Université de Montréal

LES MOYENS DE LUTTE CONTRE LA FRAUDE À LA TÉLÉPHONIE MOBILE : ÉTUDE DE CAS D'UNE ENTREPRISE DE TÉLÉCOMMUNICATION CANADIENNE

par

Lise LeChi Tran

École de criminologie

Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maître ès sciences (M. Sc.)
en criminologie

Avril, 2005

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

LES MOYENS DE LUTTE CONTRE LA FRAUDE À LA TÉLÉPHONIE MOBILE : ÉTUDE DE CAS D'UNE ENTREPRISE DE TÉLÉCOMMUNICATION CANADIENNE

présenté par :
Lise LeChi Tran

a été évalué par un jury composé des personnes suivantes :

Benoît Dupont, président-rapporteur
Jean-Luc Bacher, directeur de recherche
Véronique Parent, membre du jury

MÉMOIRE ACCEPTÉ LE : 5 août 2005

RÉSUMÉ

Cette étude analyse les réactions d'une entreprise canadienne de télécommunication sans fil vis-à-vis deux formes de fraude à la téléphonie mobile. Il y a d'abord la fraude au forfait prépayé. Elle se commet par l'utilisation non autorisée de numéros de cartes de crédit valides pour l'achat de cartes téléphoniques prépayées. Ensuite, il y a la fraude au forfait mensuel. Elle se réalise par l'usurpation de l'identité d'une personne solvable lors de la souscription à un abonnement mensuel.

Les moyens de lutter contre la fraude et qui sont susceptibles de réduire les opportunités criminelles sont analysés : prévention, détection et intervention.

Les résultats de cette recherche indiquent que les moyens déployés par l'entreprise ont des résultats qui varient selon le type de fraude. La fraude au forfait prépayé est presque été enrayée. En revanche, la vulnérabilité et les difficultés de dépistage offrent encore des opportunités en matière de fraude au forfait mensuel. Pour combattre la fraude à la lumière des techniques de prévention situationnelle, l'idéal serait de combiner la prévention, la détection et la répression. Or, l'entreprise ne fait pas appel à la répression en raison de son attitude qui découle d'une rationalité commerciale plutôt que d'une rationalité de justice.

Des recommandations sont faites pour améliorer le dépistage de la fraude et réduire l'accessibilité aux services de téléphonie mobile au sein de l'entreprise.

Mots-clés : Fraude à la téléphonie mobile, fraude cellulaire, fraude, télécommunications sans fil, téléphone portable, cellulaire, vol d'identité, carte de crédit, prévention, détection, prévention situationnelle.

ABSTRACT

This research examines the reaction of a Canadian telecommunication company in order to tackle two forms of fraud: prepaid and subscription fraud. The first type of fraud consists of stealing credit card numbers to buy prepaid services and the second type of fraud consists of stealing personal information to subscribe to a monthly service without the intention to pay.

Organizational countermeasures which are to reduce criminal opportunities such as prevention, detection and intervention are considered.

The results of this study point out that organizational countermeasures have shown different results depending upon the type of fraud in question. Prepaid mobile phone fraud has been almost eliminated. On the other hand, vulnerabilities and difficulties in detection still provide opportunities with regard to subscription frauds on monthly services. To tackle fraud according to techniques of situational crime prevention, the ideal would be a mixture of prevention, detection and repression. However, the company does not call upon repression because of its attitude, which comes from a commercial rationality rather than a rationality of justice.

Recommendations are made to improve detection of fraud and reduce the accessibility to mobile phone services within the company.

Keywords: Mobile phone fraud, fraud, cellular fraud, wireless telecommunication, mobile phone, cellular phone, theft identity, credit card, prevention, detection, situational prevention.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET DES ABRÉVIATIONS

1G : première génération

2G : deuxième génération

3G : troisième génération

ACTS : Association canadienne des télécommunications sans-fil

AMPS : American Mobile Phone System

AuC : Authentification Center

BTS : Base Transceiver Station

CDMA : Code Division Multiple Access

CDR : Call Detail Report

CFCA : Communication Fraud Control Association

CRTC : Conseil de la radiodiffusion et des télécommunications canadiennes

CTIA : Cellular Telecommunications & Internet Association

CVC : Code de vérification de la carte

DRHC : Développement des ressources humaines Canada

ESN : Electric Serial Number

FCC : Federal Communication Commission

GSM : Global System for Mobile Communications

IAC : Institut australien de criminologie

IP : Internet Protocole

LPRPDE : Loi fédérale sur la protection des renseignements personnels et les documents électroniques

MIN : Mobile Identification Number

PIN : Personnal Identification Number

SCP : Services de communications personnelles

SIM : Subscriber identification mobile

SVA : Service de vérification d'adresse

TDMA : Time Division Multiple Access

UMTS : Universal Mobile Telecommunication System

WPTA : Wireless Telephone Protection Act

REMERCIEMENTS

La réalisation de ce mémoire n'aurait pas été possible sans la précieuse collaboration de plusieurs personnes. D'abord, toute ma gratitude va à mon directeur de recherche, Monsieur Jean-Luc Bacher, pour avoir accepté de diriger ce travail de fin d'études et pour l'intérêt qu'il a porté à tout au long de sa réalisation. Je lui suis reconnaissante pour la qualité de ses commentaires et sa grande patience.

Ensuite, cette recherche est tout particulièrement dédiée à celui qui a accepté le projet initial, l'ancien directeur du Service de la fraude de l'entreprise étudiée (que je ne peux nommer afin de conserver l'anonymat de l'entreprise). Je lui souhaite beaucoup de succès en Grande-Bretagne.

De même, je remercie les professeurs suivants pour les conseils et les encouragements dont ils m'ont fait durant le dernier droit de cette recherche: André Cellard de l'Université d'Ottawa, Adelle Danovich de l'Université de Montréal et Carol Reid du Collège John Abbott.

Je profite également de l'occasion pour remercier chaleureusement mes parents, mon frère Steve, ma tante Nguyet et mes amis pour leur support moral.

Enfin, je remercie Daniel Desrochers, le réviseur qui m'a lue et relue.

INTRODUCTION

Au cours deux dernières décennies, les technologies de communications mobiles ont connu un développement considérable. Bien que ce domaine comporte de nombreux aspects positifs en termes de commodité, de productivité et de sentiment de sécurité, il a néanmoins permis l'émergence de nouveaux " espaces criminels ". En effet, si la majorité des abonnés au cellulaire payent les services obtenus auprès des fournisseurs de télécommunications sans fil, il n'en demeure pas moins que certains " malfaiteurs " et " organisations criminelles " cherchent à obtenir ces services par le biais de supercheries. Considérées par l'industrie du sans-fil comme un phénomène en pleine expansion, les fraudes par cellulaire font perdre des millions, voire des milliards de dollars aux entreprises de télécommunications en Amérique du Nord. L'augmentation de la prévalence de la fraude et le développement des moyens de la contrer sont des thèmes qui préoccupent les entreprises de télécommunications sans fil. De leur côté, les employés de ces entreprises en charge de lutter contre la fraude sont démunis face aux difficultés d'ordre technologique, institutionnel et juridique qui entravent leur lutte.

Ce mémoire sera divisé en quatre chapitres. Dans le premier chapitre, il sera question de l'état actuel des connaissances sur l'objet d'étude. Nous présenterons brièvement l'évolution de la téléphonie mobile de même que les caractéristiques des services de communications sans fil de première, de deuxième et de troisième génération. Après avoir défini le concept de fraude à la téléphonie mobile, nous exposerons les diverses formes de fraudes qui victimisent les entreprises de télécommunications sans fil. Par la suite, nous examinerons l'ampleur du phénomène ainsi que les facteurs explicatifs de la fraude. Enfin, nous traiterons des différents moyens utilisés par les opérateurs de téléphonie mobile pour prévenir et contrer la délinquance cellulaire.

Nous exposerons la démarche méthodologique dans le deuxième chapitre. Afin de comprendre en profondeur le cas de l'entreprise étudiée, nous avons conçu une triple stratégie de recherche, dont les volets ont été développés en parallèle de façon complémentaire. Nous avons d'abord effectué des observations participantes sur une période

de quatre ans auprès des employés d'une entreprise canadienne de télécommunications. Ces employés, dans le cadre de leurs activités quotidiennes, mènent des activités de surveillance et de dépistage des escrocs du cellulaire. Nous avons ensuite recueilli quelques données statistiques qui tracent un portrait du phénomène de la fraude au sein de l'entreprise. Puis, des entretiens semi-dirigés sont venus enrichir le contenu des observations et des données obtenues. Après avoir justifié, sur le plan méthodologique, le choix du terrain de recherche, du cas à l'étude et du type d'entrevues que nous avons réalisées, nous établirons la stratégie d'analyse de cette étude de cas, pour finalement évoquer les limites auxquelles cette recherche s'est heurtée.

Dans le troisième chapitre, il s'agira de présenter et d'analyser les données résultant des observations et des entretiens semi-directifs réalisés au sein de l'entreprise de téléphonie mobile à l'étude, en mettant notamment en exergue les différentes perceptions des acteurs relativement à la lutte contre la fraude. D'abord, quelques données sur la nature et les types de fraudes recensées au sein de l'entreprise seront présentées. Ensuite, les pratiques corporatives quant aux moyens déployés au niveau de la prévention et de détection seront décrites. Enfin, les résultats en matière de fraude de l'entreprise en regard de sa situation et des finalités de sa politique seront soumis à une appréciation.

Dans le quatrième et dernier chapitre, s'amorcera une discussion des résultats issus des observations participantes et des entretiens semi-directifs à la lumière des connaissances et des approches théoriques présentées dans la recension des écrits. Une conclusion ainsi que des recommandations complèteront cette étude de cas.

CHAPITRE 1 : ÉTAT DES CONNAISSANCES

Beaucoup de chercheurs en criminologie se sont penchés sur une forme particulière de fraude, mais très peu d'attention a été accordée, du moins de façon systématique, à la fraude à la téléphonie mobile. Bien que la documentation sur ce thème s'accroisse depuis 1996, le bilan bibliographique montre à quel point les études sur cette nouvelle forme de criminalité économique sont peu nombreuses. En effet, les chercheurs intéressés par l'étude de la criminalité en matière de téléphonie mobile et des réactions qu'elle suscite sont plutôt rares. Il convient toutefois de mentionner les chercheurs australiens. L'essentiel de la recherche sur le thème qui nous intéresse provient de l'Institut australien de criminologie (IAC). Elle a été entreprise au cours de la deuxième moitié des années 1990. En ce qui a trait à la production canadienne, les articles sont rares et, de surcroît, trop sommaires pour mériter toute comparaison. Les écrits des Américains sont cependant un peu plus nombreux et substantiels. Outre les articles de l'IAC qui constituent les principaux travaux de nature proprement criminologique, nous présentons dans ce chapitre des articles émanant de journalistes, de gens des milieux d'application de la loi et de personnes qui s'expriment en raison de leur expertise dans le domaine du sans-fil.

Notre recension des écrits se présente comme suit : elle nous amènera d'abord à faire un bref survol de l'évolution et des caractéristiques des systèmes de communications sans fil. Puis, pour distinguer les diverses formes de fraude, une typologie des délits sera présentée. Dans le point suivant, nous examinerons l'ampleur du phénomène ainsi que les facteurs explicatifs de ce crime. Ensuite, nous ferons état des écrits qui analysent les différents moyens dont usent les opérateurs de téléphonie mobile pour prévenir cette nouvelle forme de criminalité qu'est la délinquance cellulaire et lutter contre elle. En dernier lieu, une des théories contribuant à l'explication des stratégies déployées contre la fraude au cellulaire sera présentée. Nous clôturons le premier chapitre avec la problématique de notre étude.

Considérons d'abord l'évolution de la téléphonie mobile et les caractéristiques des systèmes de communications sans fil.

1. VERS UNE NOUVELLE ÈRE DES COMMUNICATIONS MOBILES

1.1 ÉVOLUTION DE LA TÉLÉPHONIE MOBILE

Depuis le lancement de l'ancienne technologie analogique cellulaire au début des années 1980, les progrès en matière de communications sans fil ont connu un essor considérable. Charles E. Hoffman, chef de la direction de Rogers AT&T Communications sans fil, observe à ce propos :

> " On a assisté à une évolution spectaculaire de ce moyen de communication, passant de l'affreux et encombrant appareil des débuts à celui d'aujourd'hui, véritablement portable et qui offre aux clients une communication de qualité supérieure tout en lui fournissant l'accès à l'information, au courrier électronique, à l'Internet, et plus encore. " (Hoffman, 2000 :10)

Actuellement, le marché du sans-fil s'oriente vers la combinaison des technologies cellulaires et informatiques (Mondoux, 2000a) et, en ce qui a trait à la téléphonie du troisième millénaire, Gabriel Sigrist, journaliste du quotidien *Le Temps* (en Europe) écrit :

> " L'arrivée de la transmission de données à haut débit dans les téléphones mobiles annonce une révolution aussi importante que celle qu'a représentée le développement d'Internet pour les ordinateurs de bureau. " (Sigrist, Page Web)

Ainsi, les technologies futures de communications mobiles auront la particularité d'offrir aux usagers un accès mobile à des vitesses considérablement plus élevées que celles que nous connaissons actuellement et d'introduire une façon entièrement nouvelle de communiquer, d'accéder à l'information et de mener des affaires (ACTS - Association canadienne des télécommunications sans-fil, Page Web).

Un premier concept qui sera utilisé dans le cadre de ce mémoire est celui d'" entreprises de télécommunications sans fil ". Il désigne de manière générale le " propriétaire ou exploitant d'une installation de transmission grâce à laquelle sont fournis par lui-même ou une autre personne des services de télécommunications au public moyennant contrepartie ".

Telle est la définition du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC, Page Web). D'autres appellations sont également utilisées pour désigner ces entreprises : *entreprises de télécoms, fournisseurs de téléphonie mobile, opérateurs du sans-fil, opérateurs de réseaux cellulaires.* Au Canada, l'industrie de la téléphonie cellulaire regroupe les quatre principales entreprises de télécommunications sans fil suivantes : Bell Mobilité, Rogers AT&T Communications Sans fil, Microcell Telecommunications Inc. ainsi que Telus.

Il serait trop fastidieux et complexe d'expliquer les détails techniques des principes de fonctionnement des réseaux de téléphonie sans fil. Pour les fins de la présente étude, il s'agit de distinguer sommairement les fonctionnalités et les particularités des différents modes de transmission des services de communications mobiles. Outre les aspects technologiques, nous présenterons les formes d'abonnement car elles auront également leur pertinence pour la compréhension des divers types de fraudes.

1.2 LES SERVICES CELLULAIRES ANALOGIQUES (PREMIÈRE GÉNÉRATION)

Les services cellulaires analogiques (mieux connus sous AMPS, *American Mobile Phone System*) ont été introduits en 1983 aux États-Unis (Clarke et al., 2001; Committee of the Judiciary, Page Web) alors qu'au Canada, elles sont apparues en 1985 (Microcell Telecommunications Inc., 2001:3). Cette ancienne technologie qualifiée de *première génération du sans-fil* (1G) a comme particularité de ne transporter que de la voix, c'est-à-dire de refléter les modulations de la voix humaine dans les radiofréquences transmises par les ondes, alors que la possibilité de transmettre des données est très limitée (ACTS, Page Web).

Pour qu'une communication soit effectuée, les téléphones cellulaires analogiques doivent avoir deux composantes principales. La première, le numéro de série électronique interne (ou ESN, de l'anglais *Electric Serial Number*), identifie le manufacturier du téléphone de même que le numéro de série de l'appareil. La seconde composante est le numéro de téléphone assigné à un abonné (ou MIN, de l'anglais *Mobile Identification Number*) (Beseler, 1997; Clarke et al., 2001; Delaney, 1993; Smith, 1996b). Au moment de

recevoir ou de transmettre des appels, ces deux composantes sont envoyées à la station de base (*ou* BTS, de l'anglais *Base Transceiver Station*) la plus proche. Cette dernière vérifie si l'utilisateur du sans-fil est un abonné autorisé. Une fois que l'appel est lancé, les numéros indiquent à la station de base de l'opérateur qui doit être facturé (Smith 1996b).

Les services cellulaires traditionnels reposent sur un mode de transmission par lequel la plate-forme émet un signal électrique continu (ondes sonores ou signaux radio) (ACTS, Page Web). Comme la station de base est elle-même reliée à une tour hertzienne, les signaux envoyés par la voie des ondes hertziennes peuvent être facilement captés et interceptés, ouvrant ainsi la porte à l'écoute indiscrète et aux fraudes (O'Brien, 1998), thème sur lequel nous aurons l'occasion de revenir à la section 2.1.3.1.

1.3 LES SERVICES CELLULAIRES NUMÉRIQUES OU SCP – SERVICES DE COMMUNICATIONS PERSONNELLES (DEUXIÈME GÉNÉRATION)

Quant à la deuxième génération de réseaux sans fil (2G), appelée *services de communications personnelles* (SCP), elle a été conçue au début des années 1990 (Microcell, Opus, 2001:3). Au Canada, ce n'est cependant qu'en 1995 que les premiers réseaux numériques ont été inaugurés (ACTS, Page Web). À l'heure actuelle, il existe trois principales normes (ou protocoles) de SCP sur le marché canadien : GSM (*Global System for Mobile Communications*), le protocole utilisé par Microcell Telecommunications Inc. et Rogers AT&T, CDMA (*Code Division Multiple Access*), utilisé par Bell Mobilité et Telus et TDMA (*Time Division Multiple Access*), anciennement utilisé par Rogers AT&T. Précisons toutefois que le protocole GSM est la norme numérique la plus répandue au monde et le protocole standard en Europe (Dubowski, 2001; Mondoux, 2000b). Pour leur part, les protocoles TDMA et CDMA sont tous les deux des normes nord-américaines dérivées de la norme AMPS (*American Mobile Phone System*) qui est une norme analogique, utilisée au Canada et aux États-Unis (Mondoux, 2000 b).

Les communications des téléphones numériques utilisent les ondes radio comme les téléphones cellulaires (Mondoux, 2000b). L'utilisation d'un protocole entièrement numérique faisant appel à des procédures de chiffrement qui encodent le signal (cryptographie) est ce qui les distingue de l'ancienne technologie analogique cellulaire. Les

réseaux SCP transforment tous les signaux en une série de bits numériques, ce qui assure une communication plus sécuritaire (Smith 1996b). Plus précisément, la transmission numérique des communications permet, entre autres, aux abonnés du sans-fil de communiquer en toute confidentialité, c'est-à-dire à l'abri de l'écoute indiscrète (ACTS, Page Web) et rend le piratage cellulaire beaucoup plus difficile (Natarajan et al., 1995). Parmi les autres avantages de la technologie numérique, citons la sonorité cristalline supérieure, moins sujette à interférences (ACTS, Page Web) ainsi que la capacité de transmettre des données en plus de la voix (Mondoux, 2000b). En effet, en plus des services téléphoniques, les SCP offrent à leurs usagers une gamme de services optionnels que n'offrait pas l'ancienne technologie cellulaire : la messagerie de télécopie, la messagerie texte, la boîte vocale évoluée1[1], la gestion des appels, les appels en attente, l'afficheur (ou l'identification de l'appelant), l'accès à l'information, au courrier électronique, à l'Internet sans fil, etc. (Hoffman, 2000).

