Retour d'expérience PCI DSS

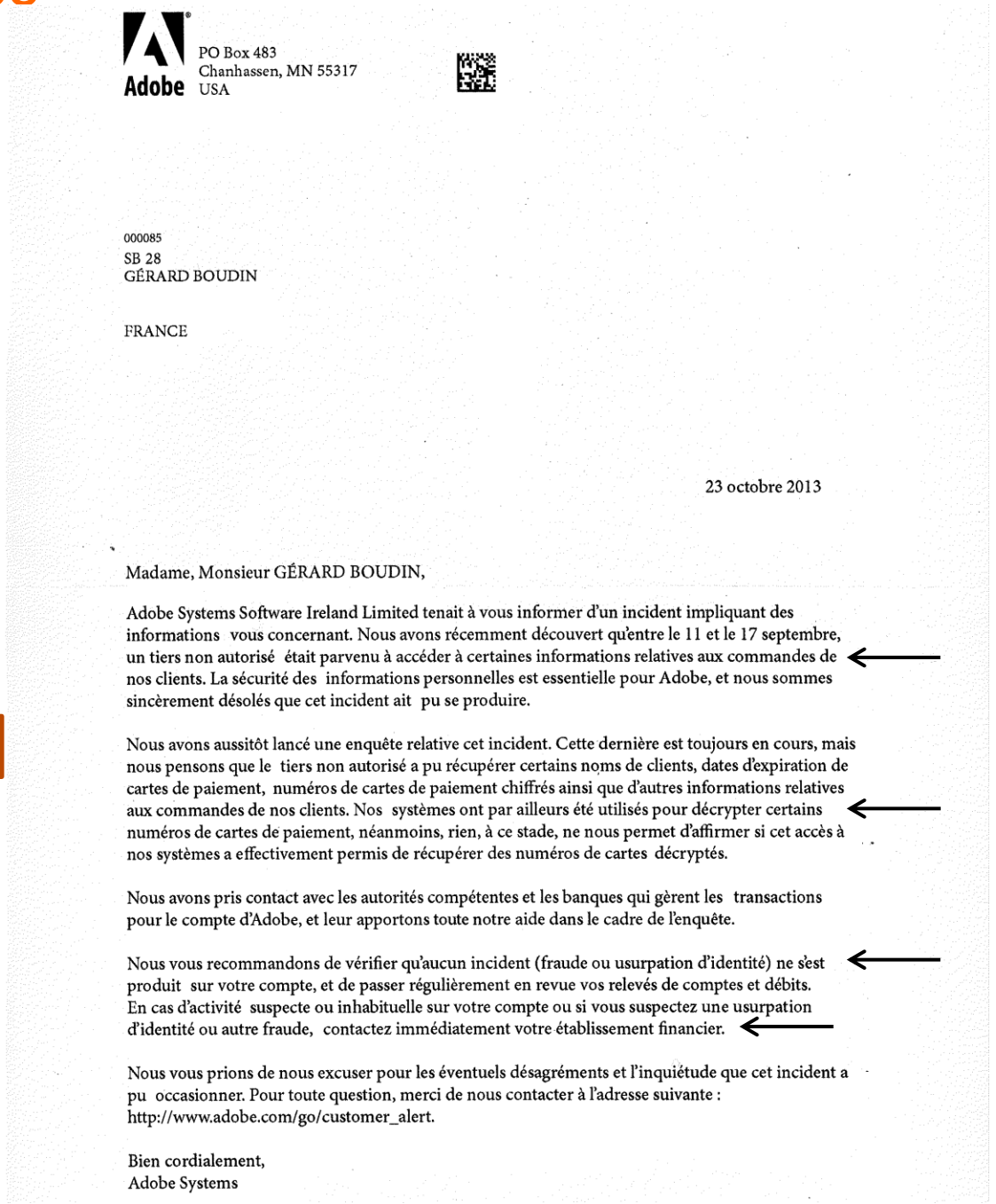
OSSIR

Gérard Boudin

8 avril 2014

Fraude Adobe

2,9 puis 38 millions de comptes affectés



Adobe
PO Box 483
Chanhassen, MN 55317
USA

000085
SB 28
GÉRARD BOUDIN

FRANCE

23 octobre 2013

Madame, Monsieur GÉRARD BOUDIN,

Adobe Systems Software Ireland Limited tenait à vous informer d'un incident impliquant des informations vous concernant. Nous avons récemment découvert qu'entre le 11 et le 17 septembre, un tiers non autorisé était parvenu à accéder à certaines informations relatives aux commandes de nos clients. La sécurité des informations personnelles est essentielle pour Adobe, et nous sommes sincèrement désolés que cet incident ait pu se produire.

Nous avons aussitôt lancé une enquête relative cet incident. Cette dernière est toujours en cours, mais nous pensons que le tiers non autorisé a pu récupérer certains noms de clients, dates d'expiration de cartes de paiement, numéros de cartes de paiement chiffrés ainsi que d'autres informations relatives aux commandes de nos clients. Nos systèmes ont par ailleurs été utilisés pour décrypter certains numéros de cartes de paiement, néanmoins, rien, à ce stade, ne nous permet d'affirmer si cet accès à nos systèmes a effectivement permis de récupérer des numéros de cartes décryptés.

Nous avons pris contact avec les autorités compétentes et les banques qui gèrent les transactions pour le compte d'Adobe, et leur apportons toute notre aide dans le cadre de l'enquête.

Nous vous recommandons de vérifier qu'aucun incident (fraude ou usurpation d'identité) ne s'est produit sur votre compte, et de passer régulièrement en revue vos relevés de comptes et débits. En cas d'activité suspecte ou inhabituelle sur votre compte ou si vous suspectez une usurpation d'identité ou autre fraude, contactez immédiatement votre établissement financier.

