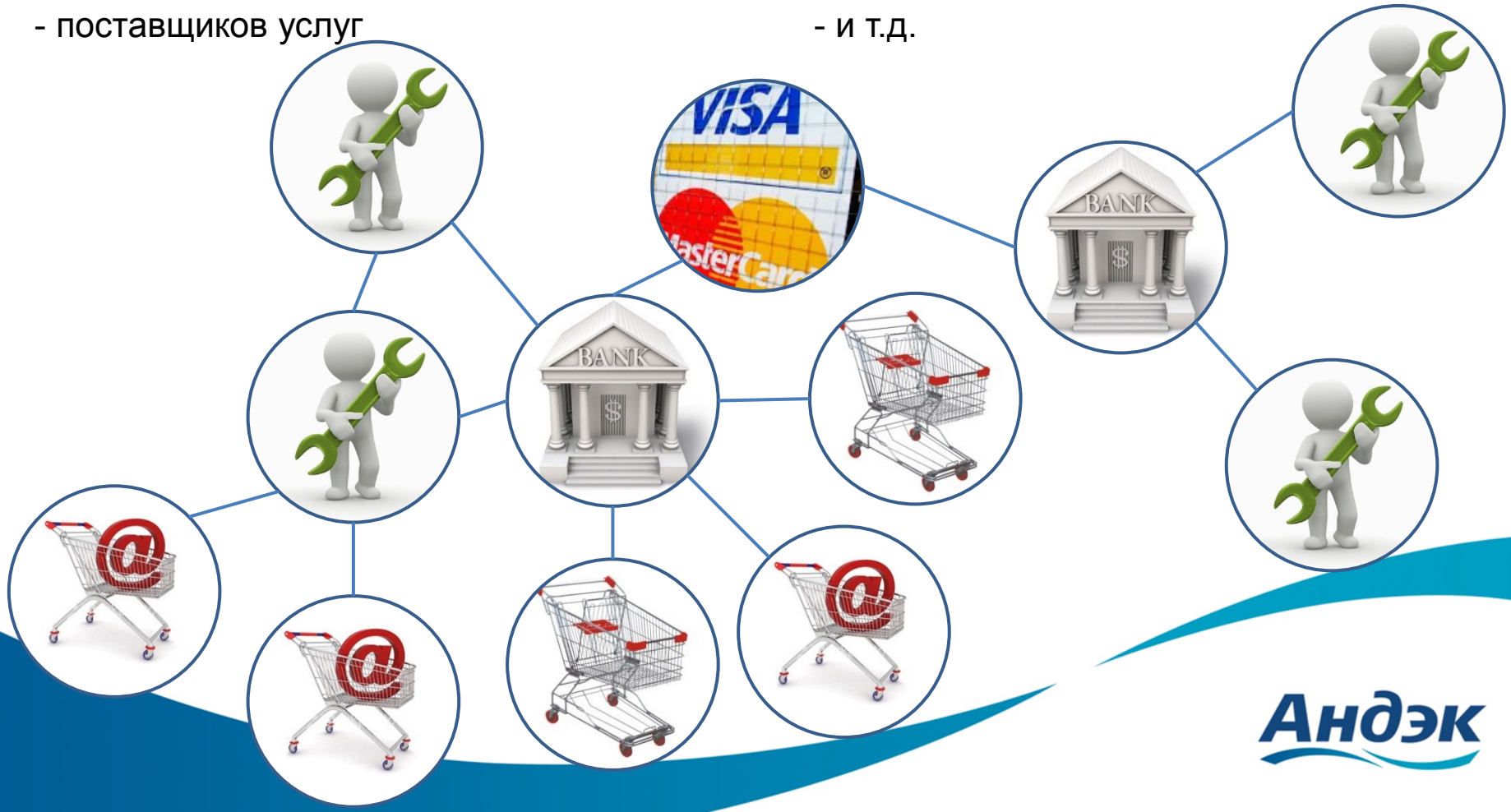

# Особенности взаимодействия организаций в рамках программы соответствия PCI DSS

Вячеслав Максимов
ЗАО «Андэк»
Заместитель генерального директора

# Напоминание №1: о применимости PCI DSS

PCI DSS применим **ко всем организациям**, вовлеченным в процессы обработки данных платежных карт, включая:

- торгово-сервисные предприятия
- процессинговые центры
- поставщиков услуг
- банки эквайеры
- банки эмитенты
- и т.д.