Cependant, bien que la technologie cellulaire numérique offre des services évolués, elle n'est pas forcément disponible en dehors des grandes villes. Par exemple, pour assurer une couverture transparente qui s'étend au-delà des régions urbaines, Microcell Telecommunications Inc. offre aux abonnés de " sans-fil " un appareil numérique bimode, c'est-à-dire la possibilité d'utiliser le téléphone à la fois sur les bandes de fréquences analogiques et numériques (Microcell Telecommunications Inc). Chez Rogers AT&T, lorsque les utilisateurs du SCP numérique se déplacent à l'extérieur de la zone de couverture numérique, leurs appels sont automatiquement pris en charge par le réseau analogique (Rogers AT&T, Page Web).

1.4 LES SERVICES MOBILES UMTS (TROISIÈME GÉNÉRATION)

Tout comme dans le domaine de la technologie de l'information, le marché de la communication mobile ne peut s'accommoder longtemps d'une grande diversité des normes. C'est ainsi que les principaux joueurs de la téléphonie cellulaire ont entamé plusieurs pourparlers afin de mettre sur pied une norme numérique " universelle " de réseaux cellulaires, nommé UMTS (Universal Mobile Telecommunication System), ou 3G (troisième

[1] La boîte vocale évoluée permet de rappeler les correspondants sans quitter la messagerie vocale. Il est également possible d'envoyer ou d'acheminer des messages vocaux à un ou à plusieurs abonnés de façon simultanée, sans toutefois déclencher la sonnerie de leur appareil.

génération), qui permet la compatibilité, ou interopérabilité, entre les différentes normes numériques actuellement en place (Mondoux, 2000ab). L'Association canadienne des télécommunications sans fil (ACTS, Page Web) est d'avis que la technologie de la troisième génération représente la prochaine ère de la communication et qu'elle tendra à mettre sur pied des normes numériques universelles à haut débit. Après la technologie numérique de deuxième génération (SCP), qui utilise le principe des ondes radio à moyenne fréquence, l'ACTS s'attend à ce que l'avènement des technologies 3G mette à contribution une technologie universelle à haute fréquence. Les téléphones mobiles de troisième génération permettront aux utilisateurs du sans-fil d'accéder à des services Internet, de magasiner et de réaliser leurs opérations bancaires à des vitesses considérablement supérieures[2] à celles actuellement offertes (ACTS, Page Web). Parmi les fonctionnalités envisagées avec ces appareils révolutionnaires, citons le téléchargement de musique, la messagerie électronique (Richardson, 2000), la vidéoconférence, les jeux en réseau, la géolocalisation, c'est-à-dire la possibilité d'être repéré rapidement en cas d'accident ou encore de connaître rapidement l'emplacement précis d'un endroit (Landry, 2001).

1.5 LES DIVERS MODES D'ABONNEMENT DES USAGERS DU SANS-FIL

Pour entrer dans l'univers des communications mobiles, les utilisateurs de sans-fil ont le choix entre deux types d'abonnement. La première porte d'entrée consiste à choisir un abonnement " mensuel " ou " postpayé ". Les fournisseurs de services préfèrent vendre ce plan mensuel fixe dont les frais à la minute sont généralement de 20 cents et moins. Ce type d'abonnement comporte toutefois une vérification de crédit et une facture mensuelle. En revanche, pour ceux qui n'ont pas de bons dossiers de crédit, qui prévoient de faire une utilisation épisodique de leur téléphone mobile ou de restreindre leur consommation d'appels téléphoniques, ou qui ne veulent ni contrat ni facture mensuelle, il y a l'autre option qui consiste à choisir un forfait " prépayé " ou " à la carte ". Mais, cette option permettant d'acheter des minutes " à la carte " entraîne des frais plus élevés, qui peuvent aller jusqu'à 50 cents la minute (Bernatchez, 2000).

---

[2] La troisième génération devrait comporter des vitesses de transmission de données sans fil pouvant atteindre un débit de deux mégabits par seconde (2 Mbps), ce qui est environ 40 fois la vitesse d'un modem conventionnel (Microcell Telecommunications Inc, 1999:9).

Les abonnés du sans-fil qui désirent payer par avance leurs services peuvent acheter des cartes de temps d'antenne prépayé, d'une valeur de 10, 25 ou 50 $ (Ramsay, 2000). Les clients parviennent à lire un code après avoir gratté la partie de la carte sur laquelle figure une série de chiffres (ou code). Ensuite, les utilisateurs du service prépayé doivent introduire ce code au clavier de leur appareil pour approvisionner leur compte en temps d'antenne (Collins, 1999b). Le montant de la recharge de la carte prépayée s'ajoute au solde, mais ce dernier n'est en vigueur que pour une certaine période, généralement de 60 jours (Bernatchez, 2000). Puis, " au-delà de la limite, le téléphone est désactivé si aucune nouvelle carte n'est achetée ", précise Ramsay (Ramsay, 2000:5).

2. LA FRAUDE À LA TÉLÉPHONIE MOBILE : UNE RÉALITÉ POLYMORPHE

Après avoir brièvement évoqué l'évolution et la nouvelle ère des télécommunications sans fil, nous allons d'abord dans la partie suivante nous attarder sur la typologie des principales fraudes recensées (2.1). Ensuite, nous allons examiner au point 2.2 le cadre juridique canadien et définir la notion de " fraude à la téléphonie mobile " qui sera utilisée tout au long de cette recherche.

2.1 TYPOLOGIE DES FRAUDES

Dans la littérature, il n'existe pas de définition claire, précise, exhaustive de la " fraude cellulaire " ou de la " fraude à la téléphonie mobile ". Dans son mode opératoire le plus aisé, la fraude consiste à trouver et utiliser un appareil portable perdu, ou encore à le voler à un consommateur pour s'en attribuer illicitement l'appartenance et l'usage (vol simple). Dans son mode opératoire le plus complexe et le plus sophistiqué, la fraude requiert des connaissances techniques de la part des fraudeurs ainsi que des manipulations des appareils téléphoniques à l'aide de matériels technologiques et informatiques (piratage). Entre les deux modes opératoires, il y a la fraude commise des suites d'un vol d'identité en vue d'obtenir un abonnement au forfait mensuel sans l'intention de le payer.

2.1.1 Le vol de cartes prépayées ou de téléphones mobiles déjà activés

Une des façons d'obtenir frauduleusement des services de communications consiste purement et simplement à voler des cartes de temps d'antenne prépayé (Collins 1999ab). Un autre stratagème repose sur le vol d'un téléphone cellulaire déjà activé (Basset Telecom Solutions, 2001; Beseler, 1997; Briscoe 2001; Clarke et al., 2001; Janhevich, 1998). Ce dernier stratagème permet aux malfaiteurs d'utiliser la ligne téléphonique jusqu'à ce qu'elle soit mise hors service par l'opérateur de téléphonie mobile (Basset Telecom Solutions, 2001; Briscoe, 2001; Clarke et al., 2001).

Dans une étude australienne réalisée par le New South Wales Bureau of Crime Statistics and Research, Briscoe (2001) souligne que les coûts abordables des services de télécommunications mobiles pour les consommateurs moyens et la disponibilité accrue des téléphones mobiles expliquent une certaine augmentation du nombre de vols d'appareils. D'une part, les résultats de l'étude réalisée sur une période de trois ans indiquent qu'en deux ans seulement, le nombre d'incidents concernant le vol de téléphones mobiles a doublé, passant de 19 433 à 39 891 vols par année (Briscoe, 2001:2). D'autre part, les résultats de l'étude démontrent une augmentation importante du nombre d'incidents violents avec vol de portables. À ce propos, Clarke et ses collaborateurs (2001) invoquent les raisons pour lesquelles les téléphones portables sont tant convoités par les voleurs : " Very high rates of theft have been documented for [...] mobiles phones [...] because they are concealable, removable, available, valuable, enjoyable and disposable. " (Clarke et al., 2001:7)

2.1.2 La fraude par usurpation (vol) d'identité lors de la souscription de l'abonnement

Dans le domaine de la téléphonie mobile, la très grande majorité des fraudes repose sur le détournement (vol) de l'identité d'une personne. Ces fraude sont communément répertoriées sous *supposition de personne* (art. 403 du Code criminel) dans le jargon policier ou encore *fraude lors de la souscription de l'abonnement* (*subscription fraud* en anglais) dans le jargon du sans fil (Blackwell, 1999; O'Brien, 1998). Cette forme de fraude très peu sophistiquée (O'Brien, 1998) consiste à voler ou à détourner l'identité d'une personne (ou même d'une entreprise) en totalité ou en partie pour présenter des demandes d'ouverture de

lignes téléphoniques sans toutefois avoir l'intention de payer le compte d'usager (Blackwell, 1999; Clarke et al., 2001). Pour parvenir à ses fins, l'usurpateur obtient d'abord des renseignements essentiels sur la victime : nom, adresse, date de naissance, numéro d'assurance sociale, numéros de cartes de crédit, etc. Il peut même obtenir un permis de conduire ou un passeport sous une fausse identité, ou faire des demandes de crédit, accumuler des dettes ou carrément vivre sous le nom d'une autre personne (Harvey, 2001).

Un rapport spécial du Solliciteur général du Canada nous apprend que le Centre national d'appels PhoneBusters de la Gendarmerie Royale du Canada a reçu 7629 plaintes de la part de Canadiens victimes de vols d'identité et dont les pertes totales s'élèvent à plus de 8,5 millions de dollars pour l'année 2002. Au cours du premier trimestre de 2003, 2250 plaintes ont été déposées et les pertes signalées ont totalisé 5,3 millions de dollars. Pour leur part, Equifax et Trans Union, les deux plus importantes agences nationales d'évaluation de crédit au Canada, déclarent avoir reçu entre 1400 et 1800 plaintes par mois de la part de Canadiens qui ont été victimes de vol d'identité (Solicitor General Canada, Page Web).

Le commissaire à la protection de la vie privée au Canada est d'avis qu'il est maintenant plus facile que jamais pour les criminels de voler les renseignements personnels car ceux-ci sont devenus très disponibles depuis l'avènement de l'autoroute virtuelle. Il précise que les progrès technologiques de ces dernières années permettent non seulement la diffusion des renseignements personnels à grande échelle, mais qu'ils favorisent également la communication entre les entreprises et les consommateurs (Office of the Privacy Commissioner of Canada, Page Web).

2.1.3 **Les fraudes reliées aux manipulations techniques, à l'altération et au piratage.**

De façon générale, les entreprises de communications sans fil permettent à leurs abonnés qui voyagent à l'extérieur de leur zone d'attache d'utiliser le réseau cellulaire d'un concurrent ou d'un partenaire. Ce faisant, les utilisateurs en déplacement sont en mode itinérance (ou *roaming,* en anglais), pour l'obtention de laquelle ils vont devoir payer des frais supplémentaires d'itinérance. En itinérance, ils peuvent également être victimes de tentatives de fraude (Basset Telecom Solutions, 2001). Deux formes de fraudes sévissent sur les réseaux cellulaires analogiques : le clonage (ou *cloning,* en anglais) et le *tumbling*. Elles

requièrent des manipulations techniques plus complexes que l'utilisation d'appareils volés déjà activés (Beseler, 1997; Blackwell, 1999; Clarke et al., 2001; Cousineau, 1995; Dupaul, 1995; Grabosky et Smith, 1997; Janhevich, 1998; Natarajan et al., 1995; O'Brien, 1998).

2.1.3.1 *Le clonage des appareils cellulaires*

Pour réaliser cette fraude, Dupaul (1995) explique qu'à l'aide de balayeurs d'ondes et de logiciels sophistiqués, les fraudeurs se postent dans des lieux où il y a une forte concentration d'utilisateurs actifs de cellulaires, dans le but de relever et de décoder le numéro de téléphone (MIN) d'un abonné ainsi que le numéro de série de son téléphone cellulaire (ESN). Ces numéros sont ensuite encodés dans de nouveaux appareils cellulaires (*clones*), qui, à leur tour, sont vendus sur le marché noir, permettant aux acheteurs de clones d'utiliser ces appareils aux frais des abonnés légitimes jusqu'à ce que la fraude soit découverte. Clarke et ses collaborateurs (2001) soulignent que les fraudeurs sont en mesure de se procurer l'équipement nécessaire, principalement les logiciels, sur Internet pour mener à bien leurs opérations illicites : " Cloners could get software that they loaded onto their PCs with detailed instructions for building equipment and cabling. Other sites listed specific hardware device for sale (p. 21) ".

2.1.3.2 *Le " tumbling "*

Durant les années 1990, une nouvelle forme de fraude communément appelée *tumbling* a vu le jour (Delaney, 1993). Ce type de fraude touchant les services cellulaires analogiques est plus insidieux que le clonage en raison des altérations techniques plus complexes qu'il exige. Le *tumbling* s'effectue par l'altération ou la reprogrammation du portable de façon à ce qu'il change de numéro de série (ESN) avant que chaque appel soit lancé, et ce, grâce à une puce spéciale. À la différence du *cloning*, le *tumbling* utilise un numéro de série (ESN) différent à chaque appel (Basset Telecom Solutions, 2001; Blackwell, 1999; Clarke et al., 2001).

> " Tumbler phones were modified so they randomly generated and sent to the cell site a different fictious MIN/ESN combination for each call. Within a carrier's own area, this technique wouldn't work. Networks do pre-call verification of the identifiers. If the MIN/ESN pair doesn't appear in its database, the carrier doesn't put the call through. But if the phone was

> roaming from its own supposed home calling area, calls would go through. " (Blackwell, 1999:63)

Qu'il s'agisse de " *cloning* "ou de " *tumbling* ", les manœuvres de piratage permettent aux malfaiteurs de faire des appels en très grand nombre, car bien souvent, il peut s'écouler un long laps de temps avant que l'activité frauduleuse soit découverte par l'abonné légitime et signalée à l'opérateur du sans-fil. Généralement, les abonnés victimes de clonage ne se rendent compte de rien lorsque leurs téléphones sont en marche. Ce n'est qu'une fois qu'ils reçoivent leurs comptes mensuels trop élevés qu'ils informent leur fournisseur de services. Dans d'autres cas, le clonage cellulaire est détecté par les dispositifs de sécurité des entreprises de télécoms qui ont la capacité de repérer certains schémas de la fraude (Basset Telecom Solutions, 2001). Nous aurons l'occasion, dans une partie subséquente, de revenir sur les divers moyens de protection destinés à alerter le personnel de la sécurité des actes de nature frauduleuse sur le réseau cellulaire. Soulignons que ce sont les entreprises de télécoms qui absorbent les pertes et que les abonnés légitimes n'ont pas à assumer les frais de la fraude (Basset Telecom Solutions, 2001; Cousineau, 1995; Dupaul, 1995).

Natarajan et ses collaborateurs (1995) présument que le grand avantage du réseau cellulaire numérique est que le piratage des appareils SPC, beaucoup plus complexe, rend cette activité illicite beaucoup moins attrayante qu'elle ne l'était avec l'ancien réseau cellulaire analogique.

2.1.3.3 *L'altération ou la manipulation des cartes de temps d'antenne prépayées*

Au cours des années, les actes délictueux se sont multipliés avec l'introduction du mode d'abonnement " à la carte " ou " prépayé ". A cause des défaillances sécuritaires que comporte le dispositif de production des cartes téléphoniques prépayées, un des délits les plus répandus consiste à ouvrir de façon illicite l'emballage de la carte pour lire le code secret sans le payer et ensuite à approvisionner son propre compte :

> " The fraudster, in most cases, make use of very simple techniques to try to obtain the hidden numbers and to put them back into circulation in the legitimate distribution channels. [...] With some vendor's card, the number can be read out through cellophane packaging or card can be disassembled and reassembled without the customer realizing that the card has been tampered with. Furthermore, were the vouchers are packaged

> in cellophane wrappers, these can often be opened and resealed without any evidence of tampering. " (Collins, 1999a :6)

Pour leur part, lorsque les abonnés légitimes se procurent des cartes prépayées, ils s'aperçoivent au moment d'introduire la série de chiffres au clavier de leur portable que la recharge d'unités téléphoniques a déjà été utilisée (Collins, 1999ab). Cela dit, dans la pratique, lorsque de tels incidents sont rapportés, les victimes de fraude reçoivent généralement un crédit téléphonique sur leur compte prépayé de la part de l'opérateur de télécommunications sans fil.

2.2 DÉFINITION DE LA NOTION DE LA FRAUDE CELLULAIRE OU À LA TÉLÉPHONIE MOBILE

Au vu du cadre juridique canadien, il n'existe pas définition claire et précise de la fraude à la téléphonie mobile. Néanmoins, à cette notion relativement nouvelle peuvent se rattacher quatre articles du code criminel qui permettent de criminaliser ce que nous appelons la " délinquance à la téléphonie mobile ".

Il y a d'abord l'article 326 (1)b du code criminel qui criminalise le vol de services de télécommunication commis par la mise en œuvre d'un : " stratagème quelconque permettant l'accès illicite ou sans apparence de droit à des services de télécommunications mobiles ".

Il y a ensuite l'article 380 (1) du code criminel canadien qui sanctionne la fraude: à savoir le comportement de celui qui, " par supercherie, mensonge ou autre moyen dolosif, constituant ou non un faux semblant au sens de la présente loi, frustre le public ou toute personne, déterminée ou non, de quelque bien, service, argent ou valeur ". La peine d'emprisonnement maximal s'élève à quatorze ans. Il est judicieux de préciser que l'article 380 du code criminel comporte un élément qu'il ne faut pas omettre : le préjudice économique.

Un troisième article a été mis en vigueur pour sanctionner et interdire, notamment, toute demande de souscription frauduleuse. Si une personne commet une usurpation d'identité à des fins de souscription frauduleuse, une accusation de supposition de personne peut être portée à l'encontre de cet individu en vertu de l'article 403 du code criminel

condamnant quiconque, frauduleusement, se fait passer pour une personne, vivante ou morte dans le but d'obtenir un bien ou un avantage pour lui-même ou pour une autre personne : a) soit avec l'intention d'obtenir un avantage pour lui-même ou pour une autre personne; b) soit avec l'intention d'obtenir un bien ou un intérêt dans un bien; c) soit avec l'intention de causer un désavantage à la personne pour laquelle il se fait passer, ou à une autre personne. La peine d'emprisonnement maximale s'élève à dix ans.

Pour conclure, une quatrième disposition criminalise l'utilisation non autorisée de cartes de crédit (art. 342 (1) du code criminel). Cela permet notamment de sanctionner l'usage abusif de cartes de crédit dans le but d'obtenir des produits et services de télécommunications sans fil. La peine d'emprisonnement maximale s'élève à dix ans.

Dans le cadre de la présente étude, nous n'assimilons pas à la fraude cellulaire certains actes préparatoires à la fraude comme la supposition intentionnelle de personne (art. 403), l'utilisation non autorisée des cartes de crédit (article 342(1)) ou le vol pur et simple de services cellulaires (art. 326(1b)). Nous axons plutôt notre recherche sur l'acte frauduleux dont les préjudices économiques atteignent exclusivement l'entreprise victimisée (art. 380(1)).