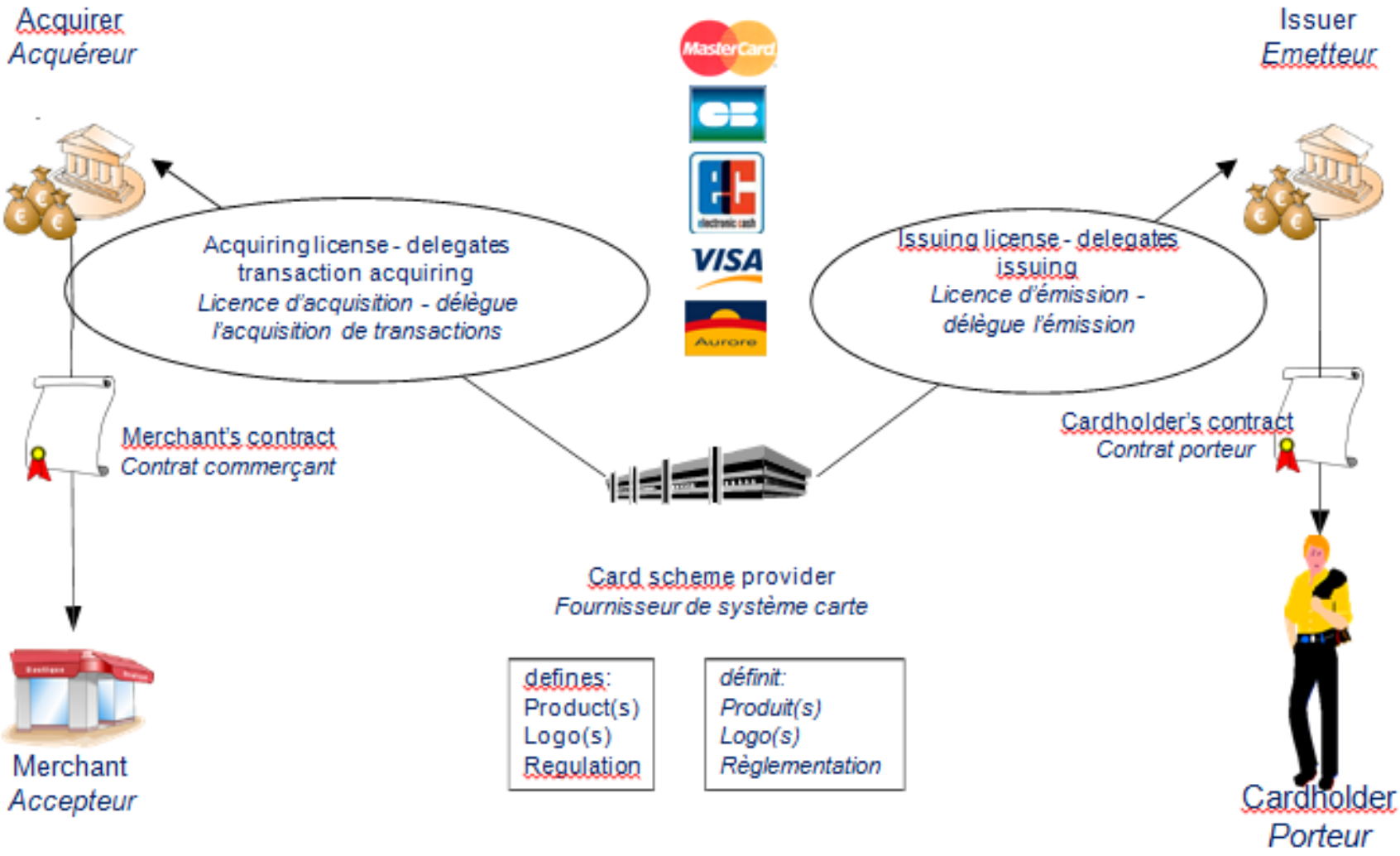
Nous vous prions de nous excuser pour les éventuels désagréments et l'inquiétude que cet incident a pu occasionner. Pour toute question, merci de nous contacter à l'adresse suivante : http://www.adobe.com/go/customer_alert.

Bien cordialement,
Adobe Systems

Autres fraudes

- SONY (2011)
  - 77 millions de comptes Network PlayStation affectés
- Subway (Sept 2012)
  - 146 000 cartes dérobées pour 10 millions de $ de perte
- Target (Déc 2013)
  - 40 puis 110 millions de cartes piratées
  - Target prendra en charge tous les coûts (estimés à 13,3 milliards d'€)
- Corée du Sud (21/01/2014)
  - 104 millions de cartes piratées (3 émetteurs de cartes impliqués + 2 banques : Citybank et Standard Chatered)
- Et toutes les autres fraudes non rendues publiques…
  - Selon le document d'inculpation rendu public par le tribunal de Newark (New Jersey), Carrefour aurait été délesté d'environ « 2 millions de numéros de carte de crédit » en 2008
- prix actuel d'une CB sur internet : de 23 à 135 $

