Zeitschrift: Schweizerische Zeitschrift für Kriminologie = Revue suisse de criminologie = Rivista svizzera di criminologia = Swiss Journal of Criminology

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 4 (2005)

Heft: 2

Artikel: Fraude à la carte de crédit : éclairage sur un phénomène en pleine expansion

Autor: Garcia, Marylaure

DOI: https://doi.org/10.5169/seals-1050855

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

Download PDF: 19.01.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Marylaure Garcia

Fraude à la carte de crédit: éclairage sur un phénomène en pleine expansion[1]

Résumé
Chaque année, la fraude à la carte de crédit occasionne des pertes financières considérables. La connaissance des dispositifs de sécurité et des différentes transactions possibles au moyen de la monnaie plastique est indispensable à une bonne compréhension des failles de sécurité dont tirent profit les délinquants pour commettre leurs délits. Une coopération intensive des organismes d'émission, des détenteurs de cartes, des commerçants, des corps de police et des autorités judiciaires aux niveaux tant régional, national qu'international est la base d'une lutte efficace contre la fraude à la carte de crédit.
Mots-clés: cartes de crédit – sécurité – fraudes – détection – auteurs – modalités – victimes – mesures.

Zusammenfassung
Der Kreditkartenbetrug verursacht jedes Jahr erhebliche finanzielle Verluste. Systeme weisen Sicherheitsmängel auf, die von Betrügern ausgenützt werden. Um das betrügerische Vorgehen zu verstehen, ist es wichtig, die Sicherheitsdispositive und die zahlreichen Arten von Kreditkartentransaktionen zu kennen. Die enge regionale, nationale und internationale Zusammenarbeit unter den Institutionen, die Kreditkarten herausgeben, den Karteninhabern, den Händlern, der Polizei und den Gerichtsbehörden ist von grundlegender Bedeutung, will man Kreditkartenbetrug wirksam bekämpfen.
Schlüsselwörter: Kreditkarten – Sicherheit – Betrug – Entdeckung – Täter – Modalitäten – Opfer – Massnahmen.

Summary
Credit card fraud causes considerable financial loss each year. Security systems contain flaws, which are exploited by card fraudsters. In order to understand credit card fraud, it is essential to have knowledge of security measures and the various forms of transactions possible using plastic cards. Close regional, national and international cooperation between the institutions that issue credit cards, card-holders, retailers, police and judicial authorities is essential if credit card fraud is to be fought effectively.
Keywords: credit cards – security – fraud – detection – authors – modalities – victims – measures.

1. Introduction

L'apparition des cartes de crédit remonte à la seconde moitié des années 1960. Depuis lors, le nombre de cartes utilisées dans le monde n'a cessé d'augmenter. En parallèle, les cas de fraudes – à savoir l'utilisation de cartes, respectivement de données, par des personnes n'étant pas légitimées[2] – se sont multipliés. En effet, les différentes vulnérabilités du système et la négligence des différents partenaires ont été mises à profit par des personnes malhonnêtes cherchant à s'enrichir rapidement et sans trop d'efforts.

S'il est vrai que les individus agissant pour leur propre compte ou certains groupes de délinquants pratiquent la fraude à la carte de crédit dans un seul but d'enrichissement personnel, il n'en demeure pas moins que ce type de fraude permet également le financement d'autres activités délictueuses/criminelles d'une plus grande ampleur (par exemple celles de mafias ou d'organisations criminelles) et d'activités terroristes.

Loin de n'être qu'un comportement illégal marginal et sans importance, la fraude en matière de cartes de crédit est bien plus un type d'actes délictueux qui touche tant les secteurs privé que public et qui engendre des pertes considérables. Activité illégale se déroulant dans le contexte de la vie économique (au sens large) au mépris du respect de la confiance et de la bonne

1 Cet article est un extrait du travail de diplôme intitulé «Les fraudes en matière de cartes de crédit en Suisse» rédigé en 2003 par l'auteure dans le cadre des études postgrades HES en lutte contre la criminalité économique de Neuchâtel. Ce travail établit un bilan des éléments caractéristiques du dispositif de sécurité des cartes de crédit, des différents types de transactions possibles au moyen de cette monnaie plastique ainsi que des formes principales de fraudes connues en Suisse, tout en soulignant par quelle(s) faille(s) de sécurité elles ont été rendues possibles; il énonce également quelques mesures propres à réduire les opportunités de fraudes. Il n'aborde ni la question des abus commis par les détenteurs légitimes de cartes (par exemple au sens de l'art. 148 CPS) ni les délits propres aux commerçants, pas plus que la problématique générale des fraudes à la carte de crédit sous l'angle juridique.

2 L'utilisation par un tiers (par exemple un membre de la famille) de la carte de crédit remise librement par son détenteur légitime dans un but déterminé viole les rapports contractuels et doit être considérée comme fraude (utilisation d'un support authentique avec connaissance du NIP ou apposition de la signature propre audit tiers ou d'une signature contrefaite). Cet aspect du problème n'est toutefois pas traité dans le présent article.

foi en affaire, réalisée par des moyens et des méthodes qui ne font en principe pas appel à la force ou à la violence physique et exigeant des connaissances et un savoir-faire particulier, la fraude en matière de cartes de crédit représente l'un des nombreux exemples de criminalité économique.

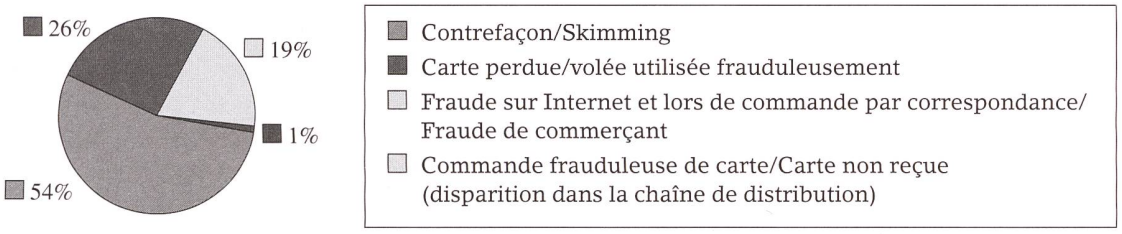
En l'absence d'ouvrages traitant des fraudes à la carte de crédit autrement que sous l'aspect juridique et compte tenu du peu d'informations – relevant du domaine public – publiées en la matière, une part importante des données ayant permis la rédaction de cet article a été obtenue lors d'entretiens personnels avec le chef de la sécurité d'un organisme d'émission, dix membres de polices judiciaires (cantonales et fédérale) et un membre du corps des gardes-frontières. Ces informations ont ensuite été «consolidées» et complétées sur la base de différents articles et publications (voir la bibliographie).

