, сертификация, че резултатите задоволяват процедурите по сканиране на PCI DSS и статус на съответствие, попълнен от ASV, трябва да бъдат предоставени на American Express най-малко веднъж на всеки 90 дни.

Ако предоставяте ROC AOC или STEP, не е необходимо да осигуряват резюме на AOSC или Сканиране от ASV, освен ако не се изисква изрично. С цел избягване на съмнения Сканиранията са задължителни, ако се изискват съгласно приложимия SAQ.

Документация за Утвърждаване на Удостоверяването по STEP (STEP) - (Годишно изискване) – STEP е достъпно само за Търговци, които отговарят на критериите, изброени в [Действие 2: „Разбиране на Вашето Ниво на Търговец/Доставчик на Услуги и Изискванията за Документацията за Утвърждаване“](#) по-горе. Ако Вашата компания отговаря на критериите, трябва да попълвате и подавате формуляра за Удостоверяване по STEP веднъж годишно на American Express. Формулярът за Годишно Удостоверяване по STEP е наличен за изтегляне от [Портала](#). Освен това можете да се свържете с Вашия мениджър на клиенти или да пишете на American Express на AXPPCIComplianceProgram@aexp.com.

Несъответствие със Стандарта PCI DSS - (Годишно, 90 дни и/или Ad Hoc изискване) – Ако не отговаряте на Стандарта PCI DSS, трябва да подадете Приоритизиран Обобщен Инструмент на PCI (PAT) (наличен за изтегляне от уебсайта на Съвета за стандарти за сигурност на PCI).

В Обобщения PAT трябва да се посочва дата за отстраняване на несъответствието, която не може да бъде по-късно от дванадесет (12) месеца след датата на попълване на документа, с цел постигане на съответствие. Вие трябва да предоставяте на American Express периодични актуализации за напредъка си по отношение на отстраняването на

несъответствието във връзка с Вашия статус на Несъответствие (Търговци Ниво 1, Ниво 2, Ниво 3 и Ниво 4; всички Доставчици на Услуги). Действията по отстраняване на несъответствието, необходими за постигане на съответствие с PCI DSS, следва да бъдат извършени на Ваши разноски.

American Express няма да налага такси за несъответствие преди датата на отстраняване на несъответствието. Според [Таблица А-4: Такса за Несъответствие](#), Вие оставате отговорни пред American Express за всички задължения за обезщетение за Инцидент с Данни и подлежите на всички други разпоредби на тази политика.

American Express, по своя преценка, си запазва правото да налага такси за несъответствие, ако:

- не е бил подаден Приоритизиран Образец на PCI в съответствие с изискванията, посочени в този раздел,
- стъпките по отстраняване на несъответствието, посочени в Приоритизирания Образец на PCI за Статус на Несъответствие, не са изпълнени,
- някое от изискванията на Приоритизирания Образец на PCI за Статус на Несъответствие не е изпълнено, или
- задължителната документация за съответствие не е предоставена на American Express в приложимия срок или при поискване.

Търговци/Доставчици на Услуги, които не отговарят на изискванията, посочени в [Действие 2: „Разбиране на Вашето Ниво на Търговец/Доставчик на Услуги и Изискванията за Документацията за Утвърждаване“](#), може да подлежат на такси, както е посочено в [Действие 4: Изпращане на Документацията за Утвърждаване до American Express](#).

С цел избягване на всякакви съмнения Търговците, които не отговарят на Стандарта PCI DSS, не отговарят на условията за STEP.

Действие 4: Изпращане на Документацията за Утвърждаване до American Express

Всички Търговци и Доставчици на Услуги, от които се изисква да участват в Програмата, трябва да подадат Документацията за Утвърждаване, отбелязана като „задължителна“ в таблиците в [Действие 2: „Разбиране на Вашето Ниво на Търговец/Доставчик на Услуги и Изискванията за Документацията за Утвърждаване“](#) на American Express в съответствие с приложимите срокове.

Трябва да предоставите Вашата Документация за Утвърждаване на American Express, като използвате Портала, който е предоставен от изборния от American Express Програмен Администратор. С предоставянето на Документацията за Утвърждаване Вие представлявате и гарантирате пред American Express, че следното е истина (доколкото е във Вашите възможности):

- Вашата оценка е пълна и изчерпателна;
- Статусът по Стандарта PCI DSS е отразен точно в момента на изпълнение, независимо дали чрез предаване на Удостоверяване на съответствие (АОС) или Приоритизиран Обобщен Инструмент на PCI (PAT) за несъответствие;
- Вие сте упълномощени да съобщите информацията, която се съдържа там, и предоставяте Документацията за Утвърждаване на American Express, без да нарушавате правата на други страни.

Такси за Несъответствие и Прекратяване на Споразумението

American Express има право да Ви налага такси за несъответствие и да прекрати Споразумението, ако не изпълните настоящите изисквания или не предоставите задължителната Документация за Утвърждаване на American Express до изтичане на крайния срок. American Express ще се опита да уведоми контакта за сигурност на данните за приложимия краен срок за всеки годишен и тримесечен отчетен период.