Deux types de fraude sont répertoriées ici; ils ont trait à deux modes différents de souscription : la fraude au forfait mensuel et celle au forfait prépayé.

3. L'AMPLEUR DU PHÉNOMÈNE ET SES CAUSES PROBABLES

3.1 LES DONNÉES ET LES ESTIMATIONS CONNUES DU PHÉNOMÈNE

Jusqu'au milieu des années 1980, la fraude à la téléphonie mobile était pratiquement inexistante. Ce nouveau délit a toutefois connu une expansion considérable depuis les années 1990 (Blackwell, 1999). D'après Chorleywood Consulting, une société située en Grande Bretagne, la fraude aux télécoms représente des pertes de 22 milliards de dollars par année dans le monde et elle augmente au rythme de deux milliards de dollars par année (GSMBOX, Page Web).

Plus près de chez nous, les données fournis par le CTIA [3] (Cellular Telecommunications & Internet Association) ont révélé que les pertes annuelles imputables à la fraude par cellulaire en Amérique du Nord étaient estimées à 440 millions de dollars en 1994, à 650 millions en 1995 et à 710 millions en 1996 (O'Brien, 1998). Pour l'année 1997, les pertes imputables à la fraude étaient de 434 millions de dollars, alors qu'en 1998, les pertes étaient estimées à 182 millions (CTIA, Page Web).

Quoi qu'il en soit, ces statistiques permettent au moins d'avoir une approximation utile de l'ampleur de la fraude car, selon Grabosky et ses collaborateurs (1998), l'une des difficultés qui se pose actuellement dans l'étude de la criminalité liée aux télécommunications est précisément la quantification exacte et complète de l'étendue du phénomène. Cette mesure est d'autant plus délicate que certains délits ne sont jamais détectés, pas même par leurs victimes (Grabosky et al., 1998). De plus, Blackwell (1999) précise qu'il est difficile dans le domaine de la téléphonie sans fil de distinguer les fraudeurs des mauvais créanciers.

La montée des activités frauduleuses se trouve favorisée par la loi du silence. Lorsque les entreprises détectent les délits dont elles sont victimes, elles renoncent généralement à porter plainte aux autorités policières ou judiciaires (Organisation for Economic Co-Operation and Development, cité dans Smith, 1996b), principalement pour des raisons commerciales (Grabosky et al., 1998). Rappelons qu'il en est de même dans les domaines de la criminalité informatique (Rosé, 1995) et de la criminalité des affaires (Rico, 1977), où les sociétés commerciales préfèrent gérer elles-mêmes leur victimisation, plutôt que d'en informer les instances du contrôle social formel.

3.2 LES MOTIVATIONS DES ESCROCS DU CELLULAIRE

Les motivations intéressent les chercheurs qui s'efforcent notamment d'appréhender les causes d'infractions comme les fraudes. Il ressort quatre catégories de mo-

[3] Le CTIA est un organisme international qui représente des exploitants de communication sans fil de services de téléphonie cellulaire, de communications personnelles (SCP), de radiocommunications mobiles et de télécommunications mobiles par satellite.

tivation dans l'ensemble de la recherche comportant des explications de la délinquance par cellulaire.

3.2.1 L'utilisation illicite et anonyme des services de téléphonie mobile

Il n'y a pas que la fraude cellulaire qui profite de l'émergence de la téléphonie mobile. Les produits et services de téléphonie mobiles peuvent également servir à l'accomplissement de divers crimes, notamment à des activités du crime organisé. Plusieurs auteurs ont d'ailleurs abordé cette question.

D'abord, dans une étude non publiée sur l'impact de la téléphonie mobile sur les organisations et pratiques criminelles, Hoad (1996:1) mentionne que le taux de pénétration et la prolifération des produits sans fil au cours des dernières années en Europe de l'Ouest et au Royaume-Uni ont notamment profité aux organisations criminelles, qui s'en sont servi pour commettre des activités illicites. En effet, l'auteur précise que ces criminels sont des adeptes de la technologie du sans-fil et qu'ils ont rapidement compris les avantages technologiques que leur procuraient ces produits (Ibid., 1996). Beseler (1997) va dans le même sens : " Stolen en cloned phones are quickly becoming popular tools for criminal [...] to conduct illegals activities using equipment that thwarts law enforcement's traditionnal wire-tapping techniques. " (Beseler, 1997:1).

Pour sa part, dans une étude sur la prévention de la criminalité en matière de téléphonie mobile, Smith (1996b) synthétise ainsi les avantages de la téléphonie mobile pour les criminels :

> " The freedom and anonymity which mobile telephony possesses, particularly where untraceable subscriptions are taken out, also makes the use of mobile telephones attractive to criminals such as drug traffickers who whish to conduct their affairs out of reach of law enforcement agencies. " (Smith, 1996b:4)

Outre le trafic de drogues (Blackwell, 1999; Briscoe, 2001; Clarke et al., 2001; Delaney, 1993; Grabosky et al., 1996; McGregor, 1998; Natarajan et al., 1995; Smith, 1996b), d'autres délits conventionnels sont facilités par l'usage des téléphones sans fil : le télémarketing frauduleux (Cherry, 2001; Ministère de la Justice, 1997), la prostitution (Be-

seler, 1997; Blackwell, 1999; Grabosky et al., 1996; Natarajan et al., 1995), le blanchiment d'argent (Clarke et al., 2001; Grabosky et al., 1996), le *gambling*, la pornographie infantile, le trafic d'armes (Grabosky et al., 1996), le kidnapping, la conspiration criminelle, l'espionnage industriel, les diverses formes de fraude, l'alerte à la bombe (*bomb hoaxes*), le harcèlement sexuel (Natarajan et al., 1995). Il est de plus en plus manifeste que ces délits sont facilités en raison de la liberté, de la commodité et de la discrétion qu'offre le sans-fil (Natarajan et al., 1995; Smith 1996b) :

> " The role of the telephone in the production of crime has expanded not just with the vast increase in the number of phones in use, but also with changes in technology with have made telephone more convenient – and more anonymous. In the days when all phones calls had to be connected by an operator (who might then "listen in" on the call), it was more difficult to use the phone for criminal purposes. There was always the risk of being overheard or of subsequently being identified. The capacity for subscribers to dial calls themselves, together with the vast expansion in phone use that this permitted, greatly reduced these risk." (Natarajan et al., 1995 :138)

Dans leur recension des écrits, Grabosky et ses collaborateurs (1998) indiquent que les immigrants illégaux qui ne peuvent pas avoir accès à des moyens légaux de services de télécommunications sans être obligés de dévoiler leur identité et leur statut figurent parmi ceux qui évitent de payer les services de télécommunications ou cherchent à les obtenir à moindre coût. Smith (1996b) ajoute que ces individus, comme ils veulent grandement téléphoner dans leurs pays, constituent une cible de choix pour les revendeurs illégaux d'appels interurbains internationaux à bas prix.

3.2.2 **Les gains financiers**

Plusieurs auteurs s'entendent pour affirmer que la perspective d'obtenir des services cellulaires sans les payer constitue la motivation essentielle des délinquants utilisant des cellulaires (Beseler, 1997; Blackwell, 1999; Clarke et al., 2001; Committee of the Judiciary, Page Web; Grabosky et al., 1996; Grabosky et Smith, 1997; Smith, 1996b). Delaney (1993) explique que le marché du vol des produits et services du sans-fil peut être très lucratif : " It can generate large profits fast [...] Some drug dealers have moved away from selling drugs to

cellular call celling operations for greater profit, the lack of enforcement, and if convicted, no expectation of serving time. " (Delaney, 1993:35-5)

Mentionnons à ce propos un cas décrit par les agents des US Secret Services à l'occasion d'un congrès sur la fraude cellulaire à Washington :

> " Working from the preliminary investigation of the local cellular phone company, our agents arrested a Lebanese national who was conducting a "call sell " operation. A call sell operation typically provides international calling activity for a variety of " customers " through the compromise of telecommunications systems. In this case, the defendant completed calls for customers in the Middle East by utilizing cellular account numbers that had been stolen with a scanner in New York. On a daily basis, the defendant's conspirators would express mail a new list of stolen account numbers to further this 24-hour per day operation. At the time of the arrest, some 26,000 account numbers were seized attributing to losses in the millions of dollars. " (Committee of the Judiciary, Page Web)

3.2.3 **Les défis technologiques**

Si, pour la majorité des fraudeurs, les motivations sont d'ordre matériel, financier ou utilitaire, pour d'autres, les motivations n'ont pas de caractère acquisitif. En effet, le désir de relever des défis, le désir ludique et enfantin de se montrer à la hauteur ou plus fort que des systèmes supposément bien protégés, d'effectuer des prouesses techniques font partie des motivations qui animent une partie des délinquants (Rosé, 1995). Dans son livre intitulé *The Fugitive Game,* Jonathan Littman, un journaliste spécialisé en informatique, rend fidèlement compte des conversations qu'il a eues avec Kevin Mitnick, le pirate informatique (*hacker*) considéré comme le plus redouté et le plus doué au monde. Ce spécialiste des intrusions informatiques et des fraudes cellulaires a finalement été capturé par le FBI le 15 février 1995, au terme d'une traque de plusieurs mois sur les réseaux de téléphones cellulaires et sur Internet. Il a été accusé d'avoir, entre autres, pénétré dans de très nombreux ordinateurs des plus grandes compagnies (Motorola, Sun Microsystems, Oki, DEC) et d'avoir volé des logiciels et des outils de surveillance des réseaux cellulaires. Les cibles principales de Mitnick, qui n'était pas motivé par l'argent, étaient les sociétés de télécommunications, les fabricants de matériel (informatique et de télécommunication) et les spécialistes de la sécurité. Il a réussi à se procurer les codes permettant de déverrouiller de nombreux

téléphones cellulaires, ce qui lui a permis d'actionner certaines de leurs fonctions. Il avait obtenu des prologiciels facilitant les intrusions dans les systèmes informatiques des organisations ou permettant de dissimuler sa véritable identité lors des connexions électroniques (en apparaissant sous une autre identité électronique et en imputant les factures de communication à d'autres comptes). C'était le défi relevé par Mitnick. Il lui importait de se prouver qu'il était le meilleur. Il disait vouloir prouver qu'aucun système n'était hors de portée de ses talents (Littman, Page Web).

3.3 LA VULNÉRABILITÉ DES ENTREPRISES DE TÉLÉCOMMUNICATIONS SANS FIL

Sans parler de la vulnérabilité de la technologie AMPS, la plus exposée au piratage cellulaire (O'Brien, 1998), un article écrit par Reuters et rapporté par *La Presse* indique que les opérateurs de téléphonie de troisième génération (3G) sont extrêmement vulnérables à la fraude et au piratage. Ces services multimédia, à haute valeur ajoutée, risquent d'engendrer plus de fraudes et d'être largement convoités par les pirates puisqu'ils sont moins sécurisés que ceux d'un réseau de téléphonie mobile. Par exemple, la manipulation de logiciels permettant de pénétrer dans les centres de facturation des sites des opérateurs de télécommunications sans fil est un genre de délit qui pourrait fort bien se produire. Pour expliquer la vulnérabilité des entreprises de télécoms, Phil Clark, directeur du département de la fraude et des investigations chez Hutchison 3G, met en cause l'insuffisance des moyens de protection. Il a d'ailleurs annoncé qu'à cause du marché très concurrentiel, " la pression des départements marketing pour fournir de nouvelles applications 3G aux consommateurs sera très forte et [...] la sécurité ne vient peut-être pas en tête de leurs priorités. " (Reuters, Page Web)

Dans un même ordre d'idée, Praesidium, une firme internationale spécialisée dans la gestion des fraudes en matière de télécommunications sans fil, ajoute que la vulnérabilité des entreprises de télécoms est particulièrement inquiétante pour les nouveaux opérateurs qui mettent davantage d'accent sur le taux de croissance des abonnés que sur la prévention des pertes :

> " It is widely known that all telecommunications operators are exposed to fraud problem. What is less well known is that telecoms fraud is a highly organized international criminal activity and that fraudsters tend to focus their resources on new mobile operators as soon as they launch their services... New operators are invariably focused on fast customer growth. Their shareholders will measure their success in their first few months, and indeed their first year, in terms of how many customers join their network. In most cases, bad debt and fraud management objectives are not usually considered key performance parameters in the first year. " (Praesidium, Page Web)

4. LES MOYENS DE PRÉVENTION ET DE LUTTE

Pour contrer la fraude à la téléphonie mobile, il existe une panoplie de moyens de lutte tant formels qu'informels qui s'étendent de la prévention à la répression, en passant par la détection. Bon nombre d'entreprises de télécommunications sans fil ont adopté des stratégies préventives et défensives en vue de limiter les activités frauduleuses dont elles sont la cible. Outre les pratiques institutionnelles et les politiques de protection des entreprises, il existe également des moyens juridiques qui permettent de sanctionner les accès frauduleux à la téléphonie mobile.

4.1 LA RÉPONSE PRÉVENTIVE ET LES MOYENS DE PROTECTION DES OPÉRATEURS DE RÉSEAUX CELLULAIRES

4.1.1 Les mesures de prévention

Au milieu des années 1990, dans le but de réduire le volume des fraudes par cellulaires analogiques, certains opérateurs de téléphonie mobile ne permettaient pas à leurs abonnés itinérants d'utiliser leurs appareils dans certaines régions connues pour leurs importants problèmes de fraude. À ce propos, Dupaul (1995) donne en exemple Bell Mobilité, qui ne permettait pas aux usagers itinérants d'utiliser leurs cellulaires lorsqu'ils séjournaient à New York, à Boston, à Miami ou à Phoenix. Pour sa part, Cousineau (1995) précisait que les escrocs du cellulaire pullulaient depuis deux ans dans ces villes et que les fraudes y avaient atteint une envergure inégalée. " C'est une décision radicale, mais nous perdions plus d'argent que nous en faisions ", avait précisé Yves Bigras, directeur de la sûreté chez Bell Mobilité (Cousineau, 1995). Au moment où les articles de Cousineau (1995) et de

Dupaul (1995) étaient écrits, rien ne permettait d'affirmer que les grands moyens entrepris par Bell Mobilité avaient fait diminuer la fraude. Cela dit, nous pouvions lire que cette solution consistant à ne pas desservir certaines villes américaines à risque était d'une durée indéterminée et ce, jusqu'à ce qu'une solution technologique soit mise au point.

4.1.2 **Les moyens technologiques**

Ainsi, au fil des ans, pour affronter la vague de fraudes par cellulaires analogiques, les opérateurs de téléphone cellulaire ont réagi en implantant un nouveau protocole technologique de communication qui comporte un processus d'authentification (Basset Telecom Solutions, 2001; Blackwell, 1999; Clarke et al., 2001). À cet égard, Blackwell (1999) explique que l'authentification permet de vérifier l'identité de chaque utilisateur qui cherche à accéder aux services téléphoniques sans fil. Ainsi, avant qu'un appel soit lancé, le réseau cellulaire vérifie d'abord la validité de la combinaison des numéros de téléphone (MIN) d'un abonné de même que le numéro de série de son téléphone cellulaire (ESN). Si cette combinaison (MIN/ESN) n'apparaît pas dans la base de données AUc (de l'anglais *Authentification Center,* " centre d'authentification ") de l'opérateur du réseau cellulaire, l'appel ne sera pas effectué. Plus important encore, outre la combinaison (MIN/ESN), le processus d'authentification vérifie également la validité de l'appareil cellulaire utilisé. Comme l'écrit Blackwell (1999), ce processus consiste à vérifier le numéro encrypté qui est habituellement donné par l'opérateur à ceux qui ont le droit d'user, comme abonnés, du réseau sans-fil.

> " Authentification works something like public key encryption in computer networks. On each call, the networks ask the handset to identify itself by generating a unique number using an encryption key and a complex algorithm. It sends this number to the cell site. The network can verify the number is valid because it also holds the encryption key. " (p.63)

L'implantation de l'authentification est une technologie qui a contribué à faire diminuer de façon considérable les pertes reliées au piratage cellulaire chez Bell Mobilité. Chez Rogers AT&T, les fraudes cellulaires ont diminué de 80 % grâce à l'introduction de ce nouveau moyen de protection (Blackwell, 1999).

4.1.3 **Les systèmes de détection**

Parmi les outils les plus évolués et actuellement disponibles sur le marché pour réduire davantage les attaques frauduleuses, citons les systèmes de détection de la fraude (Basset Telecom Solutions, 2001; Blackwell, 1999; Nortel Networks Fraud Solutions, 2000; O'Brien, 1998). Bien qu'il existe divers types de systèmes de détection sur le marché, plusieurs opérateurs ont leurs propres systèmes internes de détection pour tenir en échec les fraudeurs (Basset Telecom Solutions, 2001). De façon générale, les systèmes de détection permettent aux opérateurs de surveiller en permanence la manière dont leur réseau est utilisé et de déceler les signes révélateurs d'un comportement frauduleux en temps quasi réel. Ces systèmes experts se distinguent par leurs capacités de profilage (*profiler,* en anglais) des comportements des utilisateurs à partir de tous les enregistrements des données d'appel (*Call Detail Records* ou *CDR,* en anglais). Ensuite, ils alertent le personnel de la gestion des fraudes lorsque des seuils de typicité (*threshold*, en anglais) sont dépassés ou que des seuils comportementaux établis pour chaque abonné sont atteints (Basset Telecom Solutions, 2001; Blackwell, 1999; Nortel Networks Fraud Solutions, 2000; O'Brien, 1998). O'Brien (1998) décrit entre autres certains modes de fraude qui peuvent déclencher des alarmes lorsque des abonnés présentent un type d'utilisation suspect ou excessif :

> " Software monitors activity and flags certain calls – such as [...] high calls counts, calls to or from pay phones, calls to or from suspicious locations, and calls at suspicious times of the day. Exceeding a predetermined threshold generates an alarm and notifies security personnel." (p.23).

D'autres schémas de fraude peuvent également être détectés. Par exemple, en matière de piratage cellulaire, Dupaul (1995) souligne que ces dispositifs de sécurité ont comme particularité d'être munis de fonctions d'identification d'anomalie " par collusion " ou " par vélocité ". La première technique de dépistage intitulée " identification par collusion" permet de repérer deux individus qui utilisent simultanément le même numéro de téléphone. La seconde technique mieux connue sous le nom de " repérage par vélocité " permet de suivre la trace d'un abonné qui effectue des appels de régions éloignées les unes des autres, dans un laps de temps très bref. Ainsi, cette technique de dépistage permet d'identifier des situations comme celle-ci : un abonné fait un appel à Montréal et dix ou

quinze minutes plus tard, le même abonné effectue un appel de New York, à partir du même téléphone cellulaire.