2. Quelques chiffres (pour la Suisse)[3]

En l'absence de données officielles, le chiffre d'affaires lié à l'utilisation de cartes de crédit réalisé en Suisse en 2003 est estimé entre 22 et 25 milliards de francs. Le montant brut des fraudes – à savoir toutes les transactions qualifiées[4] de frauduleuses par les détenteurs légitimes de cartes émises par des organismes d'émission avec siège en Suisse – se serait élevé, quant à lui, à environ 50 millions de francs. Sur la base des conditions générales d'utilisation et d'acceptation des cartes de crédit, les sociétés émettrices auraient toutefois pu faire supporter un tiers[5] de ces fraudes aux commerçants, et, plus rarement, aux détenteurs légitimes, dans la mesure où un comportement négligent pouvait leur être imputé. Cela étant, le montant net des fraudes à charge des organismes d'émission se serait effectivement élevé à quelque 37,5 millions de francs, soit, en moyenne, à environ 0,15%-0,2% du chiffre d'affaires réalisé.

Les graphiques ci-dessous présentent, en pourcent, les différents types de fraudes ainsi que la distribution régionale des fraudes au moyen de cartes de crédit émises en Suisse, tels que communiqués par deux organismes d'émission avec siège en Suisse.

Graphique 1: Proportion des différents types de fraudes en matière de cartes de crédit (2003)



Graphique 2: Distribution régionale des fraudes au moyen de cartes de crédit émises en Suisse (2001)

70% des dommages seraient la conséquence de l'utilisation frauduleuse de cartes de crédit dans les 10 pays suivants: Suisse, USA, France, Espagne, Italie, Malaisie, Thaïlande, Brésil, Mexique et Colombie.

3 Le type de données et la manière de les recueillir n'étant pas connus de l'auteure (examens de validité et de fiabilité dès lors impossibles), il convient de considérer avec retenue les chiffres et statistiques mentionnés ici, communiqués par des organismes d'émission avec siège en Suisse. Relevons en outre que l'importance des «chiffres noirs» (c'est-à-dire des fraudes non reportées) ne doit pas être négligée.

4 Il convient de relever qu'un certain nombre de transactions frauduleuses ne sont pas détectées/rapportées par les détenteurs légitimes.

5 Cette proportion peut être considérée comme relativement constante dans le temps.

3. Sécurité des transactions

Par principe, une transaction avec carte de crédit devrait être une transaction effectuée par le titulaire légitime au moyen d'une carte authentique. Les organismes d'émission ont donc mis au point des dispositifs de sécurité ainsi que des procédures particulières visant à s'assurer de la validité des cartes utilisées et de la qualité de leurs détenteurs.

3.1. Dispositifs de sécurité sur les supports plastiques

Cherchant à rendre infalsifiables et inimitables les cartes de crédit qu'ils émettent, les organismes d'émission développent régulièrement de nouveaux dispositifs de sécurité. Les caractéristiques communes et visibles à l'œil nu des dispositifs actuellement mis en place sur le support plastique de la majorité des cartes de crédit circulant sur le marché sont les suivantes:

1. Numéro de compte du titulaire (estampé);
2. Nom et prénom du titulaire (estampés);
3. Date de validité (estampée);
4. Hologramme (image tridimensionnelle) ou image particulière;
5. Caractère de sécurité (estampé; par exemple, pour Eurocard/MasterCard, les lettres MC);
6. Logo de l'organisme d'émission;
7. Bande magnétique: elle renferme un certain nombre d'informations – dont certaines sont cryptées – utiles à l'utilisation de la carte (par exemple le numéro de compte, la date de validité, le nom du détenteur et la limite de dépenses autorisées). Ces données ne peuvent être lues qu'au moyen d'un lecteur de bandes magnétiques;
8. Panneau de signature: le gommage ou la manipulation de cet élément détériore le dessin visible en arrière-fond, le rendant blanc ou taché. La carte doit impérativement être signée par son titulaire légitime.

Une carte est considérée comme authentique – c'est-à-dire présumée avoir été émise par l'organisme d'émission – lorsqu'elle contient tous les éléments du dispositif de sécurité tels qu'élaborés par l'organisme d'émission concerné. Un examen détaillé de la carte permet de déterminer si cette dernière est une carte authentique ou une carte contrefaite/falsifiée. Or, un tel contrôle – lorsqu'il est physiquement possible – prend du temps et nécessite certaines connaissances, raisons pour lesquelles certains délinquants ont réussi à déjouer les procédures de contrôle.

3.2. Lien entre le détenteur et la carte

Le besoin de s'assurer du lien existant entre la personne en possession de la carte et la carte elle-même est satisfait, dans la majorité des transactions, par l'invitation au détenteur:

1. d'introduire le NIP propre à la carte dans un terminal: Le numéro d'identification personnel (NIP) – présent sous forme cryptée dans la bande magnétique de la carte – n'est connu théoriquement que du titulaire légitime. La transaction n'est acceptée que si le NIP introduit dans le terminal est le NIP propre à la carte; ou
2. d'apposer sa signature sur l'avis de vente: Tout individu a par essence une signature qui lui est propre. La transaction ne devrait être acceptée par le commerçant que lorsque la signature figurant sur l'avis de vente est identique à celle apposée par le titulaire légitime sur le panneau de signature.

Le contrôle du lien entre le possesseur de la carte et le support peut encore, le cas échéant, être renforcé par une comparaison du support, sur lequel figurent en principe le nom et le prénom de la personne à qui la carte a été délivrée, avec une pièce d'identité.

Ces procédures permettent de vérifier si, de prime abord, le détenteur de la carte pourrait en être l'ayant-droit. Elles ne permettent toutefois en aucun cas de s'assurer de la titularité légitime. En effet, et à titre d'exemple, un tiers pourrait avoir connaissance du NIP, un individu malhonnête pourrait contrefaire la signature ou s'être procuré de faux documents d'identité. Cette faille du système a été mise à profit par des personnes mal intentionnées.

3.3. Deux systèmes électroniques de transactions[6]

3.3.1. Système on-line

Chaque transaction fait en principe l'objet d'une connexion au serveur d'autorisation de l'organisme émetteur. La validité des données contenues dans la bande magnétique de la carte (une partie d'entre elles du moins) est ainsi immédi-

6 En l'absence de statistique en la matière, on estime que 98,5% des systèmes utilisés en Suisse sont électroniques (98% *on-line* et 0,5% *off-line*) et 1,5% sont manuels.

atement contrôlée. Le contrôle peut se faire sur la base d'une liste positive, à savoir d'une liste des comptes existants, ou sur la base d'une liste négative, à savoir d'une liste des comptes bloqués. Ainsi, en fonction des circonstances, la transaction est refusée s'il s'avère que les données sont erronées ou que la carte utilisée a été bloquée.