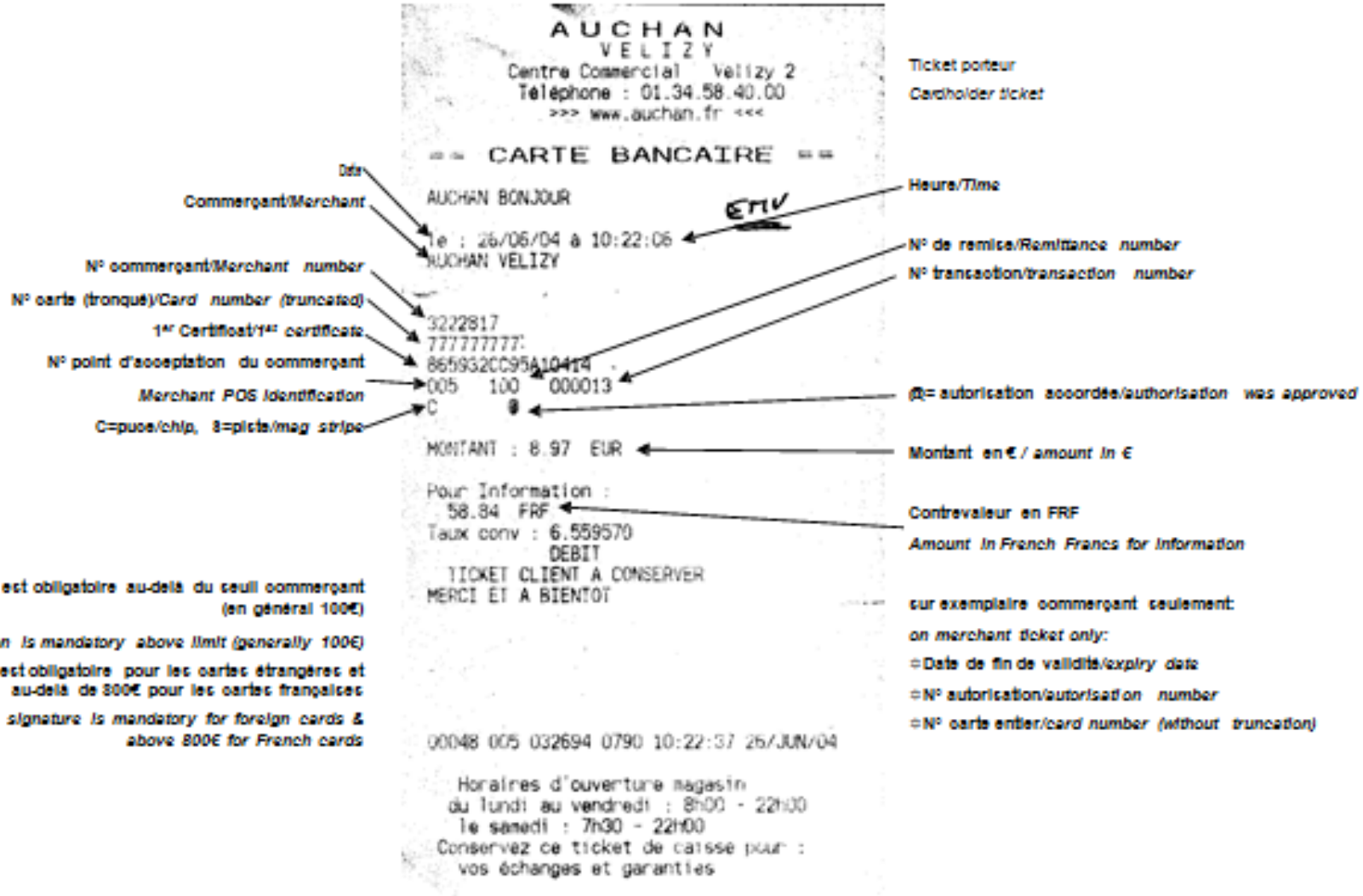
Le système Cartes



La carte bancaire

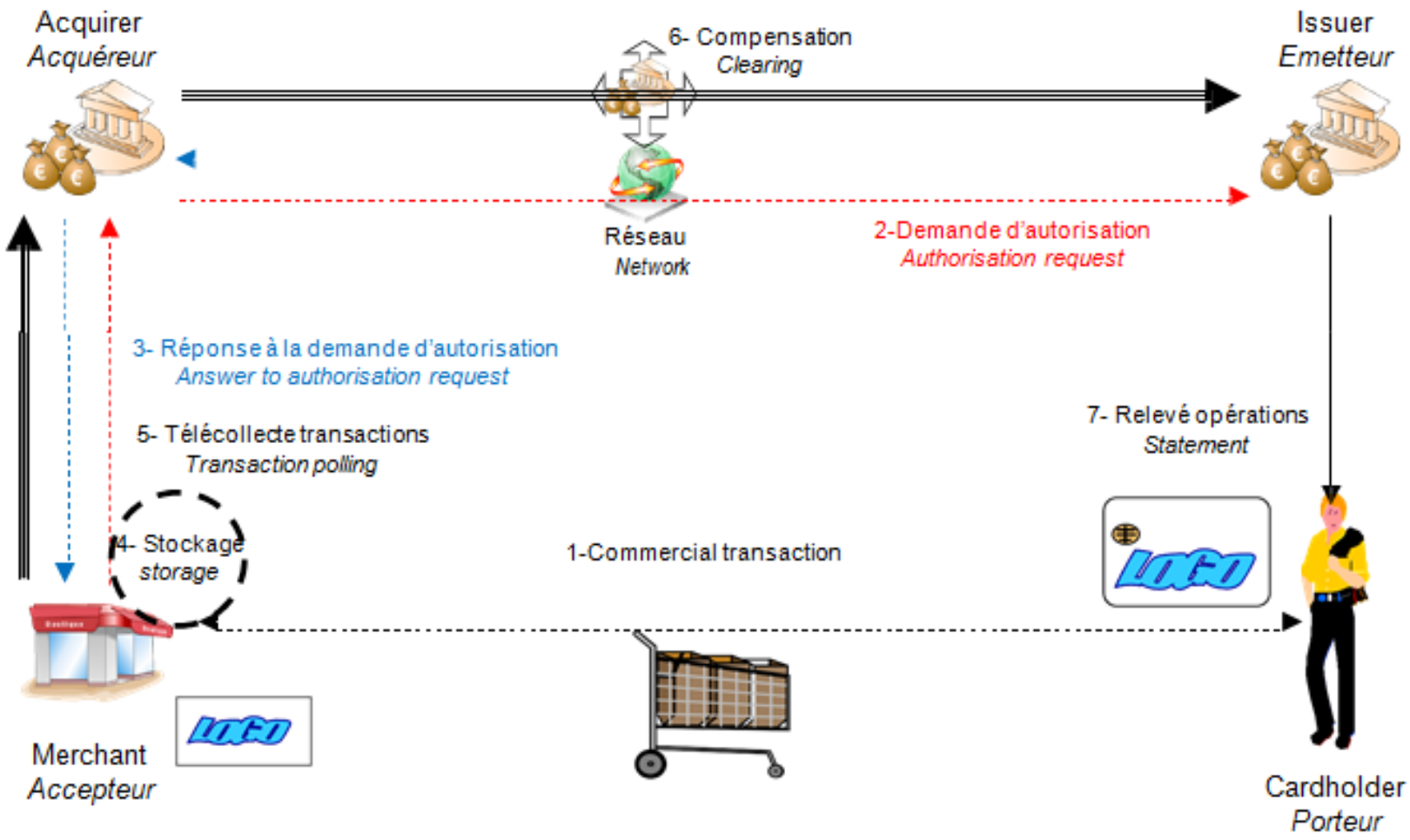
Clé de Luhn (pour éviter les erreurs de saisie : multiplication des chiffres de rang impair + chiffres de rang pair = multiple de 10)