4.1.4 La vigilance individuelle ou la sensibilisation du grand public

Il existe d'autres moyens qui tendent à réduire le piratage cellulaire. Ceux-ci relèvent de la vigilance individuelle ou de la sensibilisation du grand public. À cet égard, Smith (1996a) affirme qu'il faut inciter les abonnés à vérifier leurs factures mensuelles, à ne pas laisser leurs téléphones sans surveillance dans les voitures et à verrouiller les appareils avec un numéro d'identification personnel (en anglais PIN, pour *Personnal Identification Number*). Pour sa part, O'Brien (1998) ajoute que la plupart des opérateurs de télécoms fournissent aux utilisateurs du sans-fil un numéro d'identification personnel de quatre chiffres qu'ils doivent introduire pour effectuer tout appel. Or, Clarke et ses collaborateurs (2001) observent que, bien que ces numéros d'identification personnels procurent un certain sentiment de sécurité aux usagers du sans-fil, les malfaiteurs ont rapidement trouvé une technique permettant de décoder ces numéros d'identification personnelle, grâce à l'utilisation de balayeurs d'ondes. Cela dit, l'astuce qui permet aux pirates de décoder et ré encoder ces numéros n'est pas révélée dans l'article de Clarke et ses collaborateurs (2001).

4.2 LA RÉPRESSION ET LES ASPECTS JURIDIQUES

Souhaitant combattre plus efficacement les fraudes, les Américains ont adopté un discours répressif qui préconise des sanctions destinées à compléter l'effet des moyens de protection, qui ne sont pas considérés à eux seuls comme étant tout à fait efficaces. Ce discours préconise de faire de la fraude un délit plus risqué, moins attrayant et moins profitable, en suscitant la coopération des organismes d'application de la loi et des opérateurs de téléphonie mobile afin d'identifier et de traduire en justice les escrocs du cellulaire. (Beseler, 1997; Committee of the Judiciary, Page Web; Delaney, 1993; O'Brien, 1998). Jusqu'à présent, ce sont les États-Unis qui se sont distingués en matière de répression des fraudes. Des opérations policières ont permis de mettre à jour de nombreux réseaux de fraudeurs grâce à la collaboration des organismes d'application de la loi et des opérateurs de télécoms (Beseler, 1997; Committee of the Judiciary, Page Web; O'Brien, 1998).

Aux États-Unis, le gouvernement fédéral a adopté en 1994 une disposition pénale portant sur l'altération frauduleuse des instruments et équipements de télécommunications (18 U.S.C., Section 1029). Les peines qui y sont prévues sont des amendes pouvant aller jusqu'à 50 000 $ et une peine maximale d'emprisonnement de 15 ans. (Voir Clede dans CTIA, Page Web). De plus, la Federal Communication Commission (FCC) a apporté des modifications particulièrement contraignantes à sa réglementation en ce qui a trait à la falsification et à l'altération de numéros de série électroniques (ESN, pour *Electronic Serial Number*) à l'intérieur de téléphones sans fil. Selon les règlements de la FCC, tout téléphone sans fil doit avoir un ESN unique et en aucun cas deux téléphones ne doivent avoir ou émettre le même ESN. En 1998, la disposition pénale 18 U.S.C., Section 1029 portant sur l'accès frauduleux aux services de communications sans fil a été modifiée. Ainsi, les amendements introduits par la *Wireless Telephone Protection Act* (WPTA) prévoient notamment qu'un individu commet une infraction quand, sciemment, il utilise, produit, trafique ou possède du matériel ou des logiciels permettant le clonage des téléphones portables. La peine maximale d'emprisonnement a augmenté; elle est passée de quinze à vingt ans (United State Sentencing Commision, Page Web).

Comme nous l'avons déjà précisé à la section 2.2, au Canada, certaines dispositions du Code criminel sanctionnent toute infraction commise à l'encontre d'une entreprise de télécommunication ou d'un individu lésé. Il va s'agir maintenant de comparer les peines prévues au Canada avec celles prévues par la loi chez nos voisins du Sud.

Une accusation de vol de service de télécommunications peut être portée en vertu de l'alinéa 326(1)b) du Code criminel qui vise quiconque, frauduleusement, malicieusement ou sans apparence de droit, se sert d'installations ou obtient un service en matière de télécommunications. La peine maximale d'emprisonnement est de deux ans. Dans cette disposition, " télécommunications " désigne toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil, radioélectricité, optique ou autres systèmes électromagnétiques (art. 326.2).

En matière de piratage cellulaire, l'article 327. (1) dit que commet un acte criminel quiconque " fabrique, possède, vend ou offre en vente ou écoule des instruments ou des

pièces particulièrement utiles pour utiliser des installations ou obtenir un service en matière de télécommunications ". Comme l'alinéa 326(1)b), la peine prévue pour sanctionner l'article 327 (1) est également l'emprisonnement pouvant aller jusqu'à deux ans.

Hormis les auteurs américains, la quasi-totalité des auteurs ne semblent pas privilégier la répression en matière de téléphonie cellulaire pour enrayer la fraude. Selon Smith (1996ab), la manière la plus efficace de combattre la fraude à la téléphonie mobile consiste à la prévenir. En s'inspirant des principes traditionnels de la prévention situationnelle de Clarke, ce chercheur australien propose de rendre les cibles moins attrayantes, en augmentant les risques de détection et en minimisant les bénéfices tirés des illégalités en matière de télécommunications. Dans la même veine, en ce qui a trait au vol des téléphones portables, Briscoe (2001) a écrit: " Eliminating the capacity of a stolen mobile to receive incoming calls would significantly reduce the value of the handset and thereby reduce the incentive to steal mobile phones. " (Briscoe, 2001:4). Pour leur part, Grabosky et ses collègues constatent qu'il est difficile pour l'État ainsi que pour l'industrie des télécommunications d'exercer un contrôle coercitif à l'égard des malfaiteurs et qu'ainsi la meilleure solution demeure l'autoprotection et la discipline individuelle de la part des victimes potentielles (Grabosky et al., 1996; Grabosky et Smith, 1997; Grabosky et al., 1998).

4.3 LE RÔLE DE LA POLICE EN MATIÈRE DE JUDICIARISATION

En 1995, un sondage auprès des chefs de police membres de l'Association canadienne des chefs de police (The Canadian Association of Chiefs Police) a été mené par KMPG Investigation and Security Inc. L'étude avait pour but de cerner l'attitude et la position des chefs de police canadiens à l'égard des fraudes ainsi que des crimes en col blanc (KPMG, 1995).

À la lecture des résultats du sondage, la position des chefs de police canadiens se résume comme suit :

- D'abord, 69 % d'entre eux ont clairement souligné que leur service de police n'avait pas les effectifs nécessaires pour contrer les formes de délinquance économique.

- Les répondants ont indiqué, dans une proportion de 83 %, que les fraudes et les crimes en col blanc constituaient à l'heure actuelle un problème majeur et qu'ils s'attendaient à un accroissement des diverses formes de criminalité économique.

- Toutefois, ces types de criminalité ne constituent pas une priorité pour les divers corps de police canadiens (73 %). Parmi les principales explications à cela, notons les attentes du public (notamment à l'égard des crimes violents et des problèmes de drogues), l'avancement de la technologie, le manque d'expertise au sein des divers départements, le manque d'effectifs policiers et de ressources ainsi que, dans le passé, la faible prévalence des crimes en col blanc.

- Les entreprises canadiennes devront faire appel aux ressources privées pour se livrer à des investigations sur les crimes de nature économique. La complexité croissante des fraudes, le manque d'expertise des policiers et la priorisation d'autres formes d'infractions sont les principales explications des chefs de police.

- Pour faire face à la complexité des crimes économiques et à la sophistication des criminels, certains agents reçoivent une formation adéquate leur permettant de former des unités de crimes commerciaux (*Commercial crime division*). Dans une proportion de 70 %, les répondants ont déclaré que leur service de police n'était pas doté d'une telle unité spécialisée. La majorité des répondants ont indiqué que cela s'expliquait par la taille de leur organisation. Les autres raisons allaient du manque de ressources, tant en ce qui a trait aux effectifs que des budgets, aux besoins insuffisants en cette matière (traduction libre, KPMG, 1995).

Le sondage réalisé au Canada de KMPG met en évidence le faible niveau d'activités policières en matière de criminalité économique et son ambivalence face à la fraude en général. Un constat analogue est aussi fait par Simmonds (2000) qui souligne le peu d'intérêt des autorités policières à judiciariser la fraude en matière de télécommunications sans fil.

4.4 LES DIFFICULTÉS TECHNOLOGIQUES, ORGANISATIONNELLES ET JURIDIQUES À CONTRER LA FRAUDE

La mise en œuvre d'une lutte contre la fraude cellulaire n'est pas sans poser de problème, tant du point de vue technologique, corporatif, organisationnel que juridique. Faire échec aux délinquants qui obtiennent frauduleusement des services de téléphonie cellulaire constitue à l'heure actuelle un défi de taille car malgré leur volonté de combattre les fraudes, les entreprises de télécoms ne disposent pas forcément des moyens technologiques suffisants pour les enrayer. Par exemple, en dépit des efforts d'implantation de dispositifs d'authenfication faits par l'industrie du sans fil pour contrer le piratage cellulaire, Blackwell (1999) écrit :

> " The biggest problem with authentification is that not every cell phone is authenticatable. The industry has required equipment vendors to produce only authentification handsets since 1996, but there are still many older phones still in use that cannot be authenticated. That means they can still be cloned [...]. The other problem is that not every cellular carrier has implemented an authentication system yet. Many smaller analog carriers in the US have yet to do it. That means they can't catch roaming clone phones. " (p.63)

Il ajoute également que, malgré les systèmes novateurs de détection, certains malfaiteurs ont rapidement compris les faiblesses intrinsèques des dispositifs de sécurité, et que certaines fraudes ne seront jamais détectées ou découvertes (Blackwell, 1999).

Par ailleurs, bien que les différentes mesures de sécurité rendent aujourd'hui les entreprises de télécoms moins vulnérables au piratage cellulaire que dans les années 1990 (Blackwell, 1999), la majorité des entreprises ont perçu un effet de déplacement des fraudes au téléphone analogique vers les fraudes survenant lors de la souscription à l'abonnement (Blackwell, 1999; Clarke et al., 2001). En effet, la fraude est un phénomène dynamique. Lorsque les entreprises de télécommunication sans fil réagissent contre une forme de fraude, les escrocs du cellulaire se tournent vers de nouvelles formes de fraudes (Blackwell, 1999). À ce propos, Warren Leonhard, chef du Service de la fraude et de la sécurité de Bell Mobilité, appréhende bien le déplacement de cette forme de criminalité :

> " We expect we'll virtually eliminate cloning when the network is 100 percent authenticatable. At that point, the fraudsters will choose the path of least resistance and try other things [...] It's like squeezing a balloon [...] The volume of fraud stays the same, you just move the air around and it bulges out somewhere else. " (Blackwell, 1999:61-62)

Concernant la répression, lorsque les entreprises de télécommunications sans fil désirent dénoncer et judiciariser les actes délictueux dont elles sont la cible, elles doivent surmonter plusieurs difficultés juridiques. Cunningham (1995) fait remarquer qu'en Amérique du Nord, les lois sur les nouvelles techniques de l'information et de la communication ont un temps de retard sur les activités criminelles. Les juristes et ceux qui œuvrent dans le domaine de la justice devraient se soucier de la rapidité avec laquelle évolue la haute technologie puisque " le Code criminel est désuet et incapable de s'adapter au rythme des changements technologiques et cela contribue à faciliter la fraude dans le domaine de l'informatique et des télécommunications ". (Cunningham, 1995:7)

Outre la difficulté de déterminer clairement où le délit a été commis, les autorités judiciaires australiennes ont rencontré d'autres obstacles. En effet, en Australie: " There may be a lack of agreement about whether or not the activity in question is criminal at all, whether in fact it has been committed, who has committed it, who has been victimized because of it, who should investigate it and who should adjudicate and punish it. " (Grabosky et al., 1996:6). Nous remarquons, au vu des articles provenant de l'Australian Institute of Criminology, que les problèmes complexes de droit, plus précisément de juridictions et de conventions d'extradition, que pose l'internationalisation de la délinquance en matière de télécommunications n'en favorisent pas la détection et l'investigation, ni ne favorise la poursuite des délinquants. Les auteurs soutiennent notamment que la coopération transfrontalière, les procédures d'enquêtes, les poursuites des fraudeurs et l'application des peines constituent de réels problèmes juridiques et législatifs. En effet, une fois que les escrocs du cellulaire ont été identifiés ou repérés, les instances judiciaires doivent souvent régler des problèmes d'extradition et obtenir des mesures d'entraide judiciaire. (Grabosky et al., 1996; Grabosky et Smith, 1997; Grabosky et al., 1998).

5. CADRE THÉORIQUE ET PROBLÉMATIQUE

Dans les études en matière de fraude, les criminologues ont principalement développé des théories contribuant à l'explication du contrôle social. Pour tenter d'expliciter les réactions et les stratégies permettant de contrer la fraude dans le domaine de la téléphonie mobile, nous avons choisi pour cadre théorique l'individualisme méthodologique. C'est un paradigme qui a été développé par Max Weber et repris, entre autres, par le sociologue français Raymond Boudon. Bien que notre cadre théorique soit très général, nous devons d'emblée mentionner que certains principes de l'individualisme méthodologique ont des liens étroits avec d'autres approches théoriques, notamment celles du choix rationnel, des opportunités, de la dissuasion, de l'analyse stratégique et de la prévention situationnelle. Voyons d'abord en quoi consiste l'individualisme méthodologique.

5.1 L'INDIVIDUALISME MÉTHODOLOGIQUE

Selon la perspective de l'individualisme méthodologique de Boudon, l'agrégation et l'action sont deux notions fondamentales. En bref, l'agrégation est la combinaison, l'addition ou encore la " juxtaposition " des actions individuelles. Quant à l'action, elle est définie comme un comportement intentionnel qui vise une fin. Cette approche théorique considère que les phénomènes sociaux sont les produits agrégés d'actions individuelles dont il faut comprendre le sens. Elle s'oppose ainsi au holisme méthodologique pour lequel " le tout explique la partie " et qui postule que les comportements des groupes sociaux déterminent les comportements individuels. Selon le principe de l'individualisme méthodologique, les comportements individuels constituent le point de départ de toute analyse sociologique. Cette analyse se distingue par ses deux phases. La première, celle de " l'explication ", vise à montrer qu'un phénomène social est la résultante de la sommation (" agrégation ") de comportements individuels. La deuxième phase, celle de la " compréhension ", a pour but de saisir le sens de ces actions, croyances ou attitudes individuelles, notamment en décomposant les motivations complexes (" bonnes raisons ") des acteurs dans les différents types de situation où ils posent des actions (Boudon, 2002 : 41-76).

Boudon soutient que pour rendre compte d'un phénomène social, il est fondamental de reconnaître les processus de " décisions typiques " qui se dégagent des décisions individuelles. Dans le cadre de leurs processus décisionnels, les acteurs prennent en considération, pour atteindre leurs fins, les ressources dont ils disposent de même que les contraintes structurelles de l'action. Plus précisément, ils déterminent leurs choix en fonction de l'évaluation qu'ils font des : 1) bénéfices espérés, 2) coûts escomptés, 3) risques auxquels ils s'exposent. Si donc les acteurs sont censés prendre les meilleures décisions possibles dans la situation où ils se trouvent, c'est qu'ils sont présumés rationnels (Ibid. p. 45-55).

La rationalité postulée par Boudon est, d'une part, imparfaite, étant donné que l'information dont les acteurs disposent peut être limitée, déficiente ou fausse. D'autre part, la rationalité est " instrumentale[4] " ou utilitaire, puisque les moyens employés par les acteurs pour atteindre leurs fins sont ceux qui leur paraissent les meilleurs ou encore ceux qui vont leur procurer le plus de satisfaction au moment de passer à l'action.

Pour comprendre la logique d'un comportement individuel, il importe, selon l'auteur, de retrouver les facteurs qui incitent les acteurs à agir comme ceci ou comme cela. Parmi ceux-ci, mentionnons le contexte social, contraignant à divers degrés, dans lequel s'inscrivent des rôles plus ou moins définis. Dans tout contexte social (institution, structures sociales), il existe, selon Boudon, deux types de systèmes à l'intérieur desquels les acteurs agissent entre eux. Le premier, appelé " système de rôles ", rassemble les règles et les principes institutionnels auxquels les acteurs doivent souscrire. En d'autres termes, ces derniers, en interagissant avec autrui, sont liés par le système de rôles dans lequel ils sont engagés. Le second système, appelé " système d'interaction ", confère quant à lui plus de liberté ou plus de latitude aux acteurs. Là, ces derniers n'interagissent pas avec les autres en regard des rôles conférés mais plutôt en fonction de leurs propres intérêts (Idib., p. 77-83).

Outre les rôles qui aident à identifier " les bonnes raisons " qui motivent les acteurs à adopter une action, il y a également les croyances qui influent sur leurs intentions. Aussi,

[4] Selon Boudon (2002), la signification que les individus donnent à leurs actions ne se limite pas uniquement à la rationalité instrumentale. En effet, il reconnaît d'autres formes de rationalité, comme par exemple la rationalité cognitive. Celle-ci tient compte des bonnes raisons pour lesquelles les gens adhèrent à des croyances idéologiques, magiques ou encore à des valeurs morales (p. 91 et suivantes).

même si certains comportements découlent de croyances erronées, il n'en demeure pas moins qu'ils puissent être revêtus d'une rationalité relative puisqu'ils visent l'atteinte de certaines fins et qu'à ce titre ils demeurent de type instrumental.

5.2 LIENS ENTRE L'INDIVIDUALISME MÉTHODOLOGIQUE ET D'AUTRES APPROCHES THÉORIQUES EN CRIMINOLOGIE

Après avoir évoqué les principes de l'individualisme méthodologique, signalons quelles sont les théories avec lesquelles il partage certains de ses principes. Il y a d'abord la théorie du choix rationnel qui, comme le dit Boudon (2002a), ne doit pas être confondue avec celle de l'individualisme méthodologique, même si elle partage trois postulats avec celui-ci. Premièrement, selon Boudon (ibid.), les deux théories partagent le postulat individualiste selon lequel les phénomènes sociaux sont le résultat d'actions individuelles agrégées. Deuxièmement, l'auteur ajoute qu'elles ont en commun le postulat de la compréhension, qui permet de reconstruire un comportement ayant un sens pour l'acteur. Troisièmement, d'après Boudon (ibid.), s'y ajoute le postulat de la rationalité instrumentale qui, d'ailleurs, est également adopté par Cornish et Clark (1986), deux défenseurs de la théorie du choix rationnel. De l'avis de ces derniers auteurs, les individus, pour obtenir ce qu'ils désirent, prennent des décisions raisonnées en tenant compte, entre autres, de facteurs individuels et subjectifs (besoins, valeurs, croyances, expériences antérieures, etc.) avant de passer à l'acte.

Ensuite, l'approche de Boudon comporte aussi certains des principes consacrés par la théorie des opportunités de Cohen et Felson (1979). Ces derniers auteurs soulignent notamment l'importance des circonstances dans lesquelles se produit un délit et qui le rendent possible. La théorie des opportunités est centrée sur trois éléments : 1) les délinquants potentiels ; 2) les occasions / cibles intéressantes ; 3) l'absence de moyens de surveillance. Il ne suffit donc pas de la seule présence d'un délinquant potentiel pour commettre une action criminelle. La commission d'un délit se produit lorsqu'il y a convergence entre un délinquant potentiel, des occasions criminelles qui se présentent à lui et l'absence ou l'insuffisance de gardiens.