Lorsque la transaction exige l'introduction du NIP, chaque tentative erronée est enregistrée dans la bande magnétique de la carte et auprès du serveur d'autorisation de l'émetteur de cette dernière. Lorsque celui-là constate trois tentatives infructueuses consécutives, il refuse purement et simplement toute transaction pour le compte géré au moyen de la carte.

3.3.2. Système off-line

La transaction ne fait pas l'objet d'une connexion immédiate au serveur d'autorisation de l'organisme d'émission. La connexion avec la centrale a lieu une ou plusieurs fois par jour et porte sur les transactions passées depuis la connexion précédente. La validité des données enregistrées dans la bande magnétique de la carte n'est ainsi pas contrôlée au moment de la transaction. Tout au plus le terminal vérifie-t-il si les données sont cohérentes (par exemple, la longueur et la formation du numéro de compte ainsi que la date de validité) et refuse, le cas échéant, la transaction. Il en fait de même lorsque le numéro de compte figure sur la liste prioritaire des comptes bloqués enregistrée périodiquement dans sa mémoire.

Les terminaux «intelligents» permettent, lorsque la transaction exige l'introduction du NIP, d'enregistrer chaque tentative infructueuse du NIP dans la bande magnétique de la carte. Ils sont aussi capables de détecter si le nombre de tentatives autorisées est atteint et de refuser, le cas échéant, la transaction (par exemple après 3 tentatives infructueuses consécutives), voire de bloquer toute utilisation ultérieure de la carte.

3.4. Transactions et procédures de contrôle

Les formes de transactions (par exemple à un distributeur automatique de billets, à un distributeur à essence, auprès d'un commerçant et par correspondance) sont multiples car elles dépendent du pays dans lequel la transaction est effectuée, du type de carte utilisée, du terminal à disposition et d'une connexion immédiate ou non à la centrale d'émission.

Les procédures de contrôle imposées par les organismes d'émission pour chaque type de transactions sont claires et documentées. Leur respect devrait théoriquement permettre de rendre difficile la commission d'actes délictueux. Toutefois, certaines d'entre elles connaissent des failles intrinsèques (par exemple l'absence de contrôle de la validité des données enregistrées dans la bande magnétique avec le système off-line ou encore la possibilité, dans certains cas, d'utiliser certains types de cartes de crédit auprès d'automates sans avoir à introduire de NIP), d'autres sont mal appliquées (certains commerçants estiment par exemple que la vérification on-line est suffisante et qu'il n'est donc nécessaire de procéder ni à un examen du support ni à une comparaison du numéro de compte et de la signature), voire détournées (par exemple lors d'un achat par correspondance). Ces failles de sécurité ont été mises à profit par certaines personnes mal intentionnées.

4. Quatre constellations de fraudes en matière de cartes de crédit

Très mobiles et imaginatifs, les délinquants ont développé toute une série de fraudes à la carte de crédit. Le tableau de la page suivante offre un aperçu des quatre constellations qui seront développées ci-après.

5. Utilisation de données personnelles sans support

5.1. Buts poursuivis par le délinquant

5.1.1. Achat par correspondance

Le fait que le commerçant ne soit jamais en présence de son client a pour conséquence, qu'en principe, il ne peut être procédé ni à un contrôle de la carte ni à un contrôle du lien existant entre le détenteur de la carte et le support.

L'intérêt des délinquants pour les commandes de marchandises ou la réservation de services par correspondance est évidemment grand puisqu'il s'agit d'un mode opératoire relativement peu risqué, ceci d'autant plus dans l'hypothèse où les transactions sont effectuées depuis un cybercafé ou une cabine téléphonique, qui, par définition, assurent un certain anonymat.

Tableau 1: Aperçu des principaux types de fraudes

	I *Utilisation de donnés personnelles sans support*	*II* *Utilisation de carte «blanches»*	*III* *Utilisation de contre-façons*	*IV* *Utilisation de carte authentiques*
Buts poursuivis	Achat par correspondance/Achat dans des commerces complices	Retrait d'argent/ Achat dans des commerces complices/ auprès d'automates	Achat dans des commerces auprès d'automates	Retrait d'arent/Achat dans des commerces/ Achat auprès d'automates
Support	Aucun	Carte vièrge	Carte contrefaite	Carte authentique volée ou trouvée
Données physique[7]	Copiées/Crées de toute pièces	Aucune/Copiées/ Crées de toutes pièces	Copiées/Crées de toutes pièces	Authentiques/Copiées/ Crées de toutes pièces
Données numériques[8]	Aucune	Aucune/Copiées	Aucune/Copiées	Authentiques/Copiées
NIP	Sans	Sans/Avec	Sans	Sans/Avec
Signature	Sans/Avec	Sans/Avec	Avec	Sans/Avec

5.1.2. Achat auprès de commerçants peu regardants, voire complices

Malgré les multiples recommandations faites aux commerçants en ce qui concerne la procédure d'acceptation et de paiement par cartes de crédit, certains d'entre eux acceptent encore parfois – sur pression du client – de procéder à la transaction sans que ne leur soit présentée physiquement de carte; ils se contentent ainsi d'introduire sur le bordereau de vente les données personnelles dictées par le client et de présenter le justificatif pour signature.

Ici aussi, ce type de transactions offre l'avantage à l'individu mal intentionné de se soustraire à toute procédure de contrôle de la part du commerçant.

5.2. Création de données de toutes pièces

Des pirates informatiques ont créé, à des fins délictueuses, des logiciels générateurs de numéros de comptes «valides» téléchargeables – généralement gratuitement – sur Internet. Ces logiciels exploitent les algorithmes et méthodes de vérification utilisés par les organismes d'émission pour déterminer les numéros de comptes de leurs clients. Ils permettent à une personne malhonnête de définir les paramètres de la carte et du numéro désirés (nom de l'organisme d'émission, nom de la banque et localité par exemple) et de créer un numéro de compte par simple «clic» de souris. Ne reste plus alors au délinquant qu'à faire preuve d'imagination pour se créer une identité et fixer une date de validité cohérente.