Таблица А-4: Такса за Несъответствие

Описание*	Търговец Ниво 1 или Доставчик на Услуги Ниво 1	Търговец Ниво 2 или Доставчик на услуги Ниво 2	Търговец Ниво 3 или Ниво 4
Таксата за несъответствие ще бъде разгледана, ако Документацията за Утвърждаване не бъде получена до първия краен срок.	25 000 щ.д.	5000 щ.д.	50 щ.д.
Допълнителна такса за несъответствие ще бъде разгледана, ако Документацията за Утвърждаване не бъде получена до втория краен срок.	35 000 щ.д.	10 000 щ.д.	100 щ.д.
Допълнителна такса за несъответствие ще бъде разгледана, ако Документацията за Утвърждаване не бъде получена до втория краен срок. ЗАБЕЛЕЖКА: Таксите за несъответствие ще продължат да бъдат прилагани, докато Документацията за Утвърждаване бъде предоставена.	45 000 щ.д.	15 000 щ.д.	250 щ.д.

* Таксите за несъответствие ще бъдат оценявани в Еквиваленти на Местната Валута.

** Не е приложимо в Аржентина.

Ако Вашите задължения за Документацията за съответствие по PCI DSS не са изпълнени, American Express има правото да налага кумулативно такси за несъответствие, да задържа плащания и/или да прекрати Споразумението.

Раздел 3

Задължения за Управление на Инциденти с Данни

Трябва да уведомите American Express незабавно и в никакъв случай не по-късно от седемдесет и два (72) часа след откриването на Инцидент с Данни.

За да уведомите American Express, моля, свържете се с Програмата за реагиране при инциденти на American Express (EIRP) безплатно на 1.888.732.3750 или на 1.602.537.3021 или изпратете имейл на EIRP@aexp.com. Трябва да посочите лице като свой контакт по отношение на такъв Инцидент с Данни. Освен това:

- Трябва да извършите задълбочено разследване на всеки Инцидент с Данни и незабавно да предоставите на American Express всички Компрометирани Картови Номера. American Express си запазва правото да извърши собствен вътрешен анализ, за да идентифицира данните, включени в Инцидента с Данни.

При Инциденти с Данни, засягащи по-малко от 10 000 уникални Картови Номера, на American Express трябва да бъде предоставено обобщение на разследването в рамките на десет (10) работни дни след приключването му.

- Обобщението на разследването трябва да включва следната информация: обобщение на инцидента, описание на засегнатата/-ите среда/-и, време на протичане на събитието, основни дати, въздействие и подробности за

изложеността на данни, действия за ограничаване и отстраняване и удостоверение, че няма индикации, че и други данни на American Express са изложени на риск.

При Инциденти с Данни, засягащи 10 000 или повече уникални Картови Номера, Вие трябва да ангажирате PCI PFI, който да проведе това разследване в рамките на пет (5) дни след установяване на Инцидент с Данни.

- Нередактираният доклад от съдебното разследване трябва да бъде предоставен на American Express в рамките на десет (10) работни дни след приключването му.
- Докладите от съдебните разследвания трябва да се изготвят чрез настоящия Образец за Окончателен Доклад във връзка със Съдебно Разследване на Инциденти, който може да се намери от PCI. В доклада на PFI трябва да се включват съдебни прегледи, доклади за съответствие и всякаква друга информация, свързана с Инцидента с Данни, да се определя причината за Инцидента с Данни, да се потвърждава дали сте спазвали Стандарта PCI DSS по време на Инцидента с Данни и да се потвърждава Вашата способност да предотвратявате бъдещи Инциденти с Данни, като (i) предоставите план за отстраняване на всички недостатъци във връзка със Стандарта PCI DSS и (ii) участвате в програмата за съответствие на American Express (както е описано по-долу). По искане на American Express трябва да предоставите утвърждаване от Квалифициран Оценител по Сигурността (Qualified Security Assessor, QSA), че недостатъците са отстранени.

Независимо от предходните параграфи на [Раздел 3, „Задължения за Управление на Инциденти с Данни“](#):

- American Express може, изцяло по свое усмотрение, да изиска от Вас да ангажирате PFI да извърши разследване на Инцидент с Данни за Инциденти с Данни, включващи по-малко от 10 000 уникални Картови Номера, или ако са се случили няколко инцидента в рамките на последните 12 месеца. Всяко такова разследване трябва да отговаря на изискванията, изложени по-горе в [Раздел 3, „Задължения за Управление на Инциденти с Данни“](#) и трябва да бъде завършено в рамките на срока, изискван от American Express.
- American Express може изцяло по свое усмотрение да ангажира отделно PFI за провеждане на разследване за всеки Инцидент с Данни и може да прехвърли разходите за такова разследване на Вас.

Трябва да оцените Инцидента с Данни съгласно приложимите закони за уведомяване при нарушаване на данни в глобален план и, когато е нужно, да уведомите съответните регулаторни органи и засегнатите Картови членове в съответствие със законите за уведомяване при нарушаване на данни. Ако сте определили, че Вашият Доставчик на Услуги или друго юридическо лице носи отговорност за докладването на Инцидент с Данни, трябва да уведомите въпросния Доставчик на Услуги или друго юридическо лице, че е длъжно да оцени своите задължения за докладване съгласно приложимото законодателство за уведомяване при нарушаване на данни. Вие се съгласявате да получите писмено одобрение от American Express преди да правите отправка или да споменавате American Express при всякаква форма на комуникация с Картовите членове относно Инцидента с Данни. Вие се съгласявате да сътрудничите на American Express за предоставянето на подробности и коригирането на всякакви проблеми, произтичащи от Инцидента с Данни, включително предоставянето (и осигуряване на всички условия, необходими за предоставянето) на American Express на всичката свързана информация с цел потвърждаване на способността Ви да предотвратите бъдещи Инциденти с Данни по начин, отговарящ на Споразумението.

