

PCI DSS*

Le paradoxe français

Thierry AUTRET
Groupement des Cartes Bancaires CB

(* Payment Card Industry Data Security Standards)

Contexte

Environ 2.000 millions de cartes bancaires en circulation dans le monde

Toutes gérées au travers de systèmes d'information

De la fraude « *à l'arraché* » à la fraude « *industrielle* »

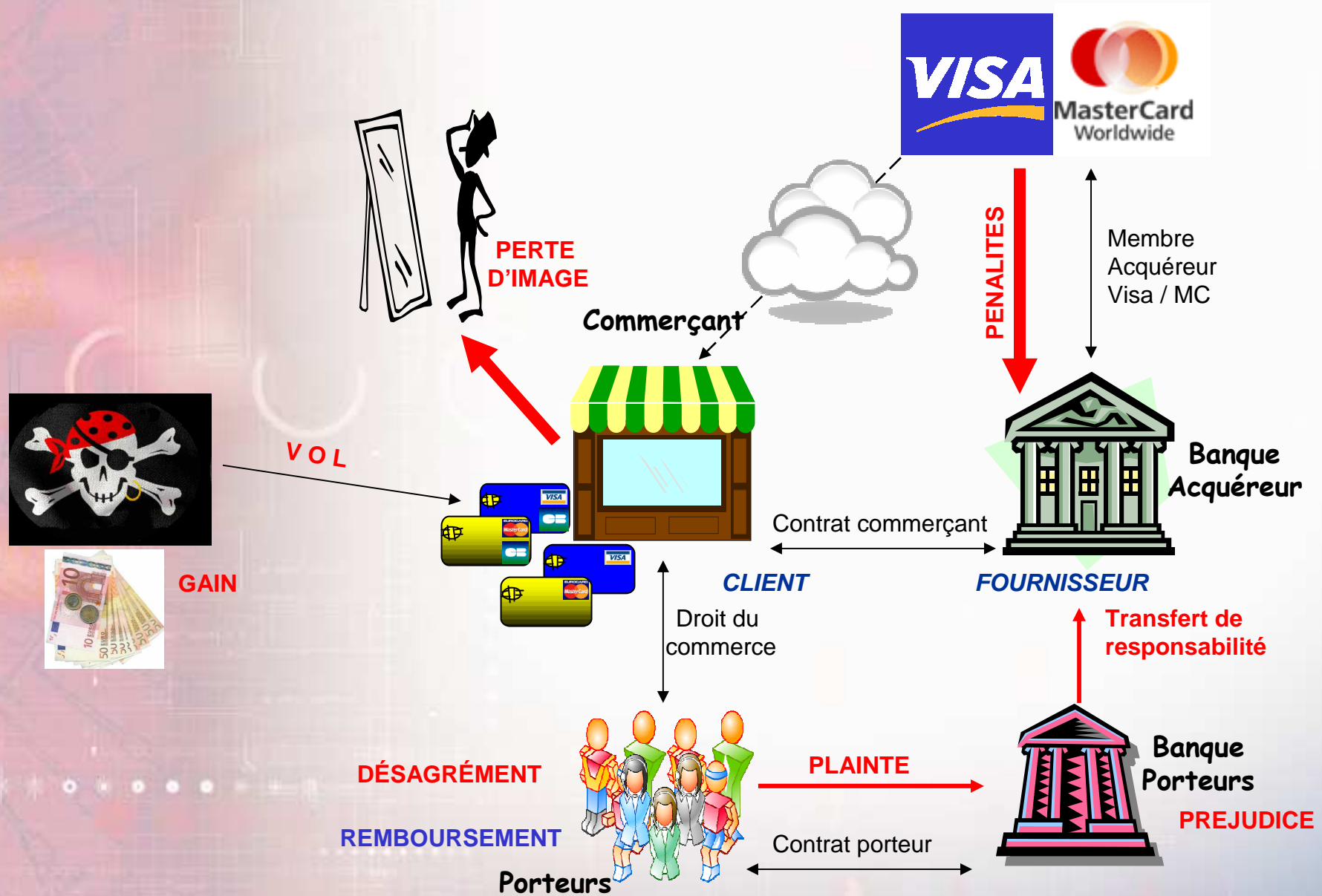
- Filières mafieuses internationales
- Voleurs / ingénieurs diplômés
- Capture, tests, revente, utilisation
- Nouveau « *marché* » des données sensibles

Conformité du secteur « *privé* »

- Dès 2004 les grands réseaux (VISA, Mastercard, Amex, Discover et JCB) développent des programmes de « *sensibilisation* » à la protection des données cartes
- Début 2005 convergence vers le standard PCI DSS
- En 2006 création du PCI Standard Security Council, organisme de maintenance des standards de conformité PCI
- Chaque réseau reste maître des conditions d'application des standards

Les acteurs

- Le porteur et ses données cartes
- Le commerçant qui collecte les données cartes
- La banque du commerçant qui est membre des réseaux internationaux
- Les réseaux internationaux
- La banque du porteur qui assume le préjudice financier
- Le fraudeur



La banque du commerçant

Doit mettre en œuvre PCI DSS dans son contexte, à savoir :