Le ticket commerçant



* : le ticket commerçant fait apparaître le PAN complet

Transaction de paiement



Les conséquences des fraudes

- Risque majeur pour le marchand :
  - perte du droit d'encaisser
    - la banque peut clore la relation avec le marchand ou augmenter la commission des transactions

- Coûts directs
  - Pour le client : remboursements par sa banque*
    - montant des transactions frauduleuses (avec ou sans franchise : 150€**)
    - renouvellement des cartes compromises (80 € par carte)

  - Amendes pour les entreprises :
    - Corée : amende dérisoire (4155€)
    - Visa = Au cas par cas : de 25 000$ à 500 000$
    - Master Card = de 20 000 à 200 000$ selon le nombre de transactions

- Coût moyen (Ponemon Institute Mai 2013)
  - 120 € de perte par donnée unitaire volée (France)

- Coûts indirects
  - réputation de la société, de la marque

* : articles L132-2,4,5,6 du code monétaire et financier

** : article 61(3) Banque centrale Européenne

La réponse des fournisseurs de cartes : le PCI Council

- Payment Card Industry Data Security Standard
  - managé par le PCI SSC : PCI Security Standards Council, fondé en 2006 par :

    - 650 organisations adhérentes représentant les marchands, les banques, les PSP (Payment Service Providers)

- Modèle basé sur la certification
  - réponse oui à 1400 exigences (RoC) pour obtenir la certification, délivrée par un QSA, lui-même certifié par le PCI council. Certificat à renouveler annuellement.
  - formations payantes, examens payants, renouvellement annuel payant

- Actuellement on est en version 3.0 (MAJ tous les 3 ans)
  - Documentation disponible en ligne https://www.pcisecuritystandards.org

  - La version 3 n'apporte pas d'exigences supplémentaires relatives au Cloud ou au NFC

Audit sur site ou questionnaire de vulnérabilités
6 thèmes regroupant 12 points

PCI DSS – Présentation détaillée

Création et gestion d'un réseau sécurisé	1. Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes 2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
Protection des données des titulaires de cartes de crédit	3. Protéger les données de titulaire de carte stockées 4. Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts
Gestion d'un programme de gestion des vulnérabilités	5. Utiliser des logiciels antivirus et les mettre à jour régulièrement 6. Développer et gérer des systèmes et des applications sécurisés
Mise en œuvre de mesures de contrôle d'accès strictes	7. Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître 8. Affecter un ID unique à chaque utilisateur d'ordinateur 9. Restreindre l'accès physique aux données des titulaires de cartes
Surveillance et tests réguliers des réseaux	10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes 11. Tester régulièrement les processus et les systèmes de sécurité
Gestion d'une politique de sécurité des informations	12. Gérer une politique de sécurité des informations pour l'ensemble du personnel.

Exemple de certificat

NTT SECURITY

This is to certify that

OGONE
www.ogone.com

has been assessed by NTT Security Ltd and was found to be compliant against the PCI Data Security Standard, endorsed by the PCI Security Standards Council.

Category:
LEVEL 1 SERVICE PROVIDER

Onsite assessment:
FEBRUARY 5,6 2013

Quarterly ASV Scans:
Passed - Qualys ASV

CERTIFICATE OF COMPLIANCE

Conditions of issuing:

1. NTT Security Ltd has issued this certificate to indicate that the aforementioned company has been assessed against the objectives of the Payment Card Industry (PCI) Data Security Standards (DSS) validation methods and were found to be compliant to PCI DSS on the date of issue only, no other guarantees are given.

2. This certificate of compliance is deemed valid if produced in conjunction with a clean external vulnerability scan validated as per ASV Program Guide.

3. This certificate is subject to compliance conditions as laid out within the PCI Security Standards Council certification program. This certificate is valid for a one year period from date of issue.

4. This certificate offers no guarantee or warranty to any third party that the company is invulnerable to attack or breaches in its security, and NTT Security Ltd accordingly accepts no liability to any third party in the event of loss or damage of any description caused by any failure in or breach of customer's security.