Независимо от всяко противоположно задължение за поверителност в Споразумението, American Express има право да разкрие информация за всеки Инцидент с Данни на Картовите членове на American Express, Издателите, другите участници в Мрежата на American Express и широката общественост според изискванията на Приложимото право; чрез съдебна, административна или регулаторна заповед, указ, призовка, искане или друг процес, за да се намали рискът от измама или друга вреда, или по друг начин, доколкото това е в обхвата, уместен за работата на мрежата на American Express.

Какво да направите, ако имате Инцидент с Данни?

Моля, следвайте тези стъпки, ако сте установили Инцидент с Данни във Вашия бизнес.

**Стъпка 1:**

Попълнете [Формуляр за Първоначално Уведомяване за Инцидент с Търговски Данни](#) и изпратете имейл на EIRP@aexp.com в рамките на 72 часа след установяването на Инцидента с Данни.

**Стъпка 2:**

Проведете подробно разследване. Това би могло да изисква наемане на [Съдебен Експерт от Индустрията за разплащане с платежни карти \(PCI\)](#).

**Стъпка 3:**

Своевременно ни предоставете всички компрометирани Картови номера на American Express®.

**Стъпка 4:**

Съдействайте ни, за да ни помогнете да разрешим всички проблеми, произтичащи от Инцидента с Данни.

Вижте [Раздел 3, „Задължения за Управление на Инциденти с Данни“](#) за повече подробности относно Задълженията за Управление на Инциденти с Данни.

Имате още въпроси?

САЩ: (888) 732-3750 (безплатно)

Международен: +1 (602) 537-3021

EIRP@aexp.com

Раздел 4

Задължения за Обезщетение за Инцидент с Данни

Вашите задължения за обезщетение към American Express съгласно Споразумението за Инциденти с Данни се определят съгласно настоящия [Раздел 4, „Задължения за Обезщетение за Инцидент с Данни“](#). В допълнение към Вашите задължения за обезщетение (ако има такива), може да сте длъжни да заплатите такса за несъответствие при Инцидент с Данни, както е описано по-долу в настоящия [Раздел 4, „Задължения за Обезщетение за Инцидент с Данни“](#).

Вие ще компенсирате American Express в размер на 5 щ.д. за всеки номер на сметка за Инциденти с Данни, които включват:

- 10 000 или повече Картови Номера на American Express с някое от следните:
 - Чувствителни Данни за Удостоверяване, или
 - Дата на Изтичане

Въпреки това, American Express няма да търси обезщетение от Вас за Инцидент с Данни, който включва:

- по-малко от 10 000 Картови Номера на American Express, или
- повече от 10 000 Картови Номера на American Express, ако отговаряте на следните условия:
 - уведомили сте American Express за Инцидента с Данни съгласно [Раздел 3, „Задължения за Управление на Инциденти с Данни“](#),
 - по време на Инцидента с Данни сте били в съответствие със Стандарта PCI DSS (както е определено от разследването на Инцидента с Данни на PFI), и
 - Инцидентът с Данни не е причинен от Вашето неправомерно поведение или това на Вашите Обхванати Страни.

Независимо от предходните параграфи на настоящия [Раздел 4. „Задължения за Обезщетение за Инцидент с Данни“](#), за всеки Инцидент с Данни, независимо от броя Картови Номера на American Express, Вие ще заплатите на American Express такса за несъответствие, която да не надвишава 100 000 щ.д. на Инцидент с Данни (както е определено от American Express изцяло по нейно усмотрение) в случай, че не спазите някое от задълженията си, изложени в [Раздел 3. „Задължения за Управление на Инциденти с Данни“](#). За избягване на съмнения, общата такса за несъответствие при Инцидент с Данни за който и да било отделен Инцидент с Данни няма да надвишава 100 000 щ.д.

American Express ще изключи от изчислението си всеки Номер на Картова Сметка в American Express, който е участвал в иск за обезщетение по предходен Инцидент с Данни, отправен в рамките на дванадесет (12) месеца преди Датата на Уведомлението. Всички изчисления, направени от American Express по тази методология, са окончателни.

American Express може да Ви таксува за пълния размер на задълженията Ви за обезщетение за Инциденти с Данни или да приспадне сумата от плащанията на American Express към Вас (или съответно да дебитиран банковата Ви сметка) съгласно Споразумението.

Вашите задълженията за обезщетение за Инциденти с Данни по тази политика не се считат за случайни, косвени, спекулативни, последващи, специални, наказателни или примерни вреди по Споразумението, при условие че такива задължения не включват вреди, свързани с или в естеството на пропуснати печалби или приходи, загуба на репутация или загуба на бизнес възможности.