Deux théories constituent le complément naturel de la théorie des opportunités : la théorie de la dissuasion et la théorie de la prévention situationnelle. Tout comme celles

précitées, ces deux théories présupposent que les individus sont des êtres capables de soupeser les conséquences favorables et défavorables de leurs actions criminelles.

Selon la théorie de la dissuasion, pour éviter qu'un crime soit commis ou pour le rendre moins attrayant, il faut recourir aux sanctions pénales. À ce sujet, Cusson (1990) distingue quatre mécanismes par lesquels agissent les sanctions pénales :

1- La dissuasion générale, qui est l'influence intimidante sur l'ensemble des citoyens de la somme des sanctions pénales qui sont infligées. À ce titre, la dissuasion rend les occasions criminelles moins attrayantes;

2- La dissuasion individuelle, qui résulte de l'influence sur le condamné des sanctions qui lui sont infligées;

3- La force de la dissuasion est fonction de la probabilité que des peines soient infligées à la suite de la commission de crimes;

4- La force de la dissuasion est fonction de l'ampleur du blâme social, qui se manifeste par la dénonciation du crime commis et par l'indignation manifestée.

Ainsi, en matière de fraude à la téléphonie mobile, tout comme en toute autre matière criminelle, la dissuasion s'avère effective si l'on est en mesure d'adopter des tactiques et des moyens d'action susceptibles de rendre les opportunités criminelles moins avantageuses qu'autrement.

D'ailleurs, les notions de tactique et de rationalité instrumentale nous permettent de mentionner une autre approche théorique qui n'est pas sans rapport avec l'individualisme méthodologique : l'analyse stratégique de Cusson (1989). Celui-ci accorde en effet à la notion de tactique criminelle une attention particulière. Il la définit comme suit : " C'est la séquence des choix et des gestes posés par le délinquant durant les faits : la manière dont il combine les moyens disponibles pour réaliser ses fins tout en s'adaptant aux circonstances. " (Ibid., p. 96). L'analyse stratégique et l'approche de l'individualisme méthodologique ont en commun l'idée que pour atteindre leurs fins, les individus qui agissent de manière rationnelle adoptent les moyens qui leur semblent les plus appropriés. Dans cette optique et lors de

l'examen des moyens mis en œuvre pour lutter contre la fraude, l'analyse stratégique nous incite, en l'occurrence, à nous interroger sur le degré d'adéquation entre les fins poursuivies par ceux qui luttent contre la fraude et les moyens qu'ils mettent en œuvre pour y parvenir.

La théorie de la prévention situationnelle s'est développée de façon spectaculaire depuis la fin des années 1970 en Grande-Bretagne, grâce aux travaux des criminologues Ronald V. Clarke et David Cornish (De Calan, 1995). Cette théorie a été appliquée à des formes très spécifiques de crimes (vols de voitures, cambriolages, vandalisme, appels obscènes, etc.) et a surtout des incidences sur la conception, la gestion et l'aménagement de l'architecture et de l'espace urbain (Clark, 1995, 1997). Le principal objectif de cette approche est donc la réduction des occasions criminelles qui s'offrent aux délinquants potentiels. Elle s'articule autour de 4 axes et de 16 techniques de prévention situationnelle. (Clark, 1997 : 15-25). Les axes sont les suivants :

1- Rendre la perception du passage à l'acte plus difficile (durcissement des cibles, contrôle d'accès, dissuasion des délinquants, contrôle des facilitateurs);

2- Rendre la perception du passage à l'acte plus risqué (contrôles des entrées-sorties, surveillance formelle, surveillance par les employés, surveillance naturelle);

3- Réduire les bénéfices escomptés du crime (élimination des cibles, marquage des biens, suppression de l'objet même du délit ou de l'incitation, suppression des gains du crime);

4- Montrer le caractère répréhensible du délit en le rendant moins « excusable » (mise en place de réglementations en matière de politiques, déclarations ou d'enregistrement), conscientisation et responsabilisation collective, contrôles des désinhibitions sociales ou morales, mesures destinées à faciliter le respect des règles).

Sur le plan de la délinquance cellulaire, l'article de Smith (1996b) donne des exemples probants et concrets de stratégies de prévention situationnelle. Ce chercheur australien, en accord avec les principes de base proposés par Ronald V. Clarke, démontre que les opérateurs cellulaires, en l'occurrence aux États-Unis, en Europe et en Australie, s'étant dotés de politiques préventives et de dispositifs de détection parviennent à dissuader certains fraudeurs d'opérer. Dans l'article intitulé " Preventing Mobile Telephone Crime ", Smith

(Ibid.) donne en exemple une situation s'étant produite aux États-Unis, où les opérateurs aux prises avec la fraude en mode itinérance ont réussi à bloquer l'accès des appels effectués à destination des pays fréquemment appelés par des délinquants, tels que la Colombie et la République Dominicaine. Au Royaume-Uni, l'opérateur Cellnet ne permet l'accès à l'itinérance internationale qu'à certains types d'abonnés. En Australie, la société de télécommunications Vodafone s'est équipée d'une base de données des numéros de séries des appareils volés permettant d'identifier les appareils volés lors de leur remise en service. Dans certains pays, les opérateurs de télécommunications sans fil n'autorisent pas leurs abonnés à faire des appels téléphoniques de l'étranger sans avoir, au préalable, fait l'objet d'une enquête de crédit plus approfondie.

Sur le sol canadien, nous avons déjà évoqué l'exemple de Bell Mobilité qui, en 1995, a décidé de réduire les opportunités de fraude en modifiant certaines politiques en matière d'itinérance analogique. En effet, l'entreprise ne permet plus à ses abonnés d'utiliser leurs téléphones cellulaires traditionnels sur le réseau cellulaire d'un concurrent ou d'un partenaire lorsqu'ils séjournent dans certaines villes américaines déjà reconnues pour leurs importants problèmes de clonage (Dupaul, 1995).

5.3 LA PROBLÉMATIQUE

Le marché des télécommunications sans fil ouvre la voie à des occasions criminelles sans précédent et à la fraude lors de la souscription (ou le vol d'identité), l'une des formes de crime les plus préoccupantes pour les opérateurs cellulaires. Le vol d'identité constitue un phénomène en pleine croissance. Il touche non seulement les entreprises mais également les consommateurs qui se font usurper leurs renseignements personnels. Il nous est donc permis de dire que les quatre principaux fournisseurs canadiens de téléphonie mobile encourent d'importants risques de fraudes au vu des nouveaux modes d'acquisition de la clientèle. En effet, pour obtenir des services de communications sans fil, les abonnés n'ont plus nécessairement à se déplacer dans les points de vente. Le commerce électronique favorise désormais les demandes de crédit à distance, incluant celles qui portent sur des services cellulaires, que ce soit par le biais des Centres d'appels ou d'Internet. Ces technologies facilitent ainsi la tâche des fraudeurs. Face à cette situation à hauts risques de fraude, les

moyens destinés à contrer la délinquance en matière de téléphonie sont nombreux; prévention, détection et répression sont autant de modes de réaction permettant aux entreprises de combattre les pratiques frauduleuses dont elles sont victimes.

La pertinence de poursuivre des recherches sur le phénomène de la fraude en matière de télécommunications sans fil tient, entre autres, à la croissance du marché des télécommunications sans fil qui est le plus dynamique de toute l'industrie des télécommunications (ACTS, Page Web). De surcroît, nous avons remarqué qu'aucune étude empirique canadienne ne s'est encore intéressée de près à ce phénomène, ni aux réactions qu'il suscite. Avec l'avènement de la technologie cellulaire de troisième génération (3G), les risques de fraudes et de piratage augmentent encore. Dès lors, les escrocs du cellulaire vont vraisemblablement continuer de profiter de la vulnérabilité des opérateurs de télécoms ainsi que de l'impunité qui leur est le plus souvent assurée. Bien que celles-ci soient généralement dirigées contre les entreprises de télécoms, soit les victimes de première ligne de ces infractions, il n'en demeure pas moins que la fraude à la téléphonie mobile fait également deux autres types de victimes indirects. Le premier type regroupe les utilisateurs du sans-fil qui, dans une large mesure, finissent par supporter les coûts de la fraude par les augmentations tarifaires des produits et des services de communications mobiles. Dans le deuxième type de victimes se retrouvent ceux dont l'identité a été utilisée contre leur gré. En conséquence, il y a un intérêt général à trouver des parades efficaces contre la fraude à la téléphonie mobile.

Notre problématique relève de la réaction sociale. Dans le cadre de cette étude de terrain, il s'agira de mettre à jour l'ensemble des réactions sociales informelles que les acteurs, qui en ont la responsabilité dans l'entreprise à l'étude, déploient contre la fraude. Les réactions formelles sont celles qui font appel à l'appareil public de régulation sociale (forces de l'ordre, institution judiciaire, politique criminelle de l'État) alors les réactions informelles sont celles qui n'y font pas appel. Ces dernières relèvent plutôt de la sphère de l'action privée, à l'intérieur de laquelle se trouvent des membres de la famille, pairs, éducateurs, associations, communautés, etc. qui exercent des pressions à la conformité sociale (Cusson, 1998 :123-125).

Dans cette étude, nous ne chercherons pas à mesurer l'importance du phénomène de la fraude par cellulaire au Canada ou au Québec; nous nous interrogeons simplement sur l'ampleur des fraudes dirigées contre une seule entreprise de télécommunications sans fil et à analyser ses réactions face à ces fraudes. Compte tenu de ce que l'entreprise en question ne déclenche pas de réactions sociales formelles, nous nous en tiendrons par conséquent à l'analyse des mesures informelles qui sont les siennes pour se protéger contre la fraude. Il s'agit donc de dégager la politique et les tactiques de cette entreprise, en décrivant ses mesures de prévention, de limitation des opportunités et de dépistage pour contrer la fraude et en mettant en évidence la rationalité et les " bonnes raisons " de cette politique. Nous voulons ultimement apprécier le degré d'adéquation entre le phénomène de la fraude et les mesures prises par l'entreprise pour y faire face. Cette recherche appliquée se propose, le cas échéant, non seulement de mettre en exergue l'éventuel décalage qu'il pourrait y avoir entre le phénomène frauduleux et la nature des moyens déployés contre lui, mais aussi d'ébaucher des propositions d'amélioration des stratégies actuellement en vigueur pour contrer la fraude affectant la téléphonie cellulaire.

Les objectifs spécifiques de notre recherche sont les suivants :

1) Présenter les données relatives à la nature et à l'ampleur du phénomène de la fraude de l'entreprise victimisée;

2) Présenter les perceptions des employés au sujet de ce phénomène de la fraude;

3) Présenter la politique générale de lutte de l'entreprise (prévention, détection, intervention), et notamment sa politique de réduction des occasions de fraude;

4) Rendre compte des choix stratégiques et de la rationalité de l'entreprise à l'égard de la fraude à la téléphonie mobile;

5) Analyser l'adéquation entre la nature et l'ampleur des fraudes et les mesures prises pour les contrer;

6) Rendre compte des perceptions des employés de l'entreprise quant aux moyens actuellement déployés par leur entreprise pour contrer le phénomène de la fraude au portable.

CHAPITRE 2 :
DÉMARCHE MÉTHODOLOGIQUE

1. L'APPROCHE QUALITATIVE

Cette recherche repose sur une démarche qualitative. Ce choix méthodologique est justifié par la nature de l'objet de recherche et les questions auxquelles nous devons répondre. Ainsi, dans cette étude, il s'agit notamment de décrire la politique anti-fraude de l'entreprise de même que l'ensemble des moyens mis en œuvre pour contrer cette infraction. Comme nous n'avons pas eu la possibilité de dresser un portrait chiffré du volume des fraudes selon les divers modes de souscription ou des montants des pertes qui affectent l'entreprise, nous avons exclu la démarche quantitative. Il faut aussi souligner le caractère exploratoire de cette recherche qui constitue une première au Canada. Notons que la communauté criminologique commence à peine à s'intéresser au phénomène de la fraude à la téléphonie mobile et aux réactions corporatives qu'elle suscite. Au sujet des recherches qui se réalisent en terrain très peu connu, Deslauriers et Kérisit (1997) précisent qu'une démarche qualitative constitue un instrument privilégié de collecte de données permettant de décrire et d'explorer un phénomène social nouveau.

Notre but est de nous familiariser avec une politique organisationnelle, en l'occurrence celle du Service de la fraude d'une entreprise canadienne de télécommunications sans fil. Pour ce faire, il s'est avéré utile de nous imprégner, sur le terrain, du quotidien des acteurs, en les observant, mais aussi en réalisant des entrevues individuelles. Nous voulions découvrir ce qu'ils avaient à dire sur le phénomène de la fraude au sein de leur entreprise, sur les stratégies corporatives déployées pour contrer ce crime et sur les difficultés rencontrées dans leur quotidien. À ce sujet, Poupart (1997) souligne que l'usage de la démarche qualitative est " un moyen de rendre compte du point de vue des acteurs sociaux et d'en tenir compte pour comprendre et interpréter leurs réalités ". (p. 175) Enfin, Mucchielli (1996) ajoute que la méthode qualitative s'applique mieux à certains types de recherche, notamment aux études de cas (Mucchielli, 1996 : voir p. 77-81). Selon la définition du *Dictionnaire des méthodes qualitatives en sciences humaines et sociales,* ce

mémoire est effectivement une étude de cas puisqu'il vise à " rapporter une situation réelle prise dans son contexte, et à l'analyser pour voir comment se manifestent et évoluent les phénomènes auxquels le chercheur s'intéresse ". (Stake, cité dans Mucchielli : 77)

2. LES TECHNIQUES DE COLLECTES DE DONNÉES

Comme pour n'importe quel objet d'étude, le choix du lieu de la recherche reposait sur divers critères. Pour des considérations pratiques, théoriques et surtout éthiques, nous ne pouvions retenir qu'un seul site pour cette étude de cas, soit celui dont nous faisions déjà partie intégrante. Notre présence en tant que chercheure sur le terrain était pour ainsi dire imperceptible car nous faisions déjà partie du personnel du service étudié depuis juin 1999, avant même que la recherche soit initiée. En ce sens, nous n'avons pas eu à négocier l'accès sur le site d'observation et notre immersion complète n'a pas eu d'incidence sur la routine de la population à l'étude. D'ailleurs, même si nous avions effectué les démarches appropriées, le caractère confidentiel des données de chacune des quatre principales entreprises de téléphonie mobile aurait constitué un empêchement à l'obtention des autorisations nécessaires pour faire une étude comparative.

Cette recherche exploratoire a été réalisée entre septembre 2000 et décembre 2003, selon trois méthodes complémentaires de collectes de données, lesquelles nous ont permis d'atteindre les objectifs que nous nous étions fixés. D'abord, le mode d'appréhension du réel par l'observation participante nous a fourni l'essentiel des renseignements qui ont été recueillis et qui nous ont permis de prendre connaissance :

- de la politique générale de lutte de l'entreprise, notamment en ce qui concerne sa politique de réduction des opportunités de fraude;
- du caractère rationnel et des choix stratégiques de l'entreprise à l'égard de la fraude à la téléphonie mobile;
- de l'adéquation entre la nature et l'ampleur des fraudes et des mesures prises pour les contrer.

Par la suite, les entretiens semi-dirigés au sein de la totalité de la population de l'entreprise étudiée ont favorisé l'approfondissement de nos observations tout en permettant aux acteurs concernés de rendre compte de leurs perceptions quant :

- au phénomène de la fraude au sein de l'entreprise
- aux moyens déployés par leur entreprise pour contrer la fraude au portable. De façon plus précise, le personnel a fait part de ses perceptions quant à la prise de risque de l'entreprise lors des nouvelles souscriptions à des services téléphoniques sans-fil, de même que ses perceptions quant au système de surveillance et de dépistage de la fraude.

Enfin, des données statistiques de l'entreprise ont permis de brosser un portrait de l'ampleur des fraudes qui l'affectent.

2.1 L'OBSERVATION PARTICIPANTE

La démarche centrale de cette recherche pour ce qui est de la collecte des données consiste en des observations participantes dans cet " univers de travail ", pour reprendre l'expression de Pires (1997), qu'est le Service des fraudes d'une entreprise canadienne de télécommunications sans fil. Ce procédé de recherche allait de soi puisque nous faisions déjà partie intégrante du milieu à l'étude depuis juin 1999. Nos observations participantes nous ont d'abord fourni de précieux renseignements pour délimiter notre objet d'étude. Dans le cadre de notre travail, nous avons également eu l'occasion d'assister à divers séminaires et réunions au cours desquels nous avons pu bénéficier d'échanges et de renseignements transmis sur le thème de la fraude à la téléphonie mobile. Cela dit, nous avons profité de notre fonction au sein de l'entreprise pour poursuivre nos observations en éprouvant personnellement et de concert avec les divers acteurs sociaux les mêmes préoccupations et difficultés que suscitent les moyens de lutte contre la fraude au sein d'une entreprise. À ce propos, Jaccoud et Mayer déclarent : " Le chercheur peut rendre compte de la réalité des acteurs parce qu'il accède aux perspectives de ceux-ci en vivant les mêmes situations ou les mêmes problèmes qu'eux. " (Jaccoud et Mayer, 1997:219).

Dès que cela fut possible, nous avons fait un compte rendu détaillé de nos observations. Par la suite, nous avons procédé à une analyse verticale de chacune des observations. Cette première étape de la stratégie d'analyse nous a permis de voir si certains thèmes ou sous-thèmes devaient être approfondis ou encore si de nouveaux thèmes pouvaient être explorés dans les observations subséquentes. Ensuite, nous avons effectué une comparaison du matériel obtenu pour chacun des deux types de fraude.

2.2 LES ENTRETIENS SEMI-DIRIGÉS

L'entretien semi-directif qualitatif permet de bien appréhender les expériences et les pratiques des personnes interviewées et d'éclairer leurs conduites sociales dans la mesure où elles ne sauraient être mieux comprises et expliquées que par les acteurs sociaux eux-mêmes (Poupart, 1997). En ce qui a trait à la profondeur des renseignements que peuvent fournir les enquêtés, Michelat (1975) écrit :

> " L'information atteinte par l'entretien non directif est considérée comme correspondant à des niveaux plus profonds, ceci parce qu'il semble bien qu'il existe une relation entre le degré de liberté laissé à l'enquêté et le niveau de profondeur des informations qu'il peut fournir. La liberté laissée à l'interviewé (la non-directivité étant toutefois relative) facilite la production d'informations symptomatiques qui risqueraient d'être censurées dans un autre type d'entretiens. " (p. 231)

Par ailleurs, pour obtenir des entretiens valables, entendus dans le sens de production d'un discours qui soit le plus vrai et le plus approfondi possible (Poupart, 1997:186), nous avons, entre autres, adopté un des principes que Poupart (1997) juge fondamental dans l'art de bien faire parler les acteurs sociaux : obtenir leur collaboration. Pour y parvenir, nous avons fermement garanti aux personnes interrogées la confidentialité quant aux sources de l'information recueillie et à l'usage purement scientifique de cette information. Mentionnons que les entrevues ont été réalisées sur les lieux du travail selon la disponibilité des interviewés et ont duré une heure en moyenne. Elles ont toutes été enregistrées après l'obtention du consentement de chaque interviewé et retranscrites de manière intégrale. Le déroulement des entrevues s'est fait dans une ambiance cordiale, la population à l'étude étant nos collègues de travail.