Signature

Francesco Consiglio, Lead QSA

issued

February 14th 2013

www.ntt-security.com

PCI DSS : cadre de contrôle

- Niveau du marchand :
  - 1 : > 6 millions de transactions/an
  - 2 : de 1 à 6 millions/an
  - 3 : de 20 000 à 1 million/an
  - 4 < 20 000 transactions/an
- Tout marchand de niveau 1 doit être conforme* PCI DSS
- Tout marchant ayant subi une attaque passe au niveau supérieur
  - déclaration obligatoire (VISA, Mastercard, dépôt de plainte)

* : certificat annuel signé par un QSA

Que faire en cas d'attaque?

- Guide VISA
  - Préserver les preuves et faciliter l'investigation
    - documenter toutes les actions
    - ne pas arrêter ni utiliser le système supposé compromis, mais le débrancher physiquement du réseau
    - préserver les logs (serveur, BDD, firewalls)
    - si présence de WIFI, changer immédiatement le SSID
    - contacter votre banque et VIFraudControl@visa.com
  - Répondre à l'attaque
    - avoir un programme de certification PCI DSS
    - Désigner une équipe restreinte
    - Contacter un QIRA (Qualified Incident Response Assessor – Cf liste)
    - Avoir un plan de communication déjà prêt
      - pourquoi communiquerai-je? Quand et comment dois-je le faire?
    - Avec qui communiquer?
      - porteurs de cartes, service client, employés, partenaires, médias, juristes, actionnaires

Cas Visa

Découverte	Certifié ?	Signalé par?	Conséquences pour le marchand
	✓	le marchand à VISA	➢ pas de pénalité et problème non rendu public
VISA	✓	VISA	➢ mesures à mettre en place ➢ pas de pénalité et problème non rendu public
	✗	le marchand à VISA	➢ obligation pour le marchand de faire un audit annuel ➢ mesures à mettre en place et test de conformité présenté à VISA ➢ des pénalités peuvent être appliquées
VISA	✗	VISA	➢ le marchand est tenu de faire un audit tous les ans ➢ le marchand paie les pénalités à VISA (de 50 à 90$ par carte) via la banque et doit assumer tous les coûts liés à la fraude

Cas MasterCard

Découverte	Certifié ?	Conséquences pour le marchand
	✓	➢ pas de pénalité
	✓	➢ pas de pénalité
 	✗	➢ Marchands niveaux 1 et 2 • pénalité de 25 000$ à 200 000$ ➢ Marchands niveau 3 et 4 • pénalité de 10 000$ à 80 000$

A quoi cela sert-il d'être certifié PCI DSS?

- **Le coût de la certification peut dépasser le coût du préjudice**
  - Discussion âpre sur ces coûts :
    - Pour une entreprise qui a 50 000 CC, une perte de 6,6 millions de $ est à comparer avec le coût de certification entre 3 et 4 millions de $ (selon le directeur Européen de PCI DSS Council).
    - A quoi il ajoute le coût de "réputation"
- **TARGET**
  - va payer 2 fois (coût de la certification + une partie des 13,3 milliards d'€)
- **Selon l'enjeu pour la société :**
  - PSP ou banque