Андэк

# Напоминание №2: о регулировании в PCI

**PCI Security Standards Council:**

- Разрабатывает и совершенствует PCI DSS и прочие стандарты безопасности индустрии платежных карт
- Проводит обучение по стандартам безопасности
- Авторизует организации на проведение проверок по стандартам
- Контроль и надзор за деятельностью организаций, авторизованных советом на проведение проверок по стандартам

**МПС (VISA, MasterCard, Discover, American Express, JCB)**

- Устанавливают программы соответствия требованиям стандартов безопасности индустрии платежных карт для организаций, осуществляющих обработку данных платежных карт их бренда
- Определяют штрафные санкции для организаций, не соответствующих требованиям стандартов
- Определяют требования по реагированию на инциденты, связанные с компрометацией данных платежных карт

Андэк

# Напоминание №2: о регулировании в PCI

Члены МПС, торгово-сервисные предприятия, сервис-провайдеры и их агенты должны формально подтвердить соответствие требованиям по защите данных платежных карт.

- VISA: *http://www.visacemea.com/ac/ais/data_security.jsp*
- MasterCard: *http://www.mastercard.com/sdp*
- American Express: *http://www.americanexpress.com/datasecurity*
- Discover Network: *http://www.discovernetwork.com/fraudsecurity/disc.html*
- JCB: *http://partner.jcbcard.com/security/jcbprogram/index.html*

Андэк

# Напоминание №3: о контроле за соответствием торгово-сервисных предприятий

- ✓ Ответственность за соблюдение ТСП требований PCI DSS несет банк эквайер
- ✓ Разные МПС устанавливают разные уровни ТСП
- ✓ Для разных уровней ТСП - разные требования по отчетности о соответствии

**> 6 млн транзакций или была допущена компрометация ДПК**

- Ежегодно: QSA-аудит (AOC)
- Ежеквартально: ASV-сканирование

**< 6 млн транзакций в год**

- Ежегодно: Самооценка (SAQ)
- Ежеквартально: ASV-сканирование

Андэк

# Напоминание №4: PCI P2PE

**Приложения и решения PCI P2PE:**

- ✓ Обеспечивают надежное шифрование ДПК при их передаче от POI в процессинг
- ✓ Позволяют управлять криптографическими ключами
- ✓ Позволяют существенно сократить область аудита PCI DSS для торгово-сервисных предприятий

Полный список сертифицированных решений и приложений публикуется на официальном сайте PCI SSC:

- ➢ *https://www.pcisecuritystandards.org/approved_companies_providers/validated_p2pe_solutions.php*
- ➢ *https://www.pcisecuritystandards.org/approved_companies_providers/validated_p2pe_applications.php*

**По состоянию на 27.05.2014:**

- ✓ Сертифицированных решений PCI P2PE – **3 (три)**
- ✓ Сертифицированных приложений PCI P2PE – **3 (три)**

Андэк

# Взаимодействие с сервис-провайдерами

**PCI DSS 2.0 – Требование 12.8**

Если привлекаемые сервис-провайдеры способны повлиять на безопасность ДПК, компания должна обеспечить:

- ✓ Ведение списка таких сервис-провайдеров
- ✓ Письменное принятие сервис-провайдерами ответственности за безопасность ДПК
- ✓ Проверку сервис-провайдеров перед их привлечением
- ✓ Контроль статуса соответствия сервис-провайдеров требованиям PCI DSS

Самая распространенная реализация:

- ✓ Attestation of Compliance, подписанный QSA
- ✓ Шаблонные фразы в типовом договоре, например:
  - *«Услуги оказываются в соответствии с требованиями PCI DSS»*
  - *«Поставщик Услуг обеспечивает конфиденциальность обрабатываемой информации»*
  - *«все операции выполняются только по письменным заявкам Клиента»*

Андэк

**Part 2 PCI DSS Assessment Information**

**Part 2a. Services Provided that WERE INCLUDED in the Scope of the PCI DSS Assessment (check all that apply)**

| | | |
|---|---|---|
| ☐ Payment Processing-POS | ☐ Tax/Government Payments | ☐ Fraud and Chargeback Services |
| ☐ Payment Processing-Internet | ☐ Payment Processing – ATM | ☐ Payment Processing – MOTO |
| ☐ Issuer Processing | ☐ Payment Gateway/Switch | ☐ Clearing and Settlement |
| ☐ Account Management | ☐ 3-D Secure Hosting Provider | ☐ Loyalty Programs |
| ☐ Back Office Services | ☐ Prepaid Services | ☐ Merchant Services |