Изцяло по собствена преценка American Express може да намали задължението за обезщетение за Търговци само при Инциденти с Данни, които отговарят на всеки от следните критерии:

- Приложимите Технологии за Намалване на Риска са използвани преди Инцидента с Данни и са използвани по време на Целия Прозорец на Инцидент с Данни,
- извършено е задълбочено проучване в съответствие с програмата на Съдебния експерт от PFI (освен ако по-рано не е уговорено друго в писмена форма),
- от съдебния доклад ясно личи, че при обработката, съхранението и/или предаването на данните по време на Инцидента с Данни, са използвани Технологиите за Намалване на Риска, и
- не съхранявате (и не сте съхранявали по време на Прозореца на Инцидент с Данни) Чувствителни Данни за Удостоверяване или каквито и да било Данни на Картодържатели, които не са станали нечетими.

Когато е възможно намаляване на обезщетението, намаляването на Вашето задължение за обезщетение (с изключение на дължимите такси за несъответствие) се определя, както следва:

Таблица А-5: Критерии за Намалване на Задължението за Обезщетение

Намаляване на Задължението за Обезщетение	Задължителни Критерии
Стандартно Намалване: 50%	>75% от общите Трансакции се обработват на Устройства с Активиран Чип ¹ ИЛИ Технология за Намалване на Риска се използва при >75% от обектите на Търговеца ²
Значително Намалване: 75% до 100%	>75% от всички Трансакции се обработват на Устройства с Активиран Чип ¹ И друга Технология за Намалване на Риска се използва при >75% от обектите на Търговеца ²

1 Както е определено от вътрешния анализ на American Express

2 Както е определено от разследването на PFI

- Значителното Намалване (от 75% до 100%) се определя въз основа на по-ниския процент на Трансакциите, извършени чрез Устройства с Активиран Чип, И на Търговските обекти, използващи друга Технология за Намалване на Риска. Примерите в [Таблица А-6: Значително Намалване на Задължението за Обезщетение](#) илюстрират изчисляването на намаляването на обезщетението.

- За да се приеме дадена технология за Технология за Намаляване на Риска, трябва да демонстрирате ефективното ѝ използване в съответствие с нейните дизайн и предназначение.
- Процентът на Вашите обекти, в които се използва Технология за Намаляване на Риска, се установява от разследването на PFI.
- Намалението на задължението за обезщетение не се прилага за такси за несъответствие, дължими във връзка с Инцидента с Данни.

Таблица А-6: Значително Намаляване на Задължението за Обезщетение

Пример	Използвани Технологии за Намаляване на Риска	Отговаря на критериите	Намаляване
1	80% от Трансакциите са на Устройства с Активиран Чип 0% от обектите използват друга Технология за Намаляване на Риска	Не	50%: Стандартно Намаление (използването на под 75% Технология за Намаляване на Риска не отговаря на изискванията за Значително Намаляване) ¹
2	80% от Трансакциите са на Устройства с Активиран Чип 77% от обектите използват друга Технология за Намаляване на Риска	Да	77%: Значително Намаляване (въз основа на 77% използване на Технологии за Намаляване на Риска)
3	93% от Трансакциите са на Устройства с Активиран Чип 100% от обектите използват друга Технология за Намаляване на Риска	Да	93%: Значително Намаляване (въз основа на 93% използване на Устройства с Активиран Чип за Трансакции)
4	40% от Трансакциите са на Устройства с Активиран Чип 90% от обектите използват друга Технология за Намаляване на Риска	Не	50%: Стандартно Намаляване (когато под 75% от Трансакциите са на Устройства с Активиран Чип, не се класират за Значително Намаляване)

¹ Инцидент с Данни, при който са засегнати 10 000 сметки на карти American Express, при ставка от 5,00 щ.д. на номер на сметка (10 000 x 5 щ.д. = 50 000 щ.д.), може да отговаря на условията за намаление от 50%, което би намалило Задълженията за Обезщетение от 50 000 щ.д. на 25 000 щ.д., като тук не се включват таксите за несъответствие.

Раздел 5

Програма за Целеви Анализ (Targeted Analysis Programme, TAP)

Компрометирането на данни на картодържателя може да се дължи на пропуски в защитата на данни във вашата Среда за Данни на Картодържателя (Cardholder Data Environment, CDE).

Примери за компрометиране на Данни на Картодържатели включват, но не се ограничават до:

- **Обща Точка на Закупуване (Common Point of Purchase, CPP):** Картовите членове на American Express съобщават за измамни Трансакции по техните Картови сметки, за които е идентифицирано и установено, че произхождат от Покупки във Вашите Предприятия.
- **Намерени Данни за Карти:** Данни за Карти и Картодържатели на American Express, намерени в интернет, свързани с Трансакции във Вашите Предприятия.
- **Подозирани злонамерен софтуер:** American Express подозира, че използвате софтуер, заразен или уязвим за злонамерен код.

TAP е проектирана да идентифицира потенциални компрометирания на данни на Картодържателя.

Вие трябва да накарате вашите Обхванати Страни да спазват следните изисквания при уведомяване от American Express за потенциално компрометиране на данни на Картодържателя.