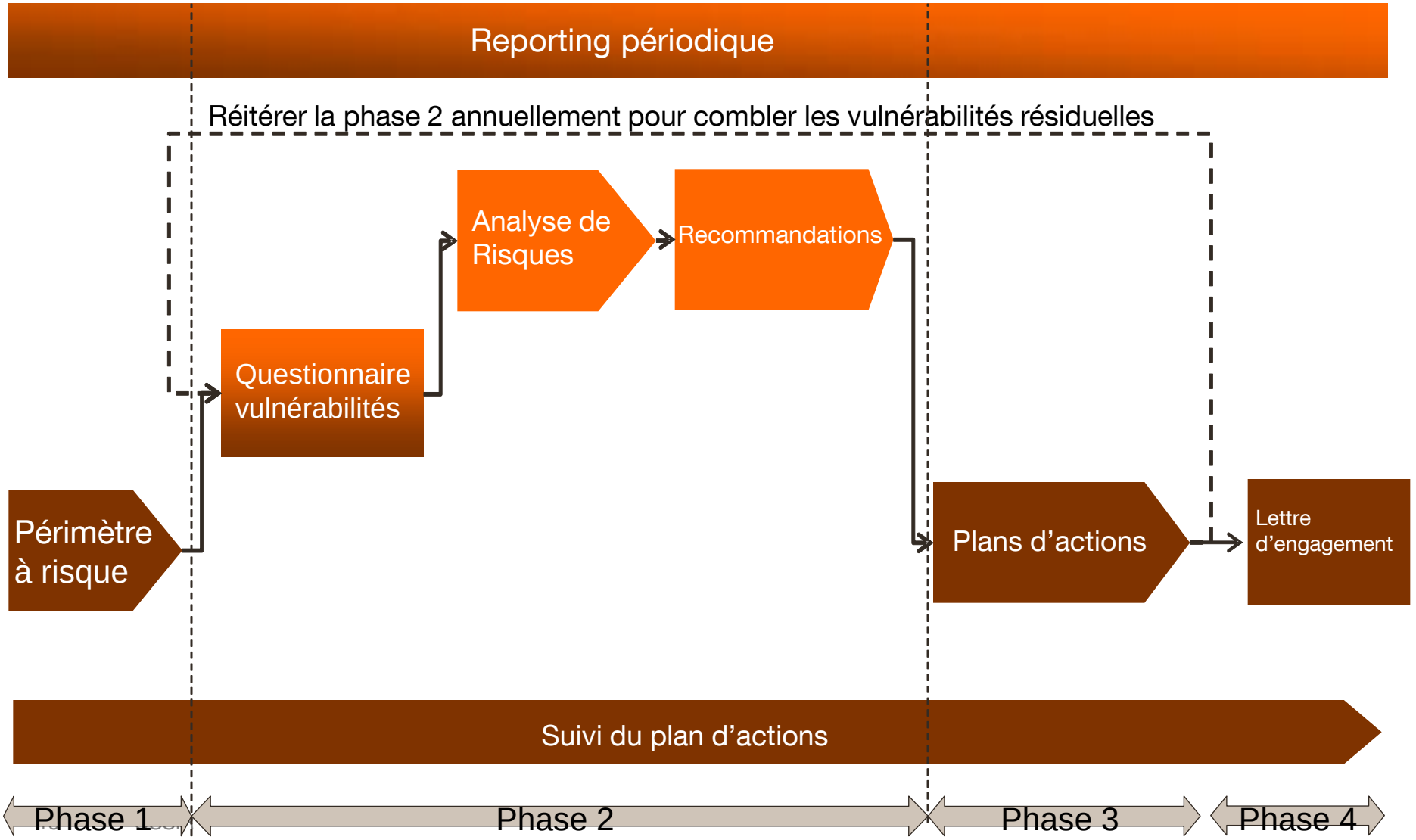
L'approche par les risques

- Pourquoi?
  - Sortir du modèle « business » de PCI DSS
    - dire que la société est « compliant » à 95% ne veut pas dire qu'elle est exempte de risque majeur
    - un audit PCI DSS ne permet pas de proposer des mesures concrètes de protection contre les risques les plus élevés
  - Pas d'intérêt si la société n'a pas pour objectif de devenir PSP

- On dispose par ailleurs d'un environnement normatif
  - ISO 27K
    - les risques liés aux cartes bancaires en sont un sous-ensemble
  - EBIOS (ANSSI)
    - scénarios de menaces (29 pertinents sur 52)

Menaces génériques :
Espionnage à distance
Ecoute passive
Vol de supports ou de documents
Récupération de supports ou de documents mis au rebut
Divulgation
Piégeage matériel
Piégeage logiciel
Altération de données
Erreur d'utilisation
Abus de droits
Usurpation de droits

Approche : Phase 1 ”Evaluer”, Phase 2 “Analyser”, Phase 3 “Remédier”, Phase 4 “consolider”



Détail du questionnaire de vulnérabilités

PCI DSS Conditions →	1	2	3	4	5	6	7	8	9	10	11	12
Network design												
Architecture principles	X			X							X	
Hardening network devices	X	X										
Event logging										X		
System design												
Architecture principles			X	X								
Hardening systems		X										
Key management (storage only)			X									
Event logging					X					X		
Development practices												
Development environment						X						
Go live practices						X						
Training and awareness						X						X
Production practices												
Configuration management												
Change management						X						
Incident management												X
Documentation	X											X
Training and awareness			X									X
SOC activities					X					X		
Backup media management								X				
Users practices												
Access control							X	X				
User activities	X			X					X			
Governance												
Policies												X
Third party management												X
Control and audit											X	
Physical security												
Access control									X			
Visitors access management									X			

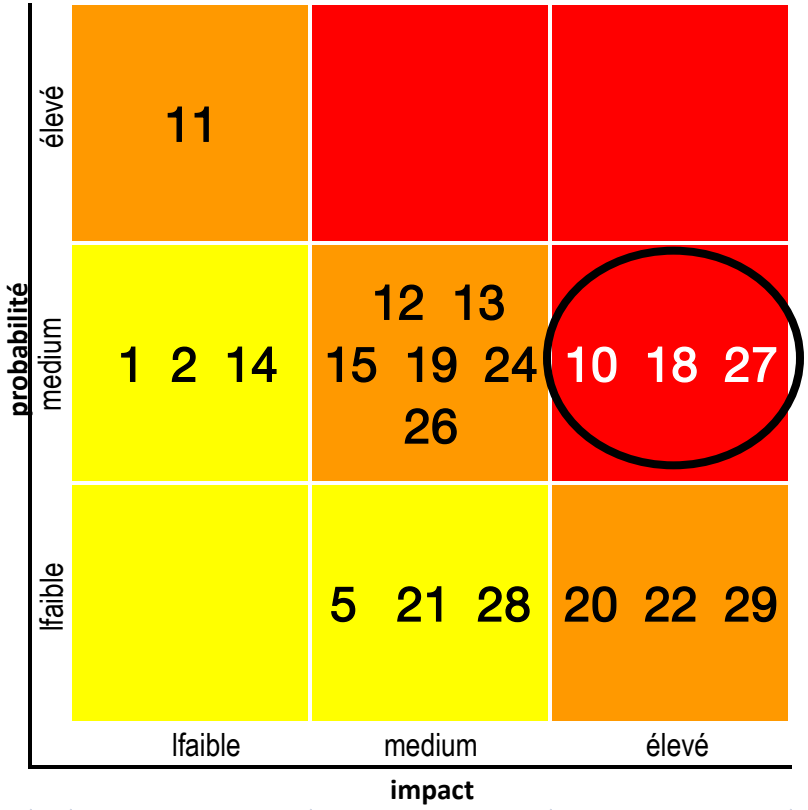
Détail du questionnaire de vulnérabilités

- Principes d'architecture réseau
  - DMZ, WIFI, IDS/IDPS
- Principes d'architecture système
  - séparation front, middle, back-office, IDS/IDPS
- Durcissement du réseau et des serveurs
  - mots de passe, ports, services
- Gestion des clés de chiffrement
  - distribution, séquestre
- Gestion des logs
  - sur un serveur séparé, protection contre l'effacement des traces, conservation d'historique
- Développement
  - revue de code, séparation des environnements, tests
- Production
  - CMDB, gestion des patches de sécurité, gestion des changements, gestion des incidents de sécurité, sauvegardes, documentation
- Gestion des utilisateurs
  - métier/privilégiés, mot de passe, expiration, résiliation
  - poste de travail avec FW et anti-virus
  - les faire signer une charte
- TMA
  - remote maintenance
  - audit chez eux?
- Accès physique
  - restrictif, tracé, filmé (accès aux baies)