Il convient de mentionner qu'au moment où ce projet de recherche a été initié, à l'automne 2000, nous avions prévu d'interviewer 10 personnes : 6 analystes chargés de la détection de la fraude, 1 analyste chargé de l'investigation, 1 technicienne et 2 gestionnaires. Or, un événement imprévisible est survenu, ce qui nous a forcée à revoir à la baisse le nombre d'entrevues. En effet, le ralentissement économique a frappé de plein fouet l'industrie des télécommunications sans-fil, en 2001, tant au Canada qu'ailleurs dans le monde. L'entreprise à l'étude n'a pas été épargnée et, par conséquent, trois périodes de mises à pied ont touché son Service des fraudes en novembre 2001, en février 2002 et en mars 2003.

La baisse des effectifs, l'insécurité de l'emploi et la situation financière précaire de l'entreprise nous ont amenée à revoir le programme des entretiens. Dans un tel contexte, nous avons donc jugé qu'il était préférable d'attendre le moment opportun, soit au troisième trimestre de 2003, après que l'entreprise eût terminé son processus de recapitalisation pour réaliser les entrevues. Les premier et deuxième trimestres étaient consacrés au plan de réorganisation ainsi que de transaction et d'arrangements avec les créanciers.

En raison des événements précités et des licenciements qui sont intervenus, un nombre plus limité d'entretiens a été mené auprès du personnel du Service de la fraude. Nous avons effectué six entretiens au total : 4 auprès des analystes chargés du dépistage de la fraude, 1 auprès d'une technicienne et 1 autre auprès du seul gestionnaire restant.

2.3 LES DONNÉES STATISTIQUES

Les quelques données statistiques issues des rapports mensuels des exercices 2001 à 2003, destinées à la direction de l'entreprise, aux gestionnaires du Service des finances et au personnel du Service de la fraude, ont été obtenues sur une base privilégiée. D'ailleurs, l'autorisation de publier les données a été reconsidérée et la personne qui gère le Service de la fraude nous a finalement demandé de ne pas dévoiler trois types de renseignements qui auraient été fort intéressants dans les deux modes de souscription:

- le nombre de fraudes;
- les pertes résultant de la fraude en valeurs absolues;
- les coûts de la fraude en pourcentages et en valeurs absolues

C'est donc malgré une certaine réticence de la part de l'entreprise étudiée que nous avons pu recueillir les données à l'origine des renseignements suivants :

- les taux de fraude par rapport au chiffre d'affaires (tableau 2);
- les taux de fraude selon le mode de souscription (tableau 3);
- les manques à gagner moyens résultant des deux types de fraude (tableau 4).

Plusieurs facteurs sont à l'origine de la faiblesse des données statistiques que nous avons obtenues dans cette recherche. D'emblée, les données recueillies peuvent sembler fort partielles du fait qu'elles ne portent que sur une période de trois ans (2001 à 2003). Cela tient au fait qu'en 2000, l'information concernant la fraude au forfait prépayé n'était pas systématiquement recueillie, cette infraction ayant atteint l'entreprise qu'à partir du milieu de l'année 2000. Outre qu'elles sont très partielles, les données statistiques comportent plusieurs caractéristiques importante qui nuisent à l'exactitude du calcul du volume des fraudes. La première caractéristique, dont il était d'ailleurs impossible de tenir compte, consiste en l'importance du chiffre noir dans la criminalité frauduleuse, ce qui porte à sous-estimer l'ampleur réelle des fraudes au sein de l'entreprise étudiée. La seconde caractéristique consiste en l'absence de toute obligation pour l'entreprise de déclarer les fraudes aux organismes du contrôle social formel (police, CRTC, PhoneBusters, etc.). Le caractère confidentiel, ou à tout le moins, peu accessible des données relatives à la fraude constitue donc un défi de taille pour celui qui tente de mesurer une telle forme de criminalité. La troisième caractéristique découle des lacunes méthodologiques en ce qui a trait à la compilation des données; les résultats de l'étude, au chapitre 3 (sous 3.2), font d'ailleurs ressortir les défauts des instruments de mesure, lesquels nuisent à la fiabilité des données statistiques. La quatrième caractéristique réside en l'absence d'outils de suivi, ce qui est susceptible de nuire à la fiabilité et la validité des chiffres. Finalement, la cinquième caractéristique tient au fait que les chiffres relatifs aux taux de fraude et des manques à gagner subis par l'entreprise ne mesurent que le travail de détection sans toutefois tenir compte des efforts non quantifiés, notamment en matière de prévention, susceptibles d'influencer les chiffres recueillis. En dépit du manque de rigueur scientifique de la collecte

des données, celles-ci nous permettent néanmoins d'entrevoir l'ampleur du phénomène de la fraude et d'en apprécier les variations.

3. LES LIMITES DE LA RECHERCHE

Cette recherche comporte certaines limites qu'il convient de souligner. Premièrement, reconnaissons que notre position de chercheur réalisant des observations dans un milieu auquel il appartient déjà à un autre titre " favorise une double construction symbolique et sociale de la réalité et une double expérience contradictoire, sinon incompatible, du monde social, ce qui rend difficile une connaissance scientifique. " (Groulx, cité dans Jaccoud et Mayer, 1997:223). Il est vrai que le fait d'avoir travaillé dans le milieu a fait en sorte que nous étions nantie d'une certaine façon, d'une connaissance préalable de notre objet d'étude. Nous sommes consciente que notre position au sein du service de la fraude constitue en quelque sorte un risque de biais susceptible d'influencer nos réflexions. Au début de la recherche, il est que vrai nous occupions deux rôles parfois inconciliables pour rendre compte des résultats de nos observations. Précisons toutefois qu'au moment de l'analyse des données, nous avions déjà quitté l'entreprise et dès lors nous n'avions qu'un seul rôle à assumer, soit celui de chercheur.

Deuxièmement, il faut souligner certaines limites relatives aux études de cas. En ce qui a trait à la généralisation des résultats, Yin écrit : " Les études de cas, tout comme les expérimentations, peuvent être généralisables à des propositions théoriques et non à des populations ou des univers. " (Yin, cité dans Mucchielli, 1996:78). Ainsi, les résultats de cette étude ne sont pas forcément transposables à l'ensemble des entreprises de télécommunications sans fil canadiennes. En effet, il nous paraît douteux que l'ampleur du phénomène, les types de fraude, la politique anti-fraude[5], les moyens de lutte[6], les difficultés rencontrées par le personnel, etc. dans cette étude de cas puissent être généralisés à l'industrie canadienne du sans-fil. D'ailleurs, une des caractéristiques de l'entreprise étudiée

[5] Les conditions d'abonnement à un service téléphonique sans-fil varient d'une entreprise à l'autre.

[6] Certaines entreprises canadiennes de télécommunications sans-fil sont dotées de système expert pour effectuer leurs activités de dépistage de la fraude alors que d'autres ont leur propre système interne de détection.

est qu'elle offre essentiellement des services de téléphonie mobile numérique. Or, il y a des entreprises de téléphonie sans fil qui offrent aussi des services sur réseau analogique et qui sont donc exposées à des risques de fraude différents (piratage).

Troisièmement, Poupart (1997) rappelle que des biais résultant du contexte de l'enquête peuvent avoir des répercussions sur le discours des interviewés. Ainsi, par exemple, dans un climat d'insécurité en matière d'emploi, certains employés peuvent taire leurs appréciations réelles ou encore ne pas parler ouvertement des difficultés qu'ils vivent au quotidien. Aussi, en dépit du fait que les acteurs sociaux ont reçu des garanties fermes quant à la confidentialité des sources d'information recueillie et quant à l'usage purement scientifique de cette information, la fiabilité de leur témoignage peut s'en être trouvée affectée.

Quatrièmement, un dernier problème de méthodologie découle de la langue dans laquelle les entrevues ont été menées. Bien que toutes les personnes interviewées soient bilingues, la moitié d'entre elles maîtrise mieux l'anglais. Or, les questions administrées lors des entrevues ont été élaborées en français et elles n'ont pas été traduites. Par conséquent, une limite peut découler de la langue dans laquelle les questions ont été posées et avoir eu une influence sur les résultats des entrevues. Ainsi, il se peut qu'un vocabulaire quelque peu limité en français pour certaines des personnes interviewées, qui s'expriment mieux en anglais, les ait empêchées de dire de façon exhaustive tout ce qu'elles pensaient ou encore de dire très exactement ce qu'elles voulaient exprimer. Précisons néanmoins qu'elles ont toutes pris la peine de répondre en français alors que l'environnement de travail (outils informatiques, rapports statistiques, dialogues avec les gens de l'industrie du sans-fil, les abonnés, etc.) est essentiellement anglophone.

CHAPITRE 3 :
PRÉSENTATION ET ANALYSE DES RÉSULTATS

1. LA NATURE ET L'AMPLEUR DES FRAUDES AU SEIN DE L'ENTREPRISE

1.1 LA DIVERSITÉ DES FRAUDES

Les entretiens réalisés avec les analystes du Service de la fraude démontrent qu'en cette époque de commerce électronique, les usagers du sans-fil ont de nombreuses possibilités de se procurer les produits et services cellulaires. Un des effets non désirés du développement du commerce électronique est que, désormais, les demandes de services cellulaires à distance comportent pour les entreprises de télécommunications bien plus de risques de fraudes qu'avant. Par ailleurs, nous avons vu au chapitre 1 (section 2.1) que plusieurs types de comportements frauduleux sont commis contre les entreprises de télécommunications et que les stratagèmes des fraudeurs varient en fonction des modes de souscription. Dans le cadre de cette recherche, nous nous attardons essentiellement à deux formes de fraude. Il y a d'abord la fraude au forfait mensuel. Elle se réalise par l'usurpation de l'identité d'une personne solvable lors de la souscription à un abonnement mensuel. Ensuite, il y a la fraude au forfait prépayé. Elle se commet par l'utilisation non autorisée de numéros de cartes de crédit valides pour l'achat de cartes téléphoniques prépayées. Quels que soient les modes opératoires, le but ultime des fraudeurs est d'obtenir, sans en payer le prix, divers services de télécommunications : des appels téléphoniques, des messages textes, des courriels, des services d'Internet mobile, etc. Dans les pages qui suivent, nous allons donc examiner en quoi la fraude commise lors de la souscription à un abonnement mensuel diffère de la fraude reliée à un abonnement prépayé, à la lumière des observations que nous avons faites dans l'entreprise à l'étude.

1.1.1 Les fraudes au forfait mensuel

Lors de la souscription à un abonnement mensuel, l'usager obtient, après approbation de crédit, un forfait de temps d'antenne qui lui permet d'utiliser son appareil

téléphonique. Par la suite, l'abonné présumé reçoit une facture mensuelle. Or, les usurpateurs d'identité se servent précisément du nom d'autrui pour éviter d'avoir à acquitter des factures. D'ailleurs, il peut s'écouler un long laps de temps avant que l'activité frauduleuse soit découverte par la victime de vol d'identité ou encore par l'entreprise victimisée. En effet, dans le but de brouiller les pistes, certains fraudeurs donneront lors de la souscription de fausses coordonnées et feront en sorte que la facture ne se rende pas au domicile de la victime de vol d'identité. D'autres escrocs attendront plutôt plusieurs jours ou semaines avant d'effectuer un changement d'adresse auprès de l'entreprise. Certains fraudeurs peuvent même annoncer un changement d'adresse à l'entreprise à plusieurs reprises afin d'éviter que les factures parviennent aux victimes d'usurpation d'identité. Ces dernières découvrent généralement la fraude plus tard, au moment où on leur refuse une demande de crédit ou lorsqu'elles font l'objet d'une demande de recouvrement pour dette impayée. Une analyste du Service de la fraude confirme que des années peuvent s'écouler avant que les victimes de vol d'identité découvrent que des fraudeurs se sont emparés de leur identité pour contracter des dettes.

> *" La majorité du temps, nos propres clients s'aperçoivent de la fraude quand ils veulent faire l'acquisition d'une maison ou obtenir un prêt. Des fois, c'est détecté trois ans plus tard. "*

Selon Option consommateurs, un organisme dédié à la défense et à la promotion des intérêts des consommateurs, " les fraudeurs n'ont pas besoin d'avoir nos cartes entre leurs mains pour usurper notre identité. Ils n'ont qu'à aller chercher nos renseignements là où ils se trouvent. [...] Dans la vie de tous les jours, nous sommes tous amenés à nous identifier, tant auprès des entreprises de services publics que d'entreprises privées. Nous semons ainsi les renseignements personnels qui constituent notre identité dans de multiples banques de données fort vulnérables. C'est notamment en puisant dans ces banques de données que les fraudeurs obtiennent sans difficulté les informations dont ils ont besoin pour commettre leurs crimes ". (Option consommateurs, Page Web)

Pour mieux comprendre le mode opératoire des fraudeurs agissant lors de la souscription, les analystes de l'entreprise à l'étude ont fait ressortir deux éléments importants qui font que, par sa vulnérabilité, l'entreprise devient une cible de choix pour les fraudeurs.

La vulnérabilité de l'entreprise s'explique d'abord par les opportunités de fraude et, ensuite, par le processus d'évaluation de crédit.

1.1.1.1 *Les opportunités de fraude*

Les opportunités de fraude découlent de deux éléments caractérisant les demandes de souscription. Le premier élément est que l'entreprise n'exige pas toujours des pièces justificatives afin de s'assurer de l'identité des usagers au moment de la demande de souscription. De façon plus précise, les fraudeurs réussissent à tirer profit des degrés de sécurisation très variables des différents modes de souscription de l'entreprise. Parmi les diverses façons de souscrire à un abonnement mensuel, mentionnons les demandes de souscription en ligne (Internet), en succursale (en face à face) ou par téléphone. Les divers modes de souscription présentent des lacunes qui favorisent l'émergence d'opportunités de fraude aux dépens des opérateurs de télécommunications sans fil. Par exemple, les demandes de souscription par Internet sont moins sécurisées parce qu'elles se font le plus souvent dans l'anonymat. Par contre, les demandes de souscription faites en magasin sont à l'inverse beaucoup plus sécurisées parce qu'elles comportent une rencontre entre le client et le vendeur, ce qui assure une certaine transparence au moment de la signature de l'entente de service. De plus, une procédure formelle en matière d'authentification de l'identité du client est incluse dans cette demande de souscription. L'abonné potentiel doit présenter des pièces d'identité pour effectuer sa demande. Les abonnements auxquels le client potentiel souscrit par téléphone présentent des risques moindres car la voix offre des indications plus fiables qu'un échange de messages écrits, comme l'explique une analyste :

> *" On ne voit pas la personne [...] Mais, [comparativement aux activations en ligne] au moins, on [l'employé qui procède à l'activation] a le son de la voix. On peut associer une nationalité avec l'accent de la voix du client ou l'âge avec le ton de voix du client. "*

Le deuxième élément à la base des opportunités de fraude tient au fait que les clients potentiels n'ont que très peu de renseignements à fournir lors de la souscription. Les premiers renseignements ont trait à l'enquête de crédit. Le demandeur de crédit (usager potentiel) fournit donc des renseignements nominatifs, ses coordonnées ainsi que des renseignements personnels à l'entreprise de télécommunications sans fil. Afin de respecter la Loi fédérale sur

la protection des renseignements personnels et les documents électroniques (LPRPDE[7]), chaque entreprise ne doit collecter les renseignements concernant ses clients qu'aux seules fins commerciales pour lesquelles ces renseignements sont recueillis, notamment pour procéder à une enquête de solvabilité. Les renseignements en question sont les suivants :

1. Nom, prénom (s);
2. Coordonnées : adresse, ville, code postal, numéro de téléphone à la maison ou au bureau ou les deux;
3. Renseignements personnels : numéro d'assurance social[8] ou numéro de carte de crédit, date de naissance.

L'entreprise procède à l'ouverture d'un compte quand le demandeur répond à ses exigences de solvabilité. Le requérant doit alors fournir une deuxième catégorie de renseignements concernant les éléments essentiels d'identification sur le réseau : les numéros de série du téléphone (IMEI) et de carte à puce (SIM). Ceux-ci doivent donc être, au préalable, achetés en succursale ou chez un détaillant autorisé. L'usager déjà en possession d'un téléphone n'a qu'à se procurer une carte SIM.

1.1.1.2 *Le processus d'évaluation de crédit*

Puisqu'il n'y a aucun contrat formel à signer, les abonnés, en faisant leur demande de souscription téléphonique ou en ligne, confirment immédiatement leur acceptation des modalités et conditions prévues dans l'entente (verbale) de service. Cette entente n'est pas enregistrée par le centre d'appels. Voici les trois principales conditions de service :

Premièrement, il y a le consentement à ce que l'entreprise fasse appel à une agence de crédit pour vérifier leur solvabilité. La divulgation des renseignements personnels à une agence de crédit se fait en conformité avec la *Loi sur la protection des renseignements personnels et les documents électroniques*. Deuxièmement, les renseignements recueillis par l'entreprise demeurent confidentiels mais peuvent être divulgués à d'autres sociétés

---

[7] Voir : http://www.privcom.gc.ca/legislation/index_f.asp

[8] Les requérants de crédit ne sont pas dans l'obligation de fournir leur numéro d'assurance social pour l'enquête de crédit. Selon nos observations, de plus en plus d'abonnés sont informés des dispositions de la LPRPDE et préfèrent donc fournir leur numéro de carte de crédit au lieu de leur numéro d'assurance social. Notre expérience pratique sur le terrain nous indique également que pour les victimes de vol d'identité, il est beaucoup plus complexe et fastidieux de faire changer leur numéro d'assurance sociale auprès de Développement des Ressources Humaines Canada (DRHC) que leur numéro de carte de crédit auprès d'une société chargée de distribuer les cartes de crédit.

(banques, autres agences de crédit existantes) pour fins d'authentification de l'identité de l'abonné. Troisièmement, le requérant consent à ce que l'entreprise évalue sa solvabilité en utilisant ses noms, coordonnées et renseignements personnels. À cet effet, l'entreprise entre en contact avec le système informatique de l'une des deux grandes agences de crédit canadiennes[9]. Ce faisant, l'entreprise fournit à l'agence de crédit les renseignements qu'elle a recueillis sur son abonné. Les objectifs de l'entreprise, en matière d'enquête de solvabilité, sont d'obtenir rapidement des renseignements fiables devant permettre de :

1. déterminer si l'abonné potentiel est un bon candidat au crédit. En d'autres termes, il s'agit pour l'entreprise d'évaluer si le requérant va vraisemblablement payer son abonnement mensuel à l'échéance;
2. vérifier la validité ou la véracité des renseignements fournis par le requérant et de s'assurer de la concordance entre les données fournies par le demandeur et celles de l'agence de crédit;
3. vérifier si les renseignements personnels qui lui sont présentés ont déjà servi à faire une demande de crédit frauduleuse ou s'ils présentent des risques d'utilisation frauduleuse par un tiers.