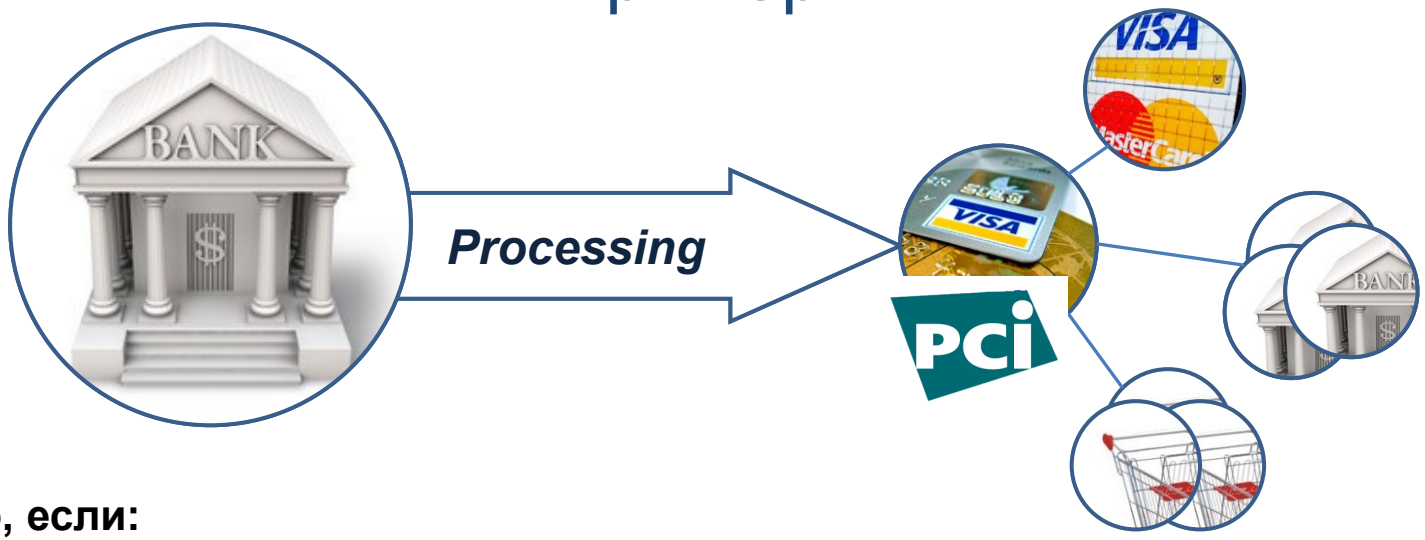
**Выбор QSA?**

**Compliance?**

**Security?**

**А ЕСЛИ ЭТО ВЫЯСНИЛОСЬ В ХОДЕ АУДИТА?**

# Пример №2




**Но что, если:**

- ✓ Процессинг расположен на территории Головной Организации, и не управляет мерами физической безопасности?
- ✓ Процессинг расположен в сети Головной Организации, и не управляет сетевым оборудованием?

**Кто для кого сервис-провайдер?**

**Удастся ли Процессингу диктовать условия Головной Организации?**

**Как убедить Головную Организацию пройти аудит?**

**А ЕСЛИ ЭТО ВЫЯСНИЛОСЬ В ХОДЕ АУДИТА?**

Андэк

## Part 2. Executive Summary

| Name of Service Assessed: | | | | |
|---|---|---|---|---|
| PCI DSS Requirement | Details of Requirements Assessed | | | |
| | Full | Partial | None | Justification for Approach (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.) |
| Requirement 1: | ☐ | ☐ | ☐ | |
| Requirement 2: | ☐ | ☐ | ☐ | |
| Requirement 3: | ☐ | ☐ | ☐ | |
| Requirement 4: | ☐ | ☐ | ☐ | |
| Requirement 5: | ☐ | ☐ | ☐ | |
| Requirement 6: | ☐ | ☐ | ☐ | |
| Requirement 7: | ☐ | ☐ | ☐ | |
| Requirement 8: | ☐ | ☐ | ☐ | |
| Requirement 9: | ☐ | ☐ | ☐ | |
| Requirement 10: | ☐ | ☐ | ☐ | |
| Requirement 11: | ☐ | ☐ | ☐ | |
| Requirement 12: | ☐ | ☐ | ☐ | |
| Appendix A: | ☐ | ☐ | ☐ | |