Matrice de risques
(risque = impact * probabilité)

- Vue d'ensemble des risques
  - 29 risques génériques analysés
  - 19 risques applicables au contexte
  - 3 risques majeurs (maillons les plus faibles de l'ensemble des applications)

- Traitement des risques :
  - Les risques en « zone rouge » sont à traiter impérativement
  - Les risques en « zone orange » doivent faire l'objet d'une décision
  - Les risques en « zone jaune » sont généralement acceptés



Stratégie en cascade de traitement du risque PCI DSS

1

Suppression du risque

Quand c'est possible

En accord avec la MOA par suppression de l'usage des cartes et de leur présence dans le SI

2

Transfert du risque

Quand la suppression n'est pas possible

Transfert des N° de cartes vers un PSP certifié sans passer par le SI

3

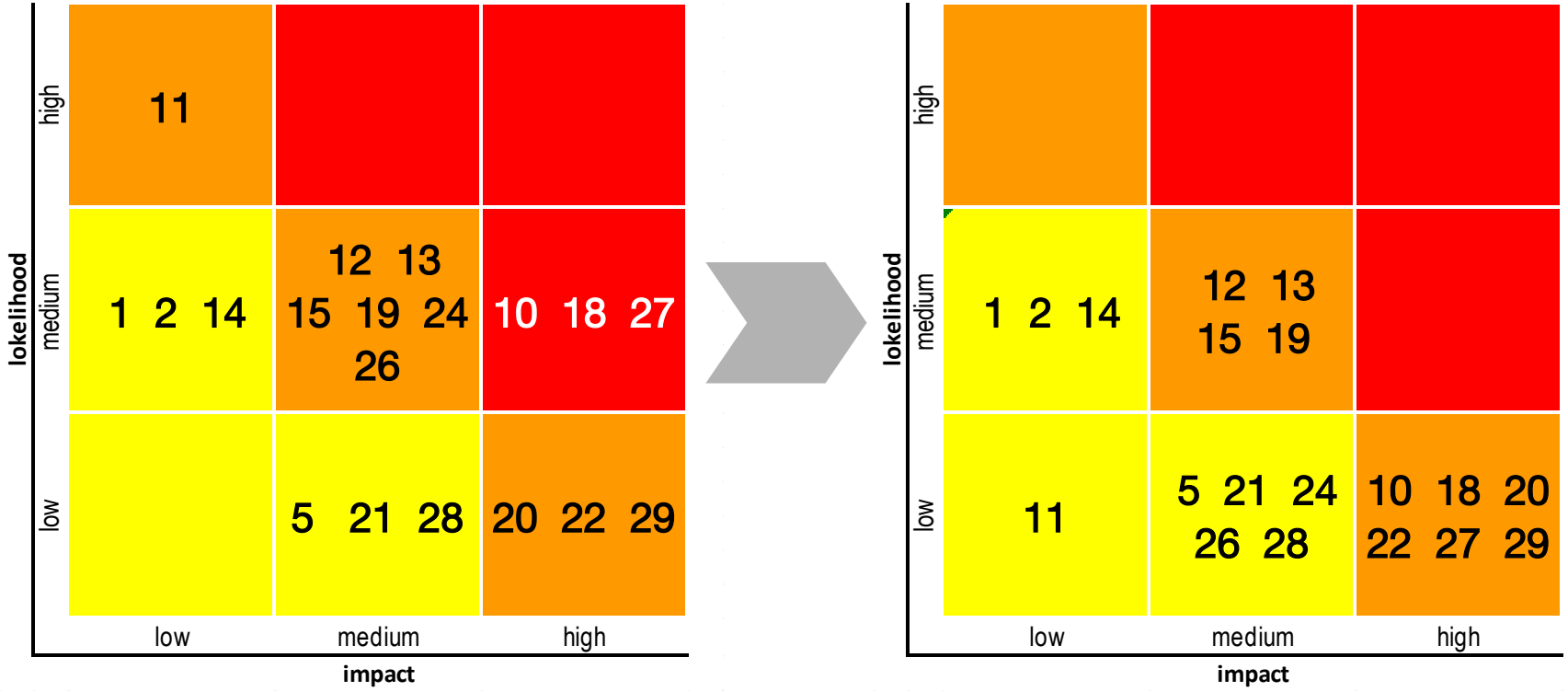
Remédier le risque

Si ni la suppression ni le transfert ne sont possibles

Démarrer un plan d'actions mettant en œuvre les recommandations

Conséquence

Risques avant/après remédiation



Retour d'expérience (les constats simples)

- PANs en clair
  - BDD ou dans emails
- Remote maintenance
  - comptes anonymes ouverts en permanence
- Centres d'appel
  - enregistrement des conversations
  - saisie des PANs, date de validité, CVV par l'opérateur
- Code non revu
  - développements spécifiques
  - ERPs pas toujours garantis
- Gestion des utilisateurs
  - ID pas révoqué systématiquement et rapidement
- PANs dans les jeux de test
  - pas toujours fictifs
- Charte, NDA
  - pas toujours signées
- Gestion de crise
  - la plupart du temps non anticipée

Retour d'expérience (les constats plus techniques)