5.3. Obtention de données authentiques

Le délinquant a plusieurs moyens de se procurer des données authentiques (sans avoir besoin de rentrer en possession de supports):

a) Par surveillance stratégique des victimes potentielles. Exemples:
- Se procurer les copies d'avis de vente et de justificatifs que certains clients négligents oublient ou ne tardent pas à jeter dans des poubelles publiques peu après la transaction;
- Prendre connaissance des données figurant sur les cartes que certains clients négligents laissent déposées sur une table ou un comptoir jusqu'à ce que le commerçant procède à la transaction;

b) Par astuce. Exemples:
- Obtenir des renseignements sur les cartes de crédit des victimes en procédant à des ventes frauduleuses de biens et services par téléphone ou par Internet;
- Intercepter le courrier électronique de personnes procédant à des achats par cartes de crédit sur Internet;

c) Par vol. Exemple:
- Voler des avis de vente et des justificatifs de transactions auprès de commerçants négligents;

d) Par achat de données auprès de personnes peu scrupuleuses. Exemples:

7 On appelle ici «données physiques» les données qu'il est possible de lire sans avoir recours à un outil permettant la transformation de caractères en signes lisibles pour l'être humain (données personnelles imprimées sur un document ou sur le support d'une carte par exemple).

8 Les données enregistrées dans la bande magnétique sont des données numériques au sens large.

- Acheter des données auprès d'employés de l'hôtellerie ou d'employés d'organismes d'émission corrompus ou manipulés;
- Acquérir des listes de données auprès de pirates informatiques qui se sont infiltrés par le biais d'Internet sur les sites et bases de données peu sécurisés de commerçants négligents.

6. Utilisation de cartes «blanches»

6.1. Buts poursuivis par le délinquant

6.1.1. Retrait d'argent aux distributeurs automatiques de billets au moyen de cartes encodées

Certains délinquants cherchent à obtenir rapidement de l'argent liquide, ceci avec le moins d'efforts possibles. L'utilisation de cartes «blanches» encodées aux distributeurs automatiques de billets permet d'atteindre ce but.

6.1.2. Achat de marchandises et paiement de services auprès de commerçants complaisants au moyen de cartes encodées ou/et gaufrées

Le procédé consistant à acheter des marchandises et à payer des services auprès de commerçants complaisants utilisant le système manuel (sabot) ou électronique (terminal) ne peut être exclu, même si sa fréquence ne doit pas être surestimée. En effet, les différents participants gardent à l'esprit que le mécanisme de fraudes sera tôt ou tard découvert par les organismes d'émission, lesquels prendront les mesures adéquates auprès des autorités compétentes. Reste que certains commerces créés dans un but purement délictueux sont déjà liquidés lorsque la supercherie est découverte.

6.1.3. Achat de marchandises et paiement de services auprès d'automates au moyen de cartes encodées

L'achat de marchandises (par exemple de l'essence) et le paiement de services (par exemple un billet CFF) ne constituent vraisemblablement pas des buts en soi, compte tenu du déséquilibre entre, d'une part, les gains potentiels et, d'autre part, les efforts et les risques liés à la création de la carte. Toutefois, un délinquant en possession d'une carte «blanche» encodée n'hésitera pas à en faire usage auprès d'automates.

6.2. Acquisition de cartes «blanches» / vierges

Les cartes «blanches» – appelées ainsi en raison de leur couleur la plus fréquente à l'achat – sont des cartes plastiques vierges à bande magnétique, aux dimensions exactes d'une carte de crédit, disponibles dans les commerces suisses et étrangers ainsi que sur Internet. Elles sont notamment utilisées pour la confection de cartes clients et de cartes d'entreprises.

6.3. Cartes «blanches» encodées

L'utilisation, d'une part, d'une carte vierge dont la bande magnétique a été encodée avec les données enregistrées sur la bande magnétique d'une carte authentique et, d'autre part, du NIP propre à cette dernière permet au délinquant de procéder à des retraits d'argent aux distributeurs automatiques de billets et d'acheter des biens ou de payer des services auprès d'automates. Au moyen de cette seule carte, le délinquant peut également procéder à des transactions auprès de commerçants complices utilisant un système électronique pour lequel l'introduction du NIP n'est pas exigée.

Pour atteindre son but, le délinquant se procure illégalement les données enregistrées dans la bande magnétique de cartes existantes, copie ces données sur la bande magnétique de cartes vierges et recherche le NIP correspondant à chaque carte. Le cas échéant, afin de pouvoir faire usage d'une carte sur une plus longue durée, il modifie une partie des informations enregistrées dans la bande magnétique au moyen de logiciels informatiques.

La procédure consistant à copier les informations figurant sur la bande magnétique d'une carte de crédit authentique, à les stocker, puis à les recopier sur la bande magnétique d'une autre carte est appelée procédure d'écrémage ou «skimming». Cette procédure peut être effectuée à l'aide des outils suivants:

1. Lecteur de bandes magnétiques: lorsque la carte de crédit authentique est passée dans la fente de lecture du périphérique, les informations enregistrées dans la bande magnétique de cette carte sont copiées sur une puce électronique. Ces données seront ultérieurement transférées par le délinquant sur un ordinateur.
2. Encodeur de bandes magnétiques: à l'aide d'un ordinateur et de logiciels adaptés, ce périphérique permet de transférer les données de la carte authentique sur la bande magnétique de la carte vierge. Le procédé est simple:

la carte à encoder est passée dans la tête de lecture de l'encodeur, lequel copie sur la bande magnétique de cette carte les données précédemment mémorisées.

Dans l'hypothèse où le délinquant n'a pas pu prendre connaissance du NIP lors de la copie des données (par exemple en raison du fait que le détenteur prudent n'a pas inscrit son NIP à même la carte), il peut l'obtenir en testant de manière systématique toutes les combinaisons de NIP possibles. Une telle recherche peut toutefois demander un investissement en temps important; elle est par contre souvent grandement facilitée dans la mesure où la majorité des titulaires de cartes se contentent d'un NIP à quatre positions et/ou n'hésitent pas à utiliser un NIP «simpliste» tel qu'une partie de leur numéro de téléphone ou de la plaque d'immatriculation de leur véhicule ou encore une date de naissance.

Les délinquants intéressés à la fraude à la carte bancaire ont mis au point un système astucieux leur permettant non seulement de copier les données figurant sur les bandes magnétiques des cartes, mais également de prendre connaissance du NIP propre à chacune d'entre elles lors de retraits aux distributeurs automatiques de billets ou à essence. Cette technique nécessite la mise en place, respectivement l'utilisation, d'un certain nombre d'outils:

1. Leurre muni d'un lecteur de cartes: ce leurre se présente sous la forme d'un boîtier muni d'un lecteur de cartes capable de copier les bandes magnétiques. Il est fixé sur la fente du distributeur dans laquelle sont introduites les cartes. Il ne représente aucun obstacle aux opérations qu'entend faire le client auprès du distributeur.
2. Trompe-l'œil: Ce trompe-l'œil, aux couleurs d'organismes d'émission, dissimule une minicaméra – dont l'objectif est orienté sur le clavier par lequel sera introduit le NIP – et un système de transmission de données à distance.
3. Récepteur de fréquences et enregistreur digital: Ils permettent au délinquant de prendre connaissance en «live» ou de manière différée des données copiées et des NIP.
4. Encodeur de bandes magnétiques, ordinateur et logiciels adaptés.