- Трябва бързо да прегледате своята CDE за пропуски в сигурността на данните и да коригирате всички евентуални находки.
 - Вие трябва да се погрижите Вашите доставчици трети страни да проведат щателно разследване на Вашата CDE, ако го възложите на външни изпълнители.
- Трябва да предоставите обобщение на предприетите или планираните от Вас действия за преглед, оценка и/или коригиране след уведомление от American Express.
- Трябва да предоставите актуализирани документи за утвърждаване по PCI DSS в съответствие с [Раздел 2, „Програма за Съответствие с PCI DSS \(Важно Периодично Утвърждаване на Вашите Системи\)“](#).
- Когато е приложимо, трябва да ангажирате квалифициран PCI PFI, за да прегледа вашия CDE, ако вие или вашата Обхваната Страна:
 - Не можете да разрешите компрометирането на данните на Картодържателя в разумен период от време, определен от American Express, или
 - Потвърдите, че е възникнал Инцидент с Данни и спазвате изискванията, изложени в [Раздел 3, „Задължения за Управление на Инциденти с Данни“](#).

Таблица A-7: Такса за Неспазване на TAP

Описание	Търговец Ниво 1 или Доставчик на Услуги Ниво 1	Търговец Ниво 2 или Доставчик на услуги Ниво 2	Търговец Ниво 3 или Ниво 4
Таксата за неспазване може да бъде оценена, когато задълженията в TAP не са изпълнени до изтичане на първия краен срок.	25 000 щ.д.	5000 щ.д.	1000 щ.д.
Таксата за неспазване може да бъде оценена, когато задълженията в TAP не са изпълнени до изтичане на втория краен срок.	35 000 щ.д.	10 000 щ.д.	2500 щ.д.
Таксата за неспазване може да бъде оценена, когато задълженията в TAP не са изпълнени до изтичане на третия краен срок. ЗАБЕЛЕЖКА: Таксите за неспазване могат да продължат да се прилагат до изпълнение на задълженията или спазване на TAP.	45 000 щ.д.	15 000 щ.д.	5000 щ.д.

Ако задълженията в TAP не се спазват, American Express има правото да налага такси за неспазване кумулативно, да задържа плащания и/или да прекрати Споразумението.

Раздел 6

Поверителност

American Express предприема разумни мерки, за съхранението (и кара своите агенти и подизпълнители, включително Доставчика на Портала, да съхраняват) на Вашите доклади за съответствие, включително Документацията за Утвърждаване, и неразкриването на Документацията за Утвърждаване на трети страни (освен на Свързани лица, агенти, представители, Доставчици на Услуги и подизпълнители на American Express) за период от три години от датата на получаване, с изключение на това, че задължението за поверителност не се прилага за Документация за Утвърждаване, която:

- вече е известна на American Express преди разкриването;
- е или става достъпна за обществеността, без да нарушава този параграф от American Express;
- е правомерно получена от трета страна от American Express без задължение за поверителност;
- е независимо разработена от American Express; или
- се изисква да бъде оповестена по заповед на съд, административна агенция или държавен орган, или по закон, правило или регламент, или чрез призовка, искане за документи от съда, призоваване или друг административен или правен процес, или чрез всяко официално или неофициално изследване или

разследване от която и да е държавна агенция и който и да е орган (включително всеки регулатор, инспектор, проверител или правоприлагаща агенция).

Раздел 7

Отказ

С НАСТОЯЩОТО AMERICAN EXPRESS СЕ ОТКАЗВА ОТ ВСЯКО И ВСИЧКИ ПРЕДСТАВИТЕЛСТВА, ГАРАНЦИИ И ЗАДЪЛЖЕНИЯ ПО ОТНОШЕНИЕ НА ОПЕРАТИВНАТА ПОЛИТИКА ЗА СИГУРНОСТ НА ДАННИТЕ, СТАНДАРТА PCI DSS, СПЕЦИФИКАЦИИТЕ ЗА EMV И ОПРЕДЕЛЯНЕТО И ИЗПЪЛНЕНИЕТО НА QSA, ASV ИЛИ PFI (ИЛИ НЯКОЙ ОТ ТЯХ), НЕЗАВИСИМО ДАЛИ ИЗРИЧНИ, МЪЛЧАЛИВИ, ЗАКОНОВИ, ИЛИ ДРУГИ, ВКЛЮЧИТЕЛНО ТЪРГОВСКА ГАРАНЦИЯ ИЛИ ГОДНОСТ ЗА ОПРЕДЕЛЕНА ЦЕЛ. ИЗДАТЕЛИТЕ НА КАРТИ AMERICAN EXPRESS НЕ СА ТРЕТИ ЛИЦА БЕНЕФИЦИЕРИ ПО НАСТОЯЩАТА ПОЛИТИКА.

Раздел 8

Терминологичен речник

Само за целите на настоящата *Оперативна Политика за Сигурност на Данните* се прилагат следните определения:

Чувствителни Данни за Удостоверяване означава свързана със сигурността информация, която се използва за удостоверяване на картодържателите и/или за удостоверяване на трансакции с платежни карти. Тази информация включва, но не се ограничава до кодове за верифициране на карти, full track данни (от магнитни ленти или еквивалент на чип), PIN-ове и PIN блокове.

Въпросник за Самооценка (SAQ) означава инструмент за самооценка, създаден от Payment Card Industry Security Standards Council, LLC, предназначен за оценяване и удостоверяване на спазването на Стандарта PCI DSS.

Данни за Сметка включват Данни на Картодържателя и/или чувствителните данни за удостоверяване. Виж Данни на Картодържателя и Чувствителни Данни за Удостоверяване.