De son côté, l'agence de crédit qui reçoit les renseignements du requérant procède immédiatement à l'évaluation de solvabilité à l'aide de sa propre base de données. Elle transmet, sur-le-champ, son évaluation de solvabilité à l'entreprise à l'aide d'un pointage de crédit composé de trois chiffres. Ce pointage reflète l'historique de crédit des individus répertoriés par l'agence. Plus le pointage est élevé, plus le requérant est solvable ou susceptible d'acquitter ses obligations financières. Dès la réception du pointage de crédit, par voie électronique ou informatique, l'entreprise de télécommunications convertit le pointage du requérant en un score allant de 1 à 6. Plus la cote de crédit est élevée, plus la probabilité

[9]Au Canada, les deux principales agences (ou bureaux) de crédit sont Equifax et TransUnion. Ces agences ne sont aucunement liées entre elles et n'échangent pas d'information sur les requérants de crédit. Comme les bureaux de crédit recueillent des renseignements de crédit de façon indépendante, elles possèdent chacune leurs propres bases de données distinctes. Les renseignements contenus dans une fiche de crédit qui sont pris en compte par l'agence de crédit lors du processus d'évaluation de la solvabilité sont présentés dans l'annexe 1. Les demandeurs de crédit ou les emprunteurs répertoriés sont des adultes, résidant au Canada, qui ont déjà fait une demande de crédit auprès d'une institution financière ou d'une entreprise qui réalise des transactions avec ladite agence de crédit. Il est à noter que les banques et les entreprises de télécommunications sans fil travaillent soit avec une seule agence de crédit, soit avec les deux agences existantes.

d'insolvabilité est grande. Comme l'indique le tableau 1, la cote de crédit attribuée influe sur certaines conditions générales de l'entente de services.

Il ressort du tableau 1 que les fraudeurs ont intérêt à subtiliser l'identité d'un individu dont la cote de crédit est favorable aux yeux de l'opérateur sans fil. Les avantages sont nombreux. Par exemple, l'usager dont la cote de crédit (1 à 3) est favorable, selon les critères de l'entreprise étudiée, peut demander qu'on lui attribue le nombre maximal de lignes téléphoniques (5). De plus, il peut avoir accès à une gamme plus étendue d'options, comme les appels internationaux ou l'itinérance internationale, lesquelles engendrent des frais supplémentaires, et pour l'entreprise, et pour l'usager. Pour leur part, les abonnés dont la cote de crédit (4 et 5) est moins favorable ont des possibilités considérablement réduites d'accès au réseau cellulaire, et ce, à double titre. D'abord, ces abonnés n'ont droit qu'à une seule ligne téléphonique au moment de la demande de souscription. Ensuite, ils ne peuvent pas obtenir l'accès aux services optionnels. Ces privilèges leur seront accordés, le cas échéant, au regard de l'évolution de leur historique de paiement avec l'entreprise. Les mêmes restrictions s'appliquent aux personnes dont la cote de crédit (6) ne répond pas aux exigences de l'opérateur quant à la cote. De plus, ces personnes doivent impérativement donner un dépôt de sécurité pour souscrire à un abonnement mensuel. En cas de refus, il leur reste la possibilité de s'abonner au service prépayé.

Selon les conditions générales de l'abonnement mensuel du tableau 1, quelle que soit la cote de crédit du requérant qui déclenche un " avertissement de fraude ", sa demande ne peut pas être traitée en ligne ou par téléphone car cet avertissement entraîne un refus temporaire. Il faut cependant préciser d'emblée que cet " avertissement de fraude " ne concerne jamais le demandeur lui-même mais indique plutôt que l'identité du demandeur a déjà été utilisée par un fraudeur. L" avertissement " inséré dans le dossier de crédit du requérant indique tout simplement aux prêteurs qu'il s'est déjà déclaré victime de vol d'identité à l'agence de crédit. L'avertissement émis par le système d'enquête de crédit invite donc l'entreprise à communiquer avec le requérant et à authentifier sa demande d'ouverture de compte. Le processus d'approbation est donc plus long car l'usager doit en fait présenter sa demande de souscription en succursale et s'identifier de façon formelle, c'est-à-dire avec des pièces d'identité.

Tableau 1

Conditions générales de l'abonnement mensuel selon la cote de crédit

Cotes de crédit attribuées par l'entreprise	Conditions spécifiques pour accéder au réseau sans fil	Nombre maximal de lignes téléphoniques	Options autorisées (sur demande)
1 à 3 (très favorable)	Aucune	5	Oui
4 (favorable)	Aucune	1	Non
5 (moins favorable)	Aucune	1	Non
6 (non favorable)	Dépôt en garantie	1	Non

1 à 6 et assorties d'un " avertissement de fraude " émis par l'agence de crédit	L'alerte indique que les renseignements personnels du futur requérant ont déjà servi à faire une demande de crédit frauduleuse. Cette demande de crédit ne peut pas être traitée en ligne ou par téléphone. L'usager doit en effet présenter sa demande de souscription en succursale et s'identifier de façon formelle, c'est-à-dire en présentant des pièces d'identité.

1.1.1.3 *L'authentification des clients qui désirent des options*

Par ailleurs, au début de l'année 1999, l'entreprise a fait œuvre de pionnière en étant le premier opérateur canadien à instaurer une politique destinée à resserrer les critères d'octroi d'options aux abonnés. Le tableau 1 montre que la requête n'est n'autorisée qu'aux clients qui en font la demande et dont la cote de crédit se situe entre 1 et 3. Bien que la mise en service soit gratuite, les frais reliés aux services optionnels ne sont pas compris avec les forfaits mensuels de temps d'antenne. Rappelons que l'entreprise facture séparément les frais d'appels internationaux et les frais d'itinérance internationale aux abonnés qui voyagent sur le réseau sans fil d'un concurrent ou d'un partenaire. C'est la raison essentielle pour laquelle ces options ne sont autorisées qu'aux catégories d'abonnés dont la probabilité de solvabilité est la plus grande (cotes 1 à 3). Les usagers, dont la cote est favorable, souhaitant effectuer des appels internationaux à partir du Canada ou encore de se déplacer à l'étranger (itinérance internationale) doivent en faire la demande 48 heures avant la mise en service de ces options. Le technicien du Service de la fraude a comme mandat d'authentifier les déclarations des clients et de vérifier leurs renseignements personnels avant de leur accorder des options. Les moyens d'authentification sont présentés au point 2.3.1. L'authentification des clients a pour

but de limiter ce qu'il est convenu d'appeler " la fraude interurbaine " ou " la fraude en mode itinérance internationale ". L'équipe assignée à la fraude dispose d'une personne affectée à l'authentification de toutes les demandes de services optionnels depuis les importantes fraudes survenues au cours de l'été 1999. En effet, cette mesure corrective a été mise en place après qu'une analyste du Service de la fraude, dans le cadre d'une procédure de vérification de rapports, a détecté des utilisations abusives de la part de quelques abonnés en mode itinérance internationale. L'analyste interviewée dit avoir mis au jour l'existence d'un groupe de fraudeurs. Son enquête lui a permis de découvrir les faits suivants :

1- Un réseau de fraudeurs a acheté quelques 25 cartes SIM ainsi que cinq appareils portables (IMEI). Tout ce matériel a été envoyé à l'étranger, en l'occurrence en Europe.

2- De faux comptes ont été créés, lors de souscriptions à des forfaits mensuels, sur la base d'identités volées de personnes solvables. La cote de crédit de chacune des victimes d'identité a permis l'activation de cinq lignes téléphoniques cellulaires, soit le maximum autorisé dans le cadre de la politique de l'entreprise. Les usurpateurs d'identité ont obtenu la mise en service des options " accès aux appels outre-mer " et " itinérance internationale " lors de la demande de souscription.

3- Un nombre volumineux d'appels a été lancé dans les heures suivant l'activation des lignes téléphoniques, tous à partir de l'étranger : Côte d'Ivoire, Irlande, France, Italie, Suisse, etc.

4- Les pertes découlant de ces fraudes ont totalisé 150 000 $ en trois fins de semaine.

Enfin, les fraudeurs n'ont jamais été identifiés et l'entreprise n'a jamais récupéré le paiement de leurs communications.

1.1.2 **Les fraudes par cartes téléphoniques prépayées**

À partir du mois de mars 2000, les usagers de l'entreprise étudiée dont la demande de crédit ne répondait pas aux normes de solvabilité de l'entreprise ou qui ne désiraient pas

recevoir de factures mensuelles avaient la possibilité de souscrire à un forfait prépayé. Contrairement à l'abonnement mensuel, ce mode de souscription sans facture est accordé à n'importe quel usager qui en fait la demande. Comme aucune vérification de crédit n'est faite, les renseignements nominatifs et les coordonnées fournies par le requérant ne sont vérifiés d'aucune façon. La recharge téléphonique prépayée, qui peut être effectuée selon trois modes de réapprovisionnement, que nous verrons plus loin, a malheureusement entraîné de nouvelles possibilités de fraude. Plus précisément, la recharge téléphonique par carte de crédit dont il est précisément question dans cette recherche, comporte de nombreuses opportunités de fraude. Ces opportunités, toutes inhérentes au dispositif de paiements électroniques de l'entreprise, ont été largement exploitées par les escrocs par carte de crédit.

Avant d'énumérer ces opportunités, il s'agit de comprendre l'ordre des opérations effectuées par un usager qui désire payer d'avance pour un nombre donné de minutes d'utilisation de temps d'antenne:

1- L'usager doit se procurer un téléphone, une carte SIM et une carte prépayée. Sur la carte prépayée figure un montant en dollars et un nombre de minutes de temps d'antenne prépayé, et à l'intérieur se trouve un code secret de 12 chiffres.
2- L'usager doit téléphoner à un représentant du centre d'appels de l'entreprise pour demander la création de son compte d'usager. Pour ce faire, il doit donner au centre d'appels, son nom, ses coordonnées et les numéros de série du téléphone (IMEI) et de la carte SIM.
3- L'usager reçoit un numéro de téléphone cellulaire ainsi qu'un code d'accès personnel temporaire de quatre chiffres pour accéder à son compte prépayé.
4- L'usager doit accéder à son compte prépayé et suivre les instructions du service automatisé :
    a. composer le numéro de téléphone cellulaire de 10 chiffres attribué par l'entreprise à l'abonné;
    b. changer le code d'accès personnel temporaire (de quatre chiffres);
    c. entrer le code secret de 12 chiffres qui lui permettra de déposer le montant (en dollars) figurant sur la carte prépayée.

5- L'abonné a alors accès au réseau sans fil et peut utiliser son portable[10]. Le compte de l'abonné sera ensuite débité lors de l'utilisation de l'appareil. Le client est dans l'impossibilité de téléphoner lorsque son crédit tombe à zéro.

6- L'abonné du prépayé peut recharger son compte en tout temps. À chaque rechargement, le crédit restant est ajouté au montant de la nouvelle recharge de temps d'antenne prépayé. Il existe trois modes de réapprovisionnement d'un compte téléphonique prépayé :

   a. acheter des cartes de temps d'antenne prépayé chez un détaillant au Canada.

   b. acheter un code de rechargement à 12 chiffres par le biais des guichets automatiques des institutions financières participantes. Les achats de codes recharges sont effectués avec une carte bancaire. Ensuite, ces achats de recharge téléphoniques sont débités de la même façon que tous les autres achats réglés avec la carte bancaire;

   c. acheter une recharge, sans se déplacer, par carte de crédit en utilisant le service automatisé du prépayé. Les achats des recharges sont alors portés au relevé de compte des titulaires de carte de crédit.

L'astuce des escrocs par cartes de crédit, relativement simple, se réalise en deux phases. La première consiste à créer un compte d'usager en fournissant des renseignements nominatifs et des coordonnées factices qui ne sont pas authentifiés par l'entreprise (opération 2). À la deuxième phase, il s'agit pour le fraudeur de fournir un numéro de carte de crédit valide pour acheter une recharge téléphonique prépayée à l'insu de son titulaire légitime. Les fraudes aux cartes prépayées qui ont été recensées prennent toujours la forme d'opérations à distance, c'est-à-dire sans la présence physique de la carte de crédit (opération 6c).

Pour commettre ce genre de fraude, les escrocs ont exploité certaines faiblesses du système de paiement par cartes de crédit. Voici les cinq principales opportunités de fraude qui ont été relevées :

1. Absence d'authentification : après avoir créé des comptes fictifs au prépayé, des fraudeurs ont profité de l'absence d'authentification des renseignements nominatifs par l'entreprise et ce, jusqu'à la première phase de l'implantation du dispositif de sécurisation des cartes de crédit. En effet, l'entreprise ne demandait pas les renseignements de base (nom, adresse de facturation, numéro de téléphone) des titulaires de cartes de crédit avant de porter

[10] Certains services ne sont pas accessibles. Les clients du service prépayé ne peuvent utiliser le service d'itinérance internationale sur d'autres réseaux de télécommunications ni faire d'appel international.

les achats aux comptes des cartes. Des numéros de cartes de crédit relevés sur des factures de restaurants ou de station d'essence pouvaient donc facilement être utilisés à des fins frauduleuses. Un analyste de Service de la fraude a confirmé la facilité avec laquelle des fraudeurs se sont emparés de numéros de cartes de crédits d'autrui pour approvisionner leur propre compte téléphonique prépayé :

> *" N'importe qui ayant un service prépayé pouvait utiliser la carte de son ami, de quelqu'un d'autre qu'il ne connaissait pas. "*

Pour maximiser l'utilisation frauduleuse des communications prépayées et passer le plus de coups de fil possible, des escrocs ont effectué concurremment les deux types d'opérations suivantes à l'aide de numéros de cartes de crédit valides :

a) la recharge à distance de plusieurs comptes d'usagers au moyen d'un seul numéro de carte de crédit : il s'agissait d'utiliser la même carte de crédit pour réapprovisionner le plus grand nombre possible de numéros de téléphone cellulaire au prépayé.

b) les transactions multiples à l'aide de plusieurs numéros de cartes de crédit différentes pour un seul compte d'usager : à l'inverse, il s'agissait d'utiliser de nombreux numéros de cartes de crédit pour réapprovisionner le même numéro de téléphone cellulaire au prépayé.

2. Absence de limites : cependant, force est de constater qu'au fur et à mesure que le dispositif de sécurisation a été renforcé vers la fin de l'année 2000, le mode opératoire des fraudeurs s'est adapté. Par exemple, un système de détection a été mis en place afin d'identifier plus facilement les fraudeurs qui utilisaient à la fois les deux derniers stratagèmes. Des fraudeurs, pour déjouer le dispositif de détection, adoptant des tactiques plus prudentes, ont opté pour l'un ou l'autre des stratagèmes précités plutôt que pour les deux en même temps. Par après, pendant la mise en œuvre des premières mesures de précaution (fin 2000), des malfaiteurs se sont mis à exploiter une deuxième faiblesse des politiques de l'entreprise en matière de recharges prépayées. Cette faille avait trait à l'absence de limites sur :

a) le nombre quotidien de recharges. Ainsi, plusieurs recharges pouvaient être faites au cours d'une seule journée.

b) le crédit téléphonique maximum pouvant être porté à un compte prépayé. Il n'y avait pas encore de politique à cet égard. Nous verrons dans le cadre des mesures de prévention (2.1.2) que l'entreprise a finalement exigé que le solde de crédit téléphonique soit inférieur à 125 $ avant d'effectuer une nouvelle recharge.

3. Absence du code de sécurité : une faiblesse dans le système de recharge des cartes prépayées à distance tenait au fait que les usagers n'avaient pas à donner le code de sécurité (de trois ou quatre chiffre) figurant à l'endos de la carte de crédit.

4. Absence de critères pour identifier les cartes de crédit admissibles : l'acceptation des cartes de crédit n'était pas réservée aux cartes canadiennes. Des fraudeurs ont donc utilisé des cartes de crédit émises à l'étranger. Conséquemment, un long laps de temps pouvait s'écouler avant qu'un émetteur ou un titulaire de carte de crédit exprime une opposition à l'endroit d'une transaction frauduleuse effectuée sur son compte.

5. Absence d'une liste noire de cartes de crédit : comme il n'existait pas de liste noire de cartes de crédit ayant déjà servi à frauder, aucun dispositif de sécurisation n'était en mesure d'empêcher automatiquement la réutilisation d'une carte de crédit ayant déjà servi à réaliser des recharges frauduleuses aux dépends de l'entreprise à l'étude, ni même l'utilisation de cartes ayant déjà été utilisées à des fins illicites auprès d'autres entreprises. À l'instar des fraudeurs agissant lors de la souscription, les usurpateurs d'identité de détenteurs de cartes de crédit utilisaient leurs comptes d'usager jusqu'à ce que leurs activités frauduleuses soient détectées ou rapportées. Souvent, les titulaires de cartes de crédit victimes de fraudes ne découvrent pas les transactions frauduleuses au moment où elles sont commises. Généralement, les recharges frauduleuses par cartes de crédit ne sont mises à jour qu'au moment où les titulaires reçoivent leur état de compte ou un appel téléphonique de la part de l'émetteur de la carte de crédit ou de l'entreprise à l'étude (du marchand dans le jargon des institutions de cartes de crédit). De plus, parce que l'entreprise étudiée et les

sociétés de cartes de crédit travaillent en vase clos[11], chacune prend elle-même ses propres mesures pour communiquer avec ses clients. L'entreprise à l'étude prend donc elle-même l'initiative de valider certaines transactions suspectes auprès des titulaires de cartes. La validation ou l'authentification d'une transaction effectuée par carte de crédit consiste essentiellement à téléphoner au détenteur légitime de la carte et à obtenir la confirmation à savoir qu'il est toujours en possession de sa carte et que c'est bien lui qui l'utilise. De manière générale, ce sont les alertes émises par le dispositif de sécurité de l'entreprise et utilisées par le personnel du Service de la fraude de l'entreprise, qui déclenchent le processus d'authentification de celui qui cherche précisément à utiliser la carte. Voici les trois types d'avis ou d'alerte qui peuvent résulter du processus d'authentification de l'identité d'un usager ayant utilisé ou tenté d'utiliser une carte de crédit pour le réapprovisionnement d'un compte téléphonique prépayé.

1. Des transactions multiples ont été effectuées à l'aide d'un seul numéro de carte de crédit : rechargement à distance de plusieurs comptes d'usagers;

2. Des transactions multiples à l'aide de plusieurs numéros de cartes de crédit différentes ont été effectuées pour recharger un seul compte d'usager ;

3. Différentes transactions faites avec la même carte ont été refusées dans les jours ou les semaines précédents par les institutions émettrices de cartes de crédit[12] pour toutes sortes de raisons possibles : utilisation non autorisée (ou fraude), vol, perte, insuffisance de fonds, etc. Fait à noter, c'est le seul moment où l'entreprise étudiée est en mesure de recevoir, en vertu des accords passés avec elles, des informations de la part des sociétés émettrices de cartes de crédit.

Dans les cas où des transactions avaient été refusées par la société émettrice de carte de crédit (n° 3), il s'agissait pour le Service de la fraude d'effectuer des vérifications auprès

[11] Il n'existe pas d'entente formelle en matière d'échanges d'informations ou de coopération entre l'industrie du sans-fil et les sociétés émettrices de cartes de crédit.