9 Le système de transactions manuel est encore utilisé dans les petits commerces n'ayant pas les moyens financiers ou ne voyant pas l'intérêt d'acquérir les outils plus sophistiqués permettant les transactions électroniques.

6.4. Cartes «blanches» gaufrées

Grâce à l'utilisation d'une carte vierge gaufrée et à l'apposition d'une signature sur l'avis de vente, le délinquant peut acheter de la marchandise ou payer des services auprès de commerçants complices utilisant le système manuel (imprimante manuelle appelée aussi fer à repasser ou sabot).

La procédure de gaufrage vise à imprimer en relief et en creux sur la carte vierge un numéro de compte, une date de validité, des nom et prénom ainsi que le caractère de sécurité correspondant au numéro de compte. La carte pourra alors être embossée à l'aide d'un sabot et l'avis de vente aura une apparence tout à fait normale. La procédure de gaufrage nécessite l'utilisation d'un outil appelé machine à imprimer en relief ou machine à gaufrer, disponible légalement sur le marché.

7. Utilisation de contrefaçons

7.1. Buts poursuivis par le délinquant

Une certaine catégorie de délinquants cherchent avant tout à acheter frauduleusement de la marchandise de luxe ou de l'électronique auprès de commerçants dans le but de revendre ces produits sur le marché noir ou à des commanditaires particuliers. Pour ce faire, ils confectionnent des cartes de crédit d'apparence authentique en veillant à respecter l'ensemble des éléments des dispositifs de sécurité (tout du moins visibles à l'œil nu) mis en place par les organismes d'émission.

7.2. Types de contrefaçons

Le type de contrefaçons fabriquées et utilisées dépend de la forme des transactions possibles auprès du commerçant.

7.2.1. Transaction manuelle avec signature de l'avis de vente

L'utilisation d'une contrefaçon partielle, à savoir d'un support d'apparence authentique avec données physiques, est suffisante. Le délinquant doit toutefois veiller à reproduire sur l'avis de vente la même signature que celle figurant sur le panneau de signature de la carte.

Le nombre de commerçants opérant avec le système manuel tendant à se réduire fortement dans les pays industrialisés[9], les délinquants tendront, si tel n'est pas encore le cas, à abandonner la confection de contrefaçons partielles au profit de contrefaçons complètes.

7.2.2. Transaction électronique avec signature du justificatif de vente

L'utilisation d'une contrefaçon complète, à savoir d'un support d'apparence authentique avec données physiques et bande magnétique encodée, est nécessaire. Le délinquant doit ici aussi veiller à reproduire sur le justificatif de vente la même signature que celle figurant sur le panneau de signature de la carte.

7.3. Opérations et outils nécessaires à la confection de contrefaçons complètes

La confection de contrefaçons complètes aussi parfaites que possible demande au délinquant de faire preuve de créativité et de précision dans les opérations nécessaires, à savoir:

1. Confection du support, aux couleurs d'un organisme d'émission;
2. Encodage de la bande magnétique (avec des données authentiques, le cas échéant modifiées);
3. Gaufrage du support avec les données correspondant aux données enregistrées dans la bande magnétique, respectivement gaufrage de données personnelles et modification des données correspondantes dans la bande magnétique[10];
4. Métallisation, à savoir coloration, des données estampées sur le support;
5. Signature de la carte par la personne qui l'utilisera avec un nom correspondant à l'identité indiquée en relief sur la carte.

Pour l'ensemble de ces opérations, le délinquant utilise toute une série d'outils:

1. Ordinateur et logiciels adaptés;
2. Imprimante laser couleur, scanner numérique couleur et autres outillages permettant l'impression lithographique et sérigraphique;
3. Périphérique d'écrémage;
4. Encodeur de bandes magnétiques;
5. Machine à gaufrer;
6. Machine à métalliser;
7. Microscope, etc.

7.4. Pièces d'identité

Dotés d'un grand professionnalisme, certains délinquants cherchent également à se prémunir contre un éventuel contrôle d'identité de la part du commerçant. Cela étant, ils confectionnent ou se procurent des pièces d'identité correspondant aux noms et prénoms des titulaires estampés sur les contrefaçons.

7.5. Tendance

La confection du support en tant que tel, l'écrémage, l'encodage, le gaufrage, la métallisation et la confection de pièces d'identité sont des opérations qui nécessitent des compétences et des connaissances particulières que ne possède en principe pas une seule et même personne. Les différentes étapes du processus sont ainsi réparties entre plusieurs individus spécialisés dans un domaine particulier.

Les délinquants du continent asiatique (Indonésie, Malaisie, Taiwan, Hong-Kong et Chine notamment) sont sans aucun doute des maîtres en matière de fraudes à la carte de crédit et de contrefaçons. Il est très fréquent que les ébauches de supports soient fabriquées en Asie puis exportées vers le reste du monde où les contrefaçons sont alors personnalisées (gaufrage, métallisation, encodage, etc.) et utilisées frauduleusement.

S'il est vrai que certaines contrefaçons sont parfois fabriquées de manière artisanale par un petit groupe de personnes, il n'en demeure pas moins que certaines bandes et organisations criminelles ont créé de véritables industries de fabrication et gèrent leur réseau de distribution en professionnels.

8. Utilisation de cartes authentiques

8.1. Buts poursuivis par le délinquant

Les buts poursuivis par le délinquant peuvent être multiples: Achat de marchandises et paiement de services auprès de commerces ou d'automates ainsi que retrait d'argent aux distributeurs automatiques de billets. En fonction de l'objectif visé, le délinquant devra prendre connaissance du NIP ou être capable de reproduire une signature semblable à celle figurant sur le panneau de signature de la carte.

10 Le respect de la concordance entre les données personnelles sur le support et les données enregistrées dans la bande magnétique limite le risque que le commerçant ne s'aperçoive de la tentative de fraude en comparant les données figurant sur le support et les données imprimées sur la facturette par son terminal.

8.2. Moyens d'obtenir des cartes, respectivement le NIP qui leur est propre

8.2.1. Moyens classiques

Les moyens d'obtenir des cartes – valides ou périmées –, respectivement le NIP qui leur est propre, sont innombrables: vol sur le lieu de travail, vol à la tire dans les transports publics, vol par effraction ou par introduction clandestine dans un véhicule, un commerce ou une habitation, racket, vol de courrier au centre de tri postal ou dans la boîte aux lettres, etc.

N'étant pas rare que la victime ait noté le NIP sur la carte, au verso d'une photo ou sur un vulgaire bout de papier rangé dans son porte-monnaie, le délinquant est souvent facilement en possession non seulement de la carte, mais aussi du NIP qui lui est propre.