Данни за Трансакция означава цялата информация, изисквана от American Express, която доказва една или повече Трансакции, включително и информация, получена в точката на продажба, информация, получена или генерирана по време на Удостоверяване и Предаване, и всяко Обратно плащане.

Данни на Картодържателя означава като минимум само пълният Основен Номер на Сметка (PAN) или пълният PAN плюс някои от следните данни: име на картодържател, дата на изтичане и/или сервизен код. Виж Чувствителни Данни за Удостоверяване за допълнителни данни, които биха могли да бъдат предадени или обработени (но не и съхранени) като част от платежна трансакция.

Данни на Картодържател имат значението, дадено им в актуалния към момента на публикуване Терминологичен Речник за Стандарта PCI DSS.

Дата на Уведомяване означава датата, на която American Express предоставя на издателите окончателно уведомление за Инцидент с Данни. Тази дата зависи от получаването от страна на American Express на окончателния съдебен доклад или от вътрешния анализ и се определя по преценка на American Express.

Документация за Утвърждаване означава AOC, означава AOC, представено във връзка с Годишния Доклад за Оценка на Сигурността на Място или SAQ, AOSC и резюмето на констатациите, направени във връзка с Тримесечните Сканирания на Мрежата или Удостоверяването на Годишната Програмата за Подобряване на Технологиите за Сигурност.

Доставчици на Услуги означава упълномощени обработващи лични данни, обработващи лични данни на трети страни, доставчици на шлюзове, интегратори на POS Системи и всички други доставчици на Търговци на POS Системи или други решения или услуги за обработка на плащания.

Доставчик на Услуги Ниво 1 означава Доставчик на Услуги с 2,5 милиона Трансакции с Карта American Express или повече на година; или Доставчик на Услуги, когото American Express поставя на Ниво 1 по друг начин.

Доставчик на Услуги Ниво 2 означава Доставчик на Услуги с по-малко от 2,5 милиона Трансакции с Карта American Express годишно; или всеки Доставчик на Услуги, който не е поставен на Ниво 1 от American Express.

Запис на Плащане означава възпроизводим (на хартия и в електронен вид) запис на Плащане, който отговаря на нашите изисквания и съдържа Номер на Карта, дата на Трансакция, сума в долари, Одобрение, подпис на Картовия член (ако е приложимо) и друга информация.

Издател на Карта Издател означава всяко Юридическо лице (включително American Express и неговите Свързани лица), лицензирано от American Express или Свързано лице на American Express да издава Картите и да участва в бизнеса за издаване на Картите.

Изисквания за Сигурност на PIN в PCI означава Изискванията за Сигурност на PIN в индустрията за разплащане с платежни карти, които са достъпни на www.pcisecuritystandards.org.

Изисквания на Стандарта за Сигурност на Данните за Разплащане с Платежни Картите (PCI SSC) означава набора от стандарти и изисквания, свързани с обезопасяването и защитата на данни за платежни карти, включително PCI DSS и PA DSS, достъпен на адрес: www.pcisecuritystandards.org.

Информация за Картовия член означава информация за Картовия член на American Express и Трансакции с Картите, включително имена, адреси, номера на картови сметки и идентификационни номера на карти (Card Identification, CID).

Инцидент с Данни означава инцидент, включващ компрометиране или предполагаемо компрометиране на криптографски ключове на American Express или поне един номер на Картова сметка в American Express, при който има:

- неоторизиран достъп или използване на Криптографски Ключове, Данни на Картодържатели или Чувствителни Данни за Удостоверяване (или комбинация от тях), които се съхраняват, обработват или предават на Вашето оборудване, системи и/или мрежи (или на техни компоненти) или ползването на които Вие сте възложили, предоставили или сте направили достъпни;
- използване на Криптографски ключове, Данни на Картодържатели или Чувствителни Данни за Удостоверяване (или комбинация от тях), различни от тези в Споразумението; и/или
- предполагаема или потвърдена загуба, кражба или незаконно присвояване чрез каквито и да било носители, материали, записи или информация, съдържащи такива Криптографски Ключове, Данни на Картодържатели или Чувствителни Данни за Удостоверяване (или комбинация от тях).

Карта American Express или **Карта** означава всяка карта, устройство за достъп до сметка или устройство за плащане или услуга, съдържащо име, лого, търговска марка, марка на услуга, търговско наименование или друг конструктивен дизайн или наименование на American Express или свързано лице собственик и издадено от издател или номер на картова сметка.

Картов член означава физическо или юридическо лице, (i) което е сключило споразумение за създаване на Картова сметка при издател, или (ii) чието име е посочено върху картата.

Картодържател означава клиент, на когото е издадена платежна карта, или всяко физическо лице, упълномощено да използва платежната карта.

Квалифициран Оценител по Сигурността (QSA) означава юридическо лице, което е квалифицирано от Payment Card Industry Security Standards Council, LLC да потвърждава спазването на Стандарта PCI DSS.

Компрометиран Картов Номер означава номер на картова сметка в American Express, свързана с Инцидент с Данни.

Кредит означава сумата на Плащанията, която възстановявате на Картовите членове за покупки или плащания, направени по Картата.

Кредитен Запис означава запис на Кредит, който отговаря на нашите изисквания.

Криптиране от Точка до Точка (P2PE) означава решение, което криптографски защитава данните за профила от точката, в която търговецът приема платежната карта до защитената точка на декриптиране.