- Son SI « *cartes bancaires* » interne
- Par extension celui de ses prestataires

et

- Le SI « *cartes bancaires* » de ses « *clients* » commerçants

Le commerçant

Tous commerçants confondus :

- Détaillant indépendant
- PME, franchisés
- Grands commerces de taille (inter)nationale
- Commerçants en ligne

Dispose trop souvent de données complètes (Coordonnées du porteur, n° carte, date, cryptogramme visuel) dans un but de gestion de ses clients

Dispose souvent d'une informatique de gestion « à plat » et ouverte sur internet

N'a pas évalué le risque lié au vol d'informations

Référentiel PCI DSS

Depuis oct.08 version 1.2

- Référentiel d'audit inspiré des objectifs de sécurité et points de contrôle de l'ISO 27002
- Plus des exigences spécifiques à la protection des données sensibles (chiffrement)
- Plus des scans trimestriels

6 thèmes, 12 exigences, 259 points de contrôle

6 thèmes, 12 exigences, 259 points de contrôle

Bâtir et exploiter un réseau sécurisé (37) : FW, mots de passe

Protéger les données « porteur » (32) : stockées et en transit

Disposer d'un programme de gestion des vulnérabilités (47) : AV, sécurité des développements

Mettre en œuvre des mesures de contrôle d'accès efficaces (58) : accès aux données, ID unique, accès physiques

Surveiller et tester régulièrement les réseaux (44) : traces et analyse des accès, tests des systèmes

Définir, maintenir et mettre en œuvre une Politique de Sécurité de l'Information (41) : PSSI, responsabilités SI, formation, documentation

Les paradoxes

- Les acteurs français partagent la finalité du programme PCI DSS : mieux protéger les données sensibles cartes
 - ⇒ Mais pas la démarche de conformité à des « *solutions prédéterminées et imposées* »
- En revanche pour les non-spécialistes le questionnaire est un bon guide pour mettre en place des solutions de sécurité
- Les pénalités s'appliquent aux banques qui sont les **fournisseurs** des commerçants dans un contexte hautement concurrentiel
 - ⇒ Elles n'ont pas de « *force de coercition* » sur les commerçants pour les obliger à être conformes
- Les commerçants n'ont pas signé de contrat avec Visa ou MC mais uniquement avec leur banque acquéreur
 - ⇒ Elles ne veulent pas voir d'auditeur « *anglo-saxons* » auditer leur SI
- Le n° de carte n'étant pas considéré comme sensible, beaucoup de commerçants l'utilisent comme donnée **d'identification** (Sncf, Air France, etc.)

Le contexte carte en France

2007: toutes les cartes françaises sont « à puce » au format EMV

Seuls les étrangers en France utilisent la piste (de + en + équipés de puce EMV)

L'investissement des différents acteurs (banques, constructeurs, commerçants) a été très important depuis 1992 pour généraliser la carte à puce

Reproche de certains : des acquéreurs étrangers ne font pas les contrôles minimaux lors d'un paiement (e-commerce: contrôle de la date de péremption, contrôle du CVV/CVC). A cause d'eux le programme PCI DSS doit s'appliquer au monde entier.

Les paiements France/France ne passent pas par Visa ou MC mais par le schéma Carte Bancaire (CB)

Le contexte SSI en France

La coordination (maturité) des RSSI des entreprises française existe depuis longtemps par le biais de Clubs (CLUSIF, Club 27001, Club EBIOS, CCA, etc..)

L'approche de la SSI est faite sur la base d'une **analyse des risques** en définissant des **objectifs de sécurité** qui doivent être atteints par la mise en place de **mesures de sécurité**

L'ensemble des sociétés françaises est sensibilisé à la protection des données personnelles parce que cela est inscrit dans la **loi CNIL depuis 1976** : le numéro de carte est une donnée indirectement personnelle

Conformité ou efficacité ?

But du commerçant = ne pas avoir de compromission de données

- Par la conformité = audit par un QSA
- Par une analyse de risques avec une potentielle « *prise de risques* »

La sécurité d'un SI peut être efficace sans être strictement en conformité

La situation fin 2008

Les PSP (Atos, Experian, etc.) se sont fait certifier PCI DSS : approche commerciale nécessaire

Malgré leurs réticences, les commerçants ont entamé des démarches de « *Gap analysis* » pour estimer leurs écarts par rapport aux exigences du questionnaire complet

- Suppression des occurrences de données non essentielles
- Gros travail de scoping : isolation de la partie du SI qui contient des données sensibles carte

Différence entre efficacité et conformité : certains organismes ont des mesures de sécurité efficaces (ex: paramétrage des FW) mais ont des défauts de conformité (ex: pas de politique écrite des règles du FW)

Des RSSI peuvent apprécier la contrainte « *réglementaire* » pour obtenir des moyens afin de mettre en place un SMSI

La situation n'est pas égale pour tous, les PME ont de grandes difficultés à atteindre une conformité

Conclusion : Au-delà de l'obtention de la conformité, les effets bénéfiques du programme PCI DSS

- **Inventaire exhaustif** des systèmes de gestion des transactions monétiques
- **Formalisation des processus** de gestion IT (surtout au niveau exploitation et gestion sécurité SI)
- **Sensibilisation** à la Sécurité/Confidentialité SI
- **Amélioration** du niveau de **Qualité** des services
- Renforcement de l'**image** de la société