8.2.2. Commande frauduleuse de cartes de crédit

Le délinquant rédige une demande d'octroi de carte de crédit en usurpant l'identité d'une personne solvable. Pour ce faire, il prend connaissance des données personnelles nécessaires en se procurant du courrier adressé à la victime; une fois la demande adressée à l'organisme d'émission, il surveille la boîte aux lettres de sa victime et vole les courriers successifs contenant la carte de crédit et le NIP. Détenant entre ses mains une carte authentique non signée, le délinquant appose sa propre signature sur le panneau de signature au verso de la carte.

8.2.3. Vol à l'astuce. L'exemple du «collet marseillais»

En utilisant un «collet marseillais» et une gestuelle/des paroles induisant une confusion chez leur victime, les délinquants sont à même de se procurer des cartes bancaires et de crédit et le NIP qui leur est propre.

Le «collet marseillais»[11] est un leurre, muni d'un dispositif de retenue, que le délinquant fixe sur la fente d'introduction de la carte bancaire du distributeur automatique de billets et fait illusion sans un examen attentif. Lorsque le client se présente et insère sa carte, cette dernière est capturée par la boucle de rétention du leurre; le distributeur ne réagit donc pas. L'un des auteurs entre alors en scène et s'adresse à la victime en lui signifiant qu'il a lui-même connu le même problème précédemment; il l'incite à composer son code une nouvelle fois puis à appuyer sur la touche stop. Sous le couvert d'une argumentation fallacieuse (parfois en se référant à des affichettes justifiant d'un dysfonctionnement du système qu'il a lui-même collées aux abords du distributeur), il persuade la victime que l'appareil rencontre un problème technique et que la carte a été avalée; convaincue, la victime quitte les lieux en sa compagnie. Un complice s'empare alors de la carte capturée. Des retraits frauduleux sont ensuite opérés au moyen de la carte et du NIP dans les plus brefs délais.

8.2.4. Recherche du NIP

Lorsque le délinquant n'a pas pu prendre connaissance du NIP par l'un des moyens cités ci-dessus, il peut encore:

1. User de ruse et prendre contact avec la victime sous un faux prétexte. Par exemple, l'auteur téléphone à la victime en se faisant passer pour un employé de sa banque; il explique alors qu'il aurait besoin du NIP de la carte pour bloquer cette dernière;
2. Procéder à une recherche systématique.

8.3. Types d'utilisation des supports authentiques

8.3.1. Support laissé intact

Dans la plupart des cas, le délinquant se contente d'utiliser la carte valide telle quelle, à savoir sans procéder à la moindre modification du support. Il doit toutefois veiller, le cas échéant (en fonction du type de transaction), à apposer sur la facturette une signature identique à celle figurant sur le panneau de signature de la carte ou à utiliser le NIP propre à la carte.

8.3.2. Support falsifié

Le support peut être falsifié de trois manières différentes, en fonction des buts recherchés par le délinquant:

1. Support avec panneau de signature modifié: les délinquants peu habiles dans l'imitation de signatures et désireux de procéder à des transactions auprès de commerçants optent pour la seule modification du panneau de signature de la carte (valide).
2. Support avec bande magnétique nouvellement encodée: l'encodement de la bande magnétique d'une carte authentique au moyen

11 Appelé ainsi en raison de l'origine des délinquants qui ont utilisé en premier ce type d'astuce sur le continent européen.

de nouvelles données permet non seulement d'éviter que la carte soit rapidement inutilisable suite à son blocage par l'ayant-droit mais aussi, le cas échéant, de prolonger la validité d'une carte périmée.

3. Support nouvellement gaufré et métallisé: certains délinquants modifient le numéro de compte original – qui pourrait tôt ou tard figurer sur une liste de comptes bloqués –, changent la date d'échéance de la carte ou font correspondre les données estampées sur le support aux données personnelles figurant sur une fausse pièce d'identité ou sur une pièce d'identité authentique volée. Pour ce faire, ils éliminent la coloration noire des caractères estampés puis procèdent à l'écrasement de la carte afin de faire disparaître les données originales. Ils réimpriment ensuite en relief et en creux les données souhaitées, puis procèdent à la métallisation des caractères.

8.4. Pièces d'identité

Dotés d'un grand professionnalisme, certains délinquants cherchent également à se prémunir contre un éventuel contrôle d'identité de la part du commerçant. Ils confectionnent ou se procurent donc des pièces d'identité correspondant aux noms et prénoms des titulaires estampés sur les cartes.

9. Découverte et importance de la fraude

La fraude est généralement découverte dans les cas suivants:

- Lorsque le détenteur légitime de la carte reçoit le décompte mensuel relatif aux dépenses faites sur son compte et qu'il constate que des transactions ont été effectuées à son insu;
- Lorsque le détenteur légitime se voit refuser l'emploi (on-line) de sa carte pour «limite atteinte des dépenses mensuelles autorisées» alors qu'il n'a en aucun cas effectué des transactions pour un montant cumulé atteignant cette limite;
- Lorsque le titulaire légitime invite l'organisme d'émission à bloquer sa carte de crédit après avoir constaté son vol ou sa perte et que celui-ci lui communique que des transactions ont été effectuées sur son compte depuis la date du vol, respectivement de la perte;
- Lorsque le délinquant se présente avec une carte bloquée ou une carte dont la bande magnétique est encodée avec des données inexistantes auprès d'un commerçant ou d'un distributeur automatique de billets et que la transaction (de type on-line) est refusée par le serveur d'autorisation de l'organisme d'émission;
- Lorsque le commerçant examine les éléments du dispositif de sécurité, compare la signature apposée sur le panneau de signature avec la signature apposée sur l'avis de vente et vérifie l'identité du détenteur de la carte et qu'il constate une tentative de fraude;
- Lorsque l'organisme d'émission constate qu'une transaction a été effectuée avec des données fictives totales ou partielles;
- Lorsque le système de surveillance automatique mis en place par l'organisme d'émission détecte des transactions inhabituelles par rapport au profil du client.

Plus la durée entre le début et la découverte de la fraude est grande, plus les dommages sont importants. De manière générale, le montant du dommage est également d'autant plus grand que le titulaire légitime de la carte est toujours en possession de sa carte[12], respectivement qu'il ne s'attend pas à recevoir une nouvelle carte de crédit par courrier. En outre, le dommage peut être très élevé dans l'hypothèse où l'utilisation de la carte de crédit en question n'est pas sujette à une limite mensuelle maximum de dépenses.