Криптографски Ключ (Криптографски ключ на American Express) означава всички ключове, използвани при обработката, генерирането, зареждането и/или защитата на Данни за Сметка. Това включва, но не е ограничено до следното:

- Основни Криптографски Ключове: Зонални Главни Ключове (Zone Master Key, ZMK) и Зонални Пин Ключове (Zone Pin Keys, ZPK)
- Главни Ключове, използвани в сигурни криптографски устройства: Местни Главни Ключове (Local Master Key, LMK)

- Ключове за Код за Безопасност на Картата (Card Security Code Key, CSCK)
- PIN ключове: Базови Ключове за Отклонение (Base Derivation Key, BDK), Ключ за Криптиране на PIN код (PIN Encryption Key, PEK) и ZPK

Ниво на Търговец е определението, което даваме на Търговците в съответствие с техните задължения за утвърждаване в съответствие с PCI DSS, както са описани в [Раздел 2, „Програма за Съответствие с PCI DSS \(Важно Периодично Утвърждаване на Вашите Системи\)“](#).

Номер на Картата означава уникалния идентификационен номер, който издателят дава на Картата, когато тя бива издадена.

Обработващ лични данни означава доставчик на услуги за търговци, който улеснява обработката на разрешения и подаване на обработването в мрежата на American Express.

Образец за Окончателен Доклад във връзка със Съдебно Разследване на Инциденти означава образецът, предоставен от Съвета за стандарти за сигурност на PCI, който е наличен на www.pcisecuritystandards.org.

Одобрен Доставчик на Сканиране (ASV) означава Юридическо Лице, което е квалифицирано от Payment Card Industry Security Standards Council, LLC да утвърждава спазването на определени изисквания на Стандарта PCI DSS чрез извършване на сканиране на уязвимостта на интернет среди.

Одобрено Решение за Криптиране от Точка до Точка (P2PE), включено в списъка на Стандарта PCI DSS на утвърдени решения или утвърдено от Квалифицирана Компания-Оценител по Сигурността на P2PE.

Обхванати Страни означава всички Ваши служители, агенти, представители, подизпълнители, Обработващи лица, Доставчици на Услуги, доставчици на Вашето оборудване за място на продажба (POS) или системи или решения за обработка на плащания, Юридически лица, свързани с Вашата сметка като Търговец на American Express, както и всяка друга страна, на която можете да предоставите достъп до Данни на Картодържателя или Чувствителни данни за Удостоверяване (или и двете) в съответствие със Споразумението.

Основен номер на сметка (PAN) има значението, посочено в актуалния към момента Терминологичен речник за PCI DSS.

Порталът означава системата за отчитане, предоставена от изборния от American Express Програмен Администратор на Програмата на PCI. Търговците и Доставчиците на услуги са задължени да използват Портала, за да предоставят на American Express документация за утвърждаване на Стандарта PCI.

Потребител се дефинира като картодържател, закупуващ стоки, услуги или и двете.

Приложение за Плащане има значението, дадено му в актуалния към момента на публикация Терминологичен Речник за Стандарта за Сигурност на софтуера и стандарта за сигурност на жизнения цикъл на софтуера, който е достъпен на www.pcisecuritystandards.org.

Програмата означава Програмата за съответствие със Стандарта PCI на American Express.

Програмата за подобряване на технологиите за сигурност (STEP) означава програмата на American Express, в която Търговците се насърчават да внедряват технологии, които подобряват сигурността на данните.

Програмата за Целеви Анализ означава програма, която осигурява ранно идентифициране на потенциално компрометиране на данни на Картодържателя във вашата Среда за Данни на Картодържателя (CDE). Вижте [Раздел 5, „Програма за Целеви Анализ \(Targeted Analysis Programme, TAP\)“](#).

Прозорец на Инцидент с Данни означава периодът на намеса (или определен по подобен начин период от време), посочен в последния окончателен доклад (напр. доклад на PFI), или, в случай че не е известен, до 365 дни преди последната Дата на уведомяване за потенциално Компрометирани картови номера, включени в Компрометиране на данни, докладвани на нас.

Разход означава плащане или покупка, направени по Карта.

PCI DSS означава Стандарт за Сигурност на Данните за Разплащане с Платежни Карти, който е достъпен на адрес: www.pcisecuritystandards.org.

Система на Мястото на Продажба (POS) означава система за обработка на информация или оборудване, включително терминал, персонален компютър, електронен касов апарат, безконтактен четец или платежен механизъм или процес, използван от Търговец, за получаване на разрешения или за събиране на Данни за трансакции или и двете.

Спецификации на EMV означава спецификациите, издадени от EMVCo, LLC, които са достъпни на www.emvco.com.

Споразумение означава Общите разпоредби, Регулациите за Търговци и всички съпътстващи допълнения и приложения, взети заедно (често наричано Споразумение за Приемане на Карта в нашите материали).

Среда за Данни на Картодържателя (CDE) означава хората, процесите и технологията, която съхранява, обработва или предава данни на картодържателя или чувствителни данни за удостоверяване.

Стандартът за Сигурност на Данните за Разплащане с Платежни Карти (PCI DSS) означава Стандарта за Сигурност на Данните за Разплащане с Платежни Карти на адрес www.pcisecuritystandards.org.