*If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

# Что это означает?

**Значительное снижение неопределенности в распределении ответственности между сервис-провайдерами и их клиентами:**

Для сервис-провайдеров

Для существующих клиентов сервис-провайдеров

Для потенциальных клиентов сервис-провайдеров

Для QSA-аудиторов

Для международных платежных систем

# Снова пример №1

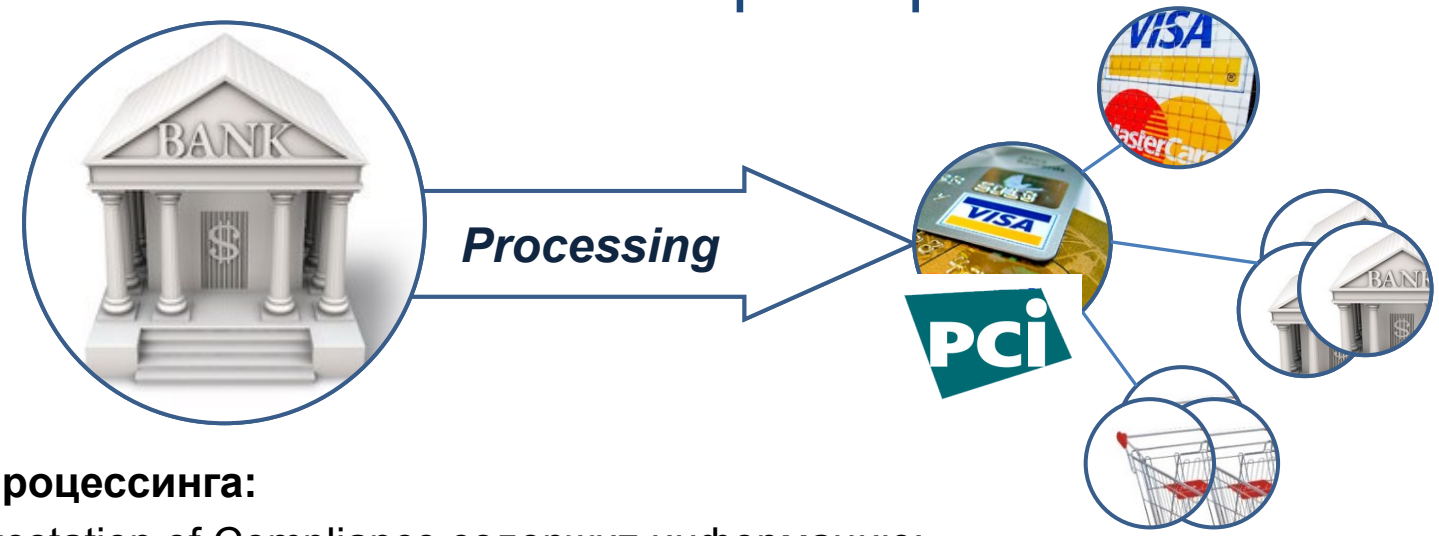

**Четко идентифицирует:**

- ✓ **какие услуги были проверены в ходе QSA-аудита**
- ✓ **какие требования PCI DSS были подтверждены для каждого проверенного сервиса**

**Уже включает необходимый текст**
***(требование 12.9 PCI DSS 3.0)***

Андэк

# Снова пример №2




**Для Процессинга:**

- ✓ Attestation of Compliance содержит информацию:
  - о перечне проверенных сервисов
  - о перечне неприменимых требований
- ✓ Дополнительные аргументы: Требование 12.9 PCI DSS 3.0 – объективный повод для пересмотра договора

**Повышение рисков для Головной Организации**

*Выход:*

- ➢ *передача всей ответственности Процессингу, ИЛИ*
- ➢ *запуск собственной программы соответствия PCI DSS*

# Заключение

**Переход на PCI DSS 3.0 потребует:**

- ✓ определить перечень требований, исполнение которых отдано на аутсорсинг
- ✓ пересмотреть договорные отношения со своими клиентами
- ✓ пересмотреть договорные отношения со своими поставщиками услуг

**Время есть:**

- ✓ PCI DSS 2.0 актуален до **31 декабря 2014 года**
- ✓ Требование 12.9 PCI DSS 3.0 обязательно с **1 июля 2015 года**

**ДИАЛОГ НУЖНО НАЧИНАТЬ УЖЕ СЕЙЧАС!**

Андэк

# ВОПРОСЫ?

Вячеслав Максимов
Заместитель генерального директора ЗАО «Андэк»
по направлению «Оптимизации процессов управления ИБ»
e-mail: v.maksimov@andek.ru
тел: +7 (495) 280-1550, доб. 1103
моб.: +7 (926) 253-4844

Андэк