10. Victimes de fraudes

Tout détenteur de carte de crédit est susceptible d'être victime de fraudes. Les personnes âgées sont certes une cible facile pour les vols à la tire ou par astuce, mais elles ne forment pas la catégorie principale de victimes. En effet, en matière de cartes de crédit, les victimes n'ont pas de profil particulier. Ainsi, même la personne la plus diligente n'est pas à l'abri que son numéro de compte soit purement et simplement créé par un programme générateur de numéros valides et utilisé frauduleusement pour une commande par correspondance.

12 En 2003, les pertes dues au «skimming» se seraient élevées à quelque 0,08% du chiffre d'affaires des organismes d'émission.

11. Auteurs de fraudes

11.1. Auteurs agissant seuls ou en bande

11.1.1. Les auteurs amateurs et d'occasion

Ces auteurs, principalement des hommes âgés de 16 à 40 ans, commettent leurs méfaits en mettant à profit leurs connaissances rudimentaires du monde des cartes de crédit. Peu sûrs d'eux et stressés, ils cherchent à atteindre leur objectif le plus rapidement possible et n'hésitent pas à accélérer si nécessaire la transaction, par exemple en refusant tout conseil du commerçant ou la rédaction de la garantie de l'objet acquis.

Ils procèdent entre autres à des achats de marchandises sans nécessité/logique apparente (par exemple des achats en masse du même bien).

Si besoin est, ils usent de violence physique contre la victime pour obtenir la carte, respectivement le NIP (par exemple vol à la tire ou retrait de la carte au distributeur automatique de billets) ou de violence verbale envers le commerçant qui examinerait de trop près la carte de crédit présentée.

Finalement, leur apparence physique est négligée et il n'est pas rare que leur tenue vestimentaire soit pour le moins inhabituelle du commerce fréquenté.

11.1.2. Les auteurs professionnels

Ces auteurs, des hommes et des femmes «plutôt intelligents» âgés de 20 à 60 ans, commettent leurs méfaits en mettant à profit leurs connaissances pointues du monde des cartes de crédit. Sûrs d'eux, ils cherchent à atteindre leur objectif sans éveiller le moindre soupçon, en adoptant un comportement le plus naturel possible – en acceptant le cas échéant les conseils du commerçant – et en procédant à des achats qui puissent correspondre à leur profil.

D'apparence élégante et inspirant la confiance, ils n'ont pas besoin de faire preuve de violence pour arriver à leurs fins.

11.2. Organisations criminelles[13]

Les organisations criminelles se caractérisent par une structure en principe compartimentée/cloisonnée donnant à chacun de leurs membres un rôle très précis qui en fait de véritables spécialistes d'un domaine particulier. Leur force repose sur la gestion professionnelle de leurs activités ainsi que sur leur réseau de contacts au niveau international (y compris avec d'autres groupes impliqués dans des activités criminelles en tout genre). Dotées de connaissances pointues en matière de cartes de crédit, les organisations criminelles mettent tout en œuvre pour maximiser leur profit.

12. Exemples de mesures permettant la réduction des opportunités de fraudes

12.1. Campagne de prévention à large échelle

Si la fiabilité et l'efficacité des composants techniques des cartes de crédit et moyens de transactions sont indispensables, il n'en demeure pas moins que le facteur humain représente fréquemment une faille importante du système. Les détenteurs légitimes et les commerçants doivent donc impérativement être rendus attentifs à l'ampleur des fraudes à la carte de crédit et aux mesures de sécurité élémentaires à respecter. Il s'agit d'éviter que la sécurité assurée par des technologies avancées soit mise à néant par la négligence des différents partenaires.

12.2. Mesures au sein des organismes d'émission

A l'heure actuelle, les organismes d'émission renoncent, en principe pour des raisons de coût, à l'envoi recommandé des courriers contenant les cartes de crédit, respectivement le NIP propre à ces cartes. Conscients de ce manque évident de sécurité, les émetteurs ont développé un système dit de «l'activation de la carte par le titulaire»[14], utilisé dans certaines circonstances. Or, pour que les vols de courriers ne représentent plus aucun intérêt pour les délinquants, il est important que les organismes généralisent cette nouvelle procédure.

Soucieux de détecter au plus vite certaines fraudes et de minimiser les pertes qui en résultent, les organismes d'émission ont mis au point des systèmes automatiques de surveillance des transactions on-line fonctionnant sur la base de profils-clients. Ces systèmes sont programmés de telle manière qu'ils réagissent principalement lorsque des transactions sont effectuées en des lieux très éloignés sur une période de temps rapprochée ou lorsque des transactions sont haute-

13 Ce terme doit être compris dans son sens large et non pas au sens restreint de l'art. 260ter CPS.

14 Le titulaire doit contacter l'organisme d'émission dès réception de sa carte et doit répondre à un certain nombre de questions permettant son identification; ce n'est qu'après cette vérification que la carte est activée.

ment inhabituelles par rapport aux profils établis. Pour une plus grande efficacité, ces systèmes devraient toutefois être utilisés de manière plus rigoureuse afin de bloquer provisoirement les comptes concernés aussitôt que des transactions sortant des profils-clients sont détectées.

12.3. Contrôle du lien entre l'individu et la carte

La faculté des délinquants à imiter une signature ou à découvrir (sans avoir besoin de recourir à la victime) le NIP à quatre positions propre à une carte ne doit pas être négligée. Il serait dès lors judicieux d'exclure les transactions avec signature du justificatif et d'imposer aux détenteurs légitimes l'adoption d'un NIP à six positions, lequel serait exigé pour toutes les transactions.

L'utilisation de NIP à six positions n'excluant toutefois pas que le délinquant prenne connaissance du NIP en usant d'astuce ou de violence, le lien existant entre le détenteur et la carte pourrait être contrôlé par le recours à la biométrie, c'est-à-dire à des technologies d'identification des personnes par mesure de leurs caractéristiques physiques uniques (par exemple les empreintes digitales).

L'ajout d'une photographie personnelle sur la carte, comme proposé par certains organismes d'émission à leurs clients, constitue certes un élément supplémentaire du dispositif de sécurité, mais son effet pervers ne doit pas être négligé: Le commerçant sera dorénavant tenté de se fier uniquement à la photographie sur le support et de ne plus procéder aux autres contrôles pourtant prescrits.

En ce qui concerne les transactions par Internet, les organismes d'émission se doivent de mettre en place des systèmes permettant de minimiser au maximum les risques de fraudes pour les exploitants de plates-formes de commerce électronique (par exemple, soumettre chaque transaction à la saisie préalable d'un mot de passe par le détenteur de la carte et à une vérification directe de celui-ci auprès de la centrale d'émission par l'exploitant).

12.4. Abolition des transactions manuelles et off-line et amélioration du système on-line

Les transactions manuelles offrent des opportunités de fraudes telles que leur remplacement par les transactions avec système électronique on-line est un impératif.