- Gestion des changements
  - pas de nouveau check après tout changement d'importance
- Algorithme de chiffrement obsolète
  - encore beaucoup de 3DES (reco : AES 256)
  - les clés dans la BDD
- Gestion des logs (connexion, commandes système, applicatifs)
  - pas surveillée quotidiennement
- Gestion des patches de sécurité
  - pas appliqués systématiquement sur Windows
- Scans de vulnérabilité
  - pas systématiques
- Tests de pénétration
  - peu fréquents

Retour d'expérience (les recommandations)

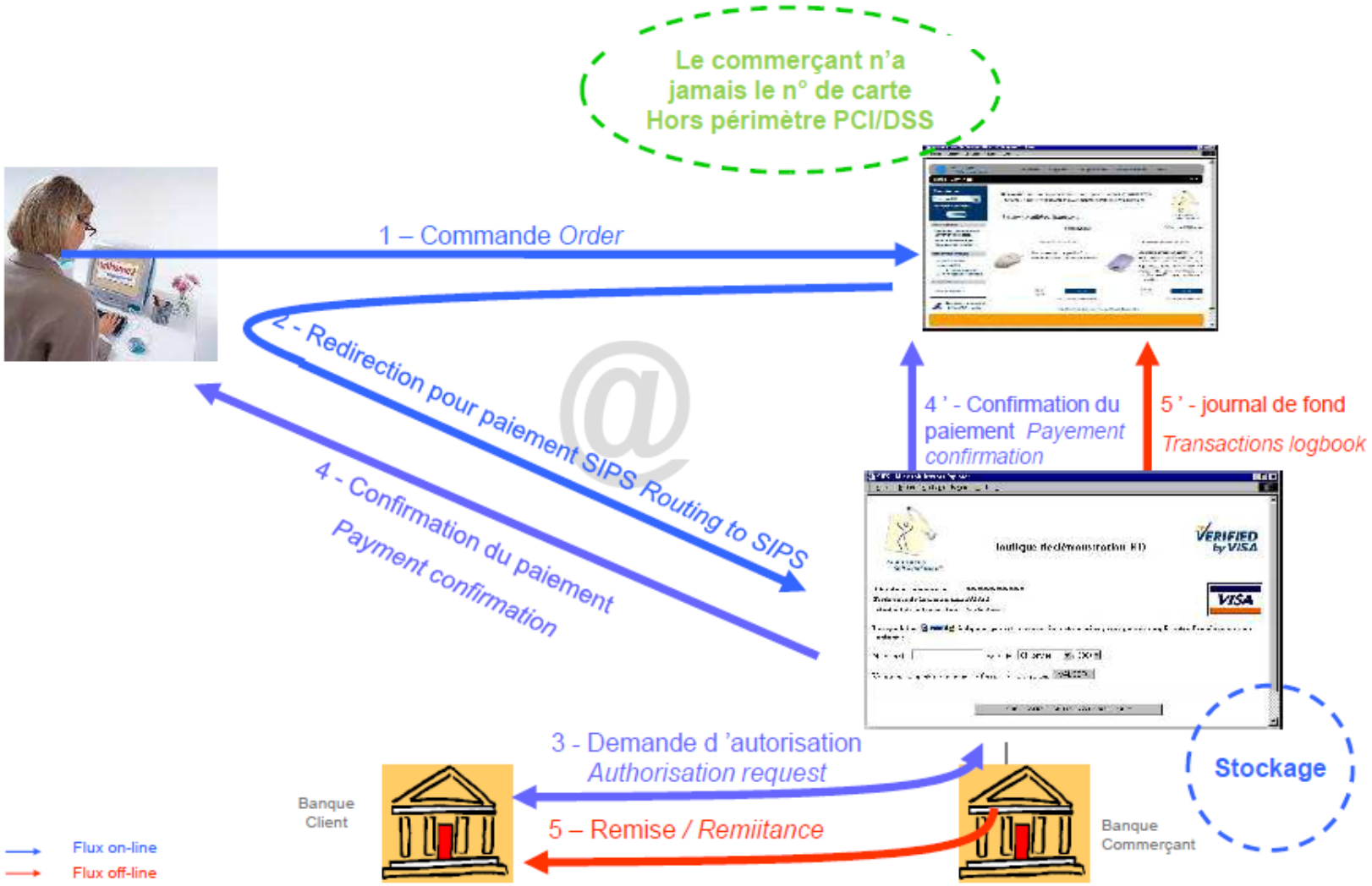
- **Supprimer le risque**
  - De façon surprenante, cela s'est produit fréquemment
    - applis historiques (il fut un temps où on ne s'en préoccupait pas)

- **Transférer le risque**
  - Les services proposés par les PSP sont payants mais une fois mis en place l'application sort du périmètre PCI DSS
    - coût dégressif à la transaction
    - demander annuellement le certificat

- **remédier**
  - Le fait de chiffrer les PANs présents est déjà un premier rideau de protection
  - Cloisonnement des réseaux
  - Le plan d'action doit être suivi (ratio nb de systèmes protégés / nb de systèmes impactés)

- **En préventif :**
  - Il faut surveiller les logs!
  - passer régulièrement les scans de vulnérabilité
  - gérer les changements (tests de non régression "sécurité")
  - prévoir une gestions de crise

Exemple de PSP



Et demain?

- **Améliorations de la sécurité :**
- 3D Secure
  - mais peut-être mal utilisé par la banque ou par le marchand

- Payweb card
  - Après avoir sélectionné *une carte personnelle* et saisi le montant de l'achat, on obtient *un numéro virtuel à recopier sur le formulaire* du site marchand (valable 30 jours). Autant de N° virtuels que d'achats.

- Wallets
  - Paypal, Paylib, V.me, Orange Money

- **Nouveaux risques :**
- Le paiement sans contact
  - transmission non chiffrée entre le smartphone et le TPE

Merci

Questions?