Съдебен експерт от индустрията за разплащане с платежни карти (PFI) означава юридическо лице, което е одобрено от PCI Security Standards Council, LLC за извършване на съдебни разследвания на нарушение или компрометиране на Данни за платежни Карти.

Технологии за Намаляване на Риска означават технологични решения, които подобряват сигурността на Данните на Картодържателя на American Express и Чувствителните Данни за Удостоверяване, както е определено от American Express. За да се приеме дадена технология за Технология за Намаляване на Риска, трябва да демонстрирате ефективното използване в съответствие с нейните дизайн и предназначение. Примерите включват, но не се ограничават до: EMV, криптиране от Точка до Точка и токенизация.

Токен означава криптографският токен, който заменя PAN, базиран на даден индекс за непредсказуема стойност.

Трансакциите с Инициирани от Купувача Плащания (BIP) означава дигитално платежно решение, което позволява на купувачите бързо и ефективно да насрочват плащания към доставчици (свързани с корпоративни карти).

Трансакция означава Плащане, Кредит, Теглене на пари в брой (или друг вид достъп до парични средства), или Трансакция на банкомат, извършена чрез Карта.

Трансакция с EMV означава Трансакция с карта с вграден микрочип (наричана понякога „IC карта“, „чип карта“, „смарт карта“, „EMV карта“ или „ICC“), извършена на POS терминал с карта с вграден микрочип с валидно и актуално типово одобрение на EMV. Типовите одобрения на EMV са достъпни на адрес www.emvco.com.

Търговец означава Търговеца и всички негови свързани лица, които приемат Карти American Express по силата на Споразумение с American Express или нейните свързани лица.

Търговец Ниво 1 означава Търговец с 2,5 милиона Трансакции с Карта American Express или повече на година; или Търговец, когото American Express поставя на Ниво 1 по друг начин.

Търговец Ниво 2 означава Търговец с 50 000 до по-малко от 2,5 милиона Трансакции с Карта American Express годишно.

Търговец Ниво 3 означава Търговец с 10 000 до по-малко от 50 000 Трансакции с Карта American Express годишно.

Търговец Ниво 4 означава Търговец с по-малко от 10 000 Трансакции с Карта American Express годишно.

Удостоверяване на Съответствието (AOC) означава декларацията относно Вашето (не)съответствие със Стандарта PCI DSS във формата, предоставена от PCI Security Standards Council, LLC.

Удостоверяване на съответствието на сканиране (AOSC) означава декларацията относно Вашето (не)съответствие със Стандарта PCI DSS във формата, предоставена от PCI Security Standards Council, LLC.

Устройство за Въвеждане на PIN има значението, дадено му в актуалния към момента на публикация Терминологичен Речник за точката на взаимодействие (Point of Interaction, POI), посочена в Изискванията за Сигурността на Трансакции с PIN (PIN Transaction Security, PTS) на Индустрията за Разплащане с Платежни Карти и Модулните изисквания за сигурност, които са достъпни на www.pcisecuritystandards.org.

Устройство, Одобрено от PCI, означава, че устройство за въвеждане на PIN или Приложение за Плащане (или и двете) се появяват по време на внедряване в списъка на одобрените компании и доставчици, поддържани от PCI Security Standards Council, LLC, който е достъпен на www.pcisecuritystandards.org.

Устройство с Активиран Чип означава устройство за продажба на място, притежаващо валидно и актуално одобрение/сертифициране от EMVCo (www.emvco.com) и в състояние да обработва съвместим Трансакции с чип карти по Спецификацията на American Express за разплащане с карти с вграден микрочип (AEIPS).

Франчайзодател означава оператор на дружество, което лицензира лица или Юридически лица (Франчайзополучатели) да разпространяват стоки и/или услуги с Марката на оператора и/или да осъществяват дейност с нея; да осигуряват помощ на Франчайзополучателите при осъществяване на дейността им или да повлияят върху начина на работа на Франчайзополучателя; и да изискват заплащане на такса от Франчайзополучателите.

Франчайзополучател означава независимо притежавано и управлявано трето лице (включително франчайзополучател, лицензополучател или клон) освен Свързано лице, което е лицензирано от Франчайзодател да управлява франчайз и което е сключило писмено споразумение с Франчайзодателя, с което последователно показва външна идентификация, която ясно се идентифицира с Марките на Франчайзодателя или се показва пред обществеността като член на групата от дружества на Франчайзодателя.

Чип означава интегриран микрочип, вграден в Карта, съдържащ информация за Картовия член и сметката.

Чип Карта означава Карта, която съдържа Чип и може да изисква PIN като средство за проверка на самоличността на Картовия член или информацията за сметката, съдържаща се в Чипа, или и двете (понякога наричана „смайт карта“, „Карта EMV“ или „ICC“ или „карта с вграден микрочип“ в нашите материали).

Чувствителните Данни за Удостоверяване означава свързана със сигурността информация, която се използва за удостоверяване на картодържателите и/или за удостоверяване на трансакции с платежни карти. Тази информация включва, но не се ограничава до кодове за верифициране на карти, full track данни (от магнитни ленти или еквивалент на чип), PIN-ове и PIN блокове.

Раздел 9

Полезни уебсайтове

Сигурност на Данните на American Express: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

EMVCo: www.emvco.com