Le système électronique off-line dans sa conception actuelle devrait lui aussi être abandonné au profit du système on-line, beaucoup plus sûr. Si ce dernier offre des avantages certains dans la lutte contre les fraudes, il n'en demeure pas moins qu'il n'est pas exempt de brèches. Il a par exemple le grand inconvénient de ne pas permettre la vérification du lien existant entre les données enregistrées dans la bande magnétique et celles figurant sur le support; les fraudes au moyen de cartes encodées de données copiées («skimming») ne sont donc pas exclues. Le système on-line devrait dès lors être adapté de manière à réduire au maximum les opportunités de fraudes.

Enfin, l'effectivité du blocage des cartes au niveau mondial prend encore trop de temps. Les organismes d'émission devraient ainsi veiller à tirer au maximum profit des possibilités offertes par les nouvelles technologies.

12.5. Abandon des bandes magnétiques

Introduites dans la seconde moitié des années 1960, les bandes magnétiques ont perdu leur (soi-disant) caractère inviolable depuis que les pirates informatiques et autres passionnés ont été capables de lire et de modifier les données qui y sont enregistrées. L'abandon progressif (dans les prochaines années) de l'utilisation de la bande magnétique au profit du microprocesseur, communément appelé «puce», permettra de palier aux nombreuses lacunes de sécurité des bandes magnétiques. Le microprocesseur offre en effet – théoriquement – une parfaite protection. Des brèches de sécurité ne sont toutefois pas exclues si les moyens nécessaires au développement et à la fabrication des puces ainsi qu'à l'adoption de procédures adaptées de transactions ne sont pas investis. En outre, les fraudes ne pourront pas être réduites de manière significative tant que certains terminaux et distributeurs seront uniquement capables de lire les bandes magnétiques (lesquelles subsisteront en parallèle aux puces aussi longtemps que le parc de machines ne sera pas remplacé dans son intégralité).

13. Conclusion

Les dispositifs de sécurité mis en place par les organismes d'émission sont toujours plus sophistiqués. Toutefois, l'accès à l'information sur Internet ainsi que la disponibilité et le coût tou-

jours moins élevé du matériel informatique et électronique ainsi que des logiciels permettent aux délinquants d'être rapidement et relativement facilement à même de contrer ces dispositifs. Ainsi, même si, pour l'heure, les algorithmes utilisés pour crypter certaines données enregistrées dans les bandes magnétiques n'ont toujours pas été cassés, les délinquants ont réussi à tirer profit des faiblesses du système.

La lutte contre la fraude en matière de cartes de crédit est un défi qui nécessite une coopération intensive des émetteurs de cartes, des différents partenaires (détenteurs de cartes, commerçants, etc.) ainsi que des forces de police et des autorités judiciaires aux niveaux tant régional, national qu'international. Cette coopération est indispensable pour faire face à la mobilité et à l'ingéniosité des délinquants et des organisations criminelles qui chercheront et exploiteront tant qu'ils le pourront les différentes failles de sécurité.

En résumé, la lutte contre la fraude à la carte de crédit doit passer par l'harmonisation législative au niveau international, par des programmes de prévention à large échelle auprès des détenteurs de cartes et des commerçants, par le développement de systèmes de transactions et de dispositifs de sécurité performants ainsi que par des mesures spécifiques offrant, le cas échéant, une base solide au travail des autorités répressives et pénales (par exemple, l'installation systématique de caméras vidéo de haute performance aux distributeurs automatiques de billets).

Bibliographie

Lakeman P.J. et Knopjes F., *Chip Card: Trump Card?, The situation as it stands in the world of cards,* 1998 (disponible sous www.interpol.int).

Oberson P.-A., *Les moyens électroniques de paiement orientés vers le particulier,* Thèse, Lausanne, 1994.

Queloz N., Borghi M. et Cesoni M. L., *Processus de corruption en Suisse,* Helbing & Lichtenhahn, Bâle/Genève/Munich, 2000.

Slotter K., Plastics Payments. Trends in Credit Card Fraud, *FBI law enforcement bulletin,* June 1997, Vol. 66, 6, 1–7.

Steinmann M., *Kundenidentifikation durch Code und ihre rechtliche Bedeutung im Bankwesen,* Thèse, Zurich, 1994.

Stoll D., *Les cartes et moyens de paiements analogues. La répression des abus et des fraudes en droit pénal suisse,* Recherches juridiques lausannoises, Zurich, 2001.

Documentation

a. Brochures d'informations:

accept, Le magazine des clients de Telekurs Multipay SA, édition 01/03.

Europay News, mai 2001.

Police cantonale vaudoise, *La monnaie plastique,* dépliant édité dans le cadre du programme de prévention de la criminalité, août 2002.

b. Communiqués de presse:

Communiqués du Commandant de la Police cantonale vaudoise du 18 octobre 2002, du 17 septembre 2002, du 28 janvier 2003, du 17 février 2003 et du 8 juillet 2003.

Communiqué de Multipay (Switzerland) SA du 2 juillet 2002.

c. Rapports:

Global Internet Solutions, *Rapport accablant sur la réalité de la fraude à la carte bancaire sur l'internet en France et en Europe,* mai 2003, disponible sous http://84.96.22.16/epaysecurity/rapport2003.html

Security command centre NSW police Service, *Fraud prevention during the Sydney 2002 OG,* document présenté à la Fraud Prevention and Control Conference, 24–25 août 2000.

d. Articles de presse:

Le Monde informatique, *Toujours une sécurité de retard,* article n° 956 du 25 octobre 2002.

Sciences et Avenir, Dossier relatif aux cartes bancaires, septembre 2003, 42–47.

ZDNet.fr, *La carte bancaire toujours vulnérable par sa piste magnétique,* article publié le 12 septembre 2002 et disponible sous http://www.zdnet.fr/actualites/technologie/0,39020809,2136183,00.htm

ZDNet.fr, *Un rapport parlementaire réclame une nouvelle loi sur la biométrie,* article publié le 18 juin 2003 et disponible sous http://www.zdnet.fr/actualites/technologie/ 0,39020809,39122994,00.htm

e. Sites Internet:

httpwww.cba.ca

http://www.geneve.ch/police/welcome.html

httpwww.incodenet.com

http://parodie.com/monetique/listevulnerabilites.htm

http://parodie.com/monetique/hacking.htm

http://www.rcmp-grc.gc.ca/crimint/cardcrime-f.htm

http://www.securiteinfo.com/attaques/divers/cartes-magn.shtml

http://www.telekurs-multipay.com/

http://84.96.22.16/epaysecurity/FRhome.html

Marylaure GARCIA
HEG Haute école de gestion Arc
50, rue de Sainte-Hélène
CH-2009 Neuchâtel
marylaure.garcia@freesurf.ch