[12] Toutes ces institutions financières compilent régulièrement les informations (nom, # carte, date de la transaction, montant de la transaction, numéro d'autorisation, etc.) sur la base desquelles des transactions ont été refusées. Ainsi, toute entreprise, et notamment l'entreprise à l'étude, peut recevoir hebdomadairement, à titre informatif de chaque institution financière, la liste des transactions refusées dont elle aurait dû bénéficier.

des titulaires des cartes, au coup par coup, afin de vérifier si les numéros de cartes de crédit refusés n'avaient pas déjà préalablement servi à des recharges téléphoniques prépayées. Rappelons que les victimes de fraudes par cartes de crédit ne découvrent pas forcément les transactions frauduleuses au moment où elles sont réalisées. Les pertes financières causées par les fraudes au prépayé et dont il est question dans cette étude, sont principalement supportées par l'entreprise. En effet, en ce qui concerne les paiements par cartes de crédit à distance (sans présentation de carte physique), le risque est supporté par les marchands qui acceptent cette modalité de paiement en cas de fraude. Ça résulte de ce qu'il leur est impossible de procéder à une vérification formelle, c'est-à-dire sur la base du relevé imprimé de la transaction. Par contre, quand les paiements par cartes de crédit se font en succursale (avec carte physique), les pertes sont supportées par l'institution émettrice de carte de crédit si le marchand est en mesure de rendre vraisemblable qu'il a vérifié l'authenticité de l'identité de l'abonné potentiel, c'est-à-dire comparé la signature à l'endos de la carte avec celle qui est apposée sur le reçu de la transaction. Cela se fait préalablement avec le relevé écrit de la transaction.

1.2 L'AMPLEUR ET L'ESTIMATION DU PHÉNOMÈNE DE LA FRAUDE

1.2.1 Des données rassurantes quant aux pertes frauduleuses

La mission du Service de la fraude consiste à réduire le taux global de fraudes. Celui-ci est obtenu par la formule suivante : somme des fraudes recensées divisée par le chiffre d'affaires. À la demande de l'entreprise étudiée, aucune valeur absolue sur l'ampleur de la fraude n'est divulguée en raison de la nature strictement confidentielle de cette information. Ainsi, le tableau 2 présente des données relatives à l'évolution des taux globaux de fraude quant aux biens et services sans fil. Tout d'abord, il y a lieu de mentionner que les des taux de fraude annuels demeurent relativement minimes et que les statistiques sont très rassurantes, par rapport aux taux émanant de l'ensemble du marché du sans-fil : Selon Collins (1999b) et le Communication Fraud Control Association - CFCA (Ericsson, Page Web), *le* taux moyen de fraude se situe entre 3 et 5 % du chiffre d'affaires des entreprises de télécommunication sans fil.

En 2001, l'ampleur de la fraude recensée par l'entreprise à l'étude ne représentait que 0,27 % de l'ensemble du chiffre d'affaires. L'année suivante, il y a eu une légère baisse du taux de fraude, passant de 0,27 % (en 2001) à 0,22 % en 2002. Pour ce qui est de l'exercice 2003, l'entreprise étudiée déclare avoir subi un taux annuel de fraudes qui ne représente que 0,12 % du chiffre d'affaires. Bien que le taux de 2001 était déjà fort bas, il a diminué encore de 55% en 2 ans.

Tableau 2

Taux de fraude par rapport au chiffre d'affaires sur trois ans

2003	0,12 %
2002	0,22 %
2001	0,27 %

Les données de l'année 2001 du tableau 3 indiquent une proportion à peine supérieure des fraudes aux paiements électroniques de recharges téléphoniques prépayées (51,58 %), par rapport aux fraudes à la souscription à un forfait mensuel (48,42 %). D'après les chiffres d'affaires de l'exercice 2002, la proportion de fraudes à la souscription était considérablement plus important (96,57 %) que celle des fraudes aux cartes prépayées effectuées par paiements électroniques (3,43 %). Au vu de la répartition des fraudes selon le mode de souscription (tableau 3), il semble que le phénomène de la fraude des cartes prépayées est en forte diminution. Nous supposons que cette diminution est responsable de la baisse globale, bien que minime, du taux annuel de fraude, qui est passé de 0,27 % en 2001 à 0,22 % en 2002 (tableau 1). Nous présumons aussi que cette diminution résulte notamment des mécanismes de sécurisation des paiements électroniques (ou par cartes de crédit) qui ont été déployés par l'entreprise dès la fin de l'an 2000. Mais qu'elle résulte principalement d'un déplacement de la fraude au forfait prépayé vers la fraude au forfait mensuel.

Tableau 3

Répartition des fraudes selon le mode de souscription sur trois ans

	Fraudes au forfait mensuel (%)	Fraudes au forfait prépayé (%)
2003	97,10	2,90
2002	96,57	3,43
2001	48,42	51,58

Bien que le taux de fraude par paiement électronique de cartes téléphoniques prépayées ait régressé en 2002, le coût moyen des pertes par ligne a pour sa part augmenté, passant de 150 $ en 2001 à 168 $ en 2002 (Tableau 4). L'année suivante, soit en 2003, il y a eu une diminution considérable des pertes moyennes résultant de fraudes aux cartes téléphoniques prépayées (de 168 $ à 44 $). Si les variations des pertes moyennes sont relativement en matière de prépayé, nous ne pouvons en dire autant des pertes découlant de fraude à la souscription. Tandis que les pertes résultant des fraudes aux cartes prépayées ont fondu de 71 % en à peine deux ans, passant de 150 $ en 2001 à 44 $ en 2003, les fraudes à la souscription ont causé des pertes moyennes qui ont légèrement augmenté, passant de 212$ en 2001 à 225 $ en 2002, ce qui représente une croissance de 6 %. En 2003, ces pertes moyennes ont atteint 264 $, ce qui représente une augmentation de 15 % par rapport à 2002 et de 20 % par rapport à 2001.

Tableau 4

Manques à gagner moyens résultant des fraudes selon le mode de souscription sur trois ans

	Fraudes au forfait mensuel ($)	Fraudes au forfait prépayé ($)
2003	264	44
2002	225	168
2001	212	150

1.2.2 La fiabilité des données relatives au volume de la fraude

Le chiffre noir en criminologie nous incite à relativiser les données de l'entreprise sur la fraude. En effet, les analystes consultés sont d'avis que l'ampleur de la fraude à la souscription est difficile à mesurer et qu'il faut appréhender les statistiques avec prudence. De façon unanime, les analystes du Service de la fraude n'hésitent pas à dire que les statistiques de l'entreprise comportent certaines disparités par rapport à la réalité du phénomène de la fraude. De fait, les statistiques ne recensent que des cas où il y a eu intervention réactive. Les données ne prennent pas en considération les fraudes qui n'ont pas fait l'objet d'une intervention réactive du Service de la fraude. Les interventions de nature réactive se produisent à la condition que des employés soient avisés d'une activité potentiellement frauduleuse par le biais d'un système de détection. Les données du Service de la fraude correspondent donc uniquement aux fraudes recensées par le service. Elles ignorent donc tout du chiffre noir de la fraude, et donc du préjudice économique qui en résulte.

1.2.2.1 *Un phénomène sous-estimé*

Parmi les fraudes non comptabilisées, il y a d'abord celles " qui ne sont pas repérées et rapportées ", qui ne sont donc pas encore connues ou qui ne seront jamais mises à jour. Il

peut, par exemple, y avoir des cas de fraude reliées à la souscription qui ne sont pas portés à l'attention de l'entreprise ou de la victime d'usurpation d'identité, et donc non recensés comme tels. Tant et aussi longtemps que la fraude n'est pas rapportée à l'agence de crédit ou à l'entreprise victimisée, le montant à payer est simplement inscrit, par l'une des deux agences de crédit, sur la fiche de crédit de la personne dont l'identité a été empruntée.

Il y a de plus les erreurs de classement de la fraude, c'est-à-dire " les fraudes traitées comme de simples défauts de paiement ", qui sont répertoriées par le Service du recouvrement et portées sur le compte d'une victime de fraude. L'ampleur de ce type d'erreur est difficilement quantifiable car l'entreprise ne dispose d'aucunes données statistiques à cet égard. À défaut de nous donner une estimation même approximative de ces fraudes mal classées, la responsable du département de la fraude explique pourquoi de nombreuses fraudes ont vraisemblablement été traitées comme de simples cas d'insolvabilité.

> *" En 2001, [...] on avait la fraude prepaid [au forfait prépayé] par dessus la tête [...].Tu n'avais pas le temps de regarder tous les comptes [...] Tu avais moins de temps à dévouer à tes postpaids [fraudes au forfait mensuel]. C'est sûr que tes postpaids [fraudes au forfait mensuel] se retrouvaient en recouvrement. Ils étaient désactivés pour non-paiement quand, en réalité, c'était de la fraude. "*

Le Service des fraudes de l'entreprise reçoit régulièrement des demandes d'enquête provenant du Service d'aide aux victimes de fraude de l'agence de crédit de l'une des deux principales agences canadiennes de renseignements sur la solvabilité. Ces demandes d'enquête sont émises à la suite de plaintes de présumées victimes de vol d'identité qui prétendent qu'il y a eu utilisation de leurs informations personnelles pour une demande de service téléphonique sans fil. L'agence de crédit envoie à cette occasion un relevé à l'entreprise qui a accordé du crédit. Sur les demandes d'enquête figurent la date à laquelle l'entreprise a accordé du crédit de même que les renseignements personnels qui ont servi la demande frauduleuse de souscription. Généralement, les demandes d'enquête sont donc initiées par les personnes victimes d'usurpation d'identité. Il convient de mentionner que toute personne a le droit de consulter sa fiche de crédit auprès de l'une des deux agences nationales de crédit, de contester tout renseignement inexact, de la faire vérifier auprès des créanciers et, le cas échéant, de faire corriger les informations inexactes. Dans ce cas,

l'agence de crédit a trente jours pour faire enquête auprès des créanciers et communiquer une réponse à la victime de fraude.

En pareilles circonstances, les tâches du Service d'aide aux victimes de fraude de l'agence nationale de crédit sont les suivantes :

1- guider les victimes quant aux démarches à effectuer auprès des fournisseurs de crédit. (ex : les aviser qu'elles ont la responsabilité de communiquer avec le fournisseur de crédit, de signaler l'incident à un service de police, à la seconde agence canadienne de crédit nationale, à l'institution émettrice de carte de crédit si la fraude implique une carte de crédit et enfin à Développement des Ressources Humaines Canada (DRHC) si la fraude implique le numéro d'assurance social) ;

2- noter l'incident de fraude dans le dossier de crédit de la victime en inscrivant une alerte pour aviser les futurs commerçants qui feront à l'avenir crédit à cette personne qu'une demande de crédit frauduleuse a déjà été faite ;

3- apporter les modifications utiles à l'historique de crédit des victimes (ex : supprimer la date et l'identité de l'entreprise qui a fait crédit, la note concernant la dette impayée, etc).

Malgré toutes les démarches des victimes de fraude auprès de l'entreprise, celle-ci n'en tire pas d'avantage pour mettre à jour plus de cas de fraude. Ce ne sont que les victimes qui bénéficient de la suite qui est donnée aux demandes d'enquête provenant du Service d'aide aux victimes de fraude de l'agence de crédit.

1.2.2.2 *Les données sur les fraudes aux cartes prépayées*

S'il faut relativiser l'exactitude des données sur la fraude lors de la souscription, la fraude aux cartes prépayées est quant à elle beaucoup plus facile à mesurer. Il ne fait aucun doute que les données sur ce type de fraude sont considérablement plus fiables en raison du taux de reportabilité (ou de fraudes rapportées par les victimes ou les banques). De façon générale, nous avons observé que les sociétés émettrices de cartes de crédit ont, dans une large mesure, toujours mené la même politique en ce qui concerne les transactions à distance.

En effet, elles remboursent totalement les consommateurs et ceux-ci se libèrent de toute responsabilité en cas de fraude si :

1. la transaction a été effectuée sans qu'il y ait eu présentation d'une carte (donc par téléphone ou par Internet);

2. la fraude a été dénoncée dans les 90 jours suivant la date de la transaction.

Bref, comme les sociétés émettrices de cartes de crédit remboursent les victimes de fraude qui font opposition, les titulaires de cartes de crédit lésés ont donc intérêt à dénoncer les transactions frauduleuses par paiements électroniques. Quant à eux, les commerçants qui acceptent des paiements électroniques doivent supporter une bonne partie des frais relatifs à la fraude. Ces frais comprennent généralement le montant de la fraude en opposition et des frais administratifs.

En somme, nous soutenons que les statistiques de l'entreprise ne fournissent pas de mesure fiable de l'ampleur de la fraude, notamment en raison de la façon dont les données sont compilées. Il n'empêche que les données partielles fournies par l'entreprise étudiée nous permettent tout de même de suivre l'évolution du phénomène de la fraude, c'est-à-dire de savoir si son volume augmente ou diminue.

1.2.3 Les perceptions du phénomène de la fraude par les employés de l'entreprise victimisée

Compte tenu des taux de fraude relativement minimes que déplore l'entreprise étudiée, cinq employés sur six semblent considérer le phénomène de la fraude comme un problème peu inquiétant. À ce sujet, celle qui gère le Service de la fraude est d'avis que les résultats peu alarmants indiquent que le phénomène de la fraude est en baisse et par conséquent contrôlé, non seulement au sein de l'entreprise, mais également dans l'ensemble de l'industrie canadienne des télécommunications :

> *" Ils [les opérateurs de télécommunications] n'ont jamais vu de mois [où le taux de fraude est] si bas que ça. C'est comme s'ils [les fraudeurs] étaient partis aux États-Unis. "*

La responsable du Service de la fraude semble croire à un déplacement géographique du phénomène de la fraude, vers les États-Unis. À son avis, ce mouvement serait attribuable au fait que l'industrie états-unienne des télécoms a mis en place moins de mesures préventives que son voisin canadien. Cela dit, en dépit des statistiques plutôt rassurantes, une technicienne a perçu le phénomène de la fraude d'une toute autre manière. Sa perception du phénomène de la fraude semble plus inquiétante que celle du reste des personnes interviewées. La technicienne semblait grandement se fier à ses impressions quant au chiffre noir et a fait part de son intuition :

> *" Moi, je sais que c'est plein [de cas de fraude]. Je pense que les fraudeurs sont sur une autre avenue [et sont en mesure de déjouer les mesures de lutte de l'entreprise]. "*

Même si le phénomène de la fraude ne passe pas pour un grave problème au sein de l'entreprise étudiée, l'ensemble des personnes interrogées semble exprimer une certaine acceptation résignée du phénomène. En effet, une analyste semblait plutôt dire que la fraude est un aléa inévitable :

> *" On [l'entreprise] n'est pas à l'abri des fraudes. On ne sera jamais à l'abri des fraudes. "*

Cette perception du phénomène de la fraude visant l'entreprise est également partagée par une deuxième analyste, selon qui il serait insensé de croire que l'entreprise puisse se mettre à l'abri des fraudes. Malgré l'ensemble des moyens de prévention et de détection déployés par l'entreprise dans le cadre de sa lutte contre la fraude, l'employée affirme, non sans résignation :

> *" On a beau avoir tous les outils nécessaires pour en éviter le plus possible, mais à quelque part, les fraudeurs ont toujours le dessus sur nous autres. Ils sont toujours un petit peu plus vite que nous autres. [...] la fraude, il va toujours y en avoir. "*

De plus, une autre analyste soutient que le phénomène de la fraude est un problème généralisé et que son entreprise ne fait pas bande à part dans l'industrie du sans-fil. Selon elle, tant et aussi longtemps que l'entreprise continuera à privilégier des mécanismes de

souscription à distance (Internet et téléphone) et de vérification de crédit peu rigoureux, les demandes de souscription comporteront des risques de fraude. En dépit de la légèreté de la procédure d'abonnement à des services de téléphonie mobile, elle ne conclut pas pour autant à un manque de vigilance de la part de l'entreprise :

> *" On suit l'industrie... simplement. [...] Malheureusement, toutes les compagnies sont en train de faciliter l'activation. "*

2. LA POLITIQUE ANTI-FRAUDE DE L'ENTREPRISE

L'entreprise a adopté une politique afin de contrer les fraudes lors de la souscription et celles aux cartes prépayées. Cette politique repose sur trois approches parallèles et complémentaires qui continuent d'être renforcées année après année. Brièvement, la première approche consiste à déployer un arsenal préventif. À titre d'exemple, l'entreprise a recours à des dispositifs de sécurité visant, pour chacun des deux modes de souscription (avec et sans abonnement), à réduire les possibilités de fraudes. La deuxième approche vise le dépistage des usagers soupçonnés d'accéder frauduleusement au réseau sans fil lors de la souscription. Une équipe est exclusivement assignée à cette tâche depuis le tout début des opérations de l'entreprise. Enfin, la troisième approche vise à déterminer le cadre d'intervention des employés du Service de la fraude envers les auteurs de fraudes présumées.

2.1 LES MESURES DE PRÉVENTION EN PLACE

2.1.1 Le système d'enquête de crédit

Comme nous l'avons déjà mentionné au point 1.1.1.2, au moment de l'enquête de crédit, l'entreprise recueille et utilise les renseignements personnels des abonnés potentiels en vue d'atteindre les trois objectifs suivants :

1- Évaluer sa solvabilité;

2- S'assurer que ses renseignements personnels n'ont pas déjà été utilisés dans le cadre d'une demande frauduleuse;

3- Vérifier la véracité de ses renseignements personnels;

L'atteinte de ces objectifs se réalise par un croisement de l'information recueillie auprès de l'abonné potentiel avec celle qui est fournie par la base de données de l'agence de crédit. D'abord, dans le but de fournir une évaluation globale de solvabilité, nous avons déjà mentionné que le système d'enquête de crédit prend en compte une panoplie de renseignements de crédit personnels pour, ultimement, émettre un pointage de solvabilité. Ensuite, pour prévenir les demandes de souscription frauduleuses, le système d'enquête de crédit est doté d'un double mécanisme de protection. D'une part, comme le démontre le tableau 1, le système refuse, temporairement, toute demande de crédit assortie d'un " avertissement de fraude ". Le refus d'une demande de crédit pour un compte d'usager n'est toutefois pas définitif. Afin d'augmenter le degré de sécurisation de la demande de crédit du requérant, cette dernière ne pourra pas être traitée en ligne ou par téléphone. Le client doit donc présenter sa demande d'abonnement mensuel et s'identifier formellement dans un point de vente. D'autre part, afin de réduire les risques d'activités frauduleuses, le système d'enquête de crédit est en mesure de signaler des anomalies par un croisement de l'information recueillie auprès de l'abonné potentiel et celle fournie par la base de données de l'agence. Le cas échéant, un " avertissement d'anomalie " est émis à titre d'information seulement à l'intention du personnel de la fraude de l'entreprise à l'étude. Ces avertissements servent, à titre informatif, de procédures d'authentification de l'identité des requérants que nous examinerons au point 2.3.1. Contrairement à l' " avertissement de fraude " qui entraîne un refus temporaire, avec un " avertissement d'anomalie", les employés du Service de la fraude peuvent, selon la nature des anomalies constatées, décider ou non de faire enquête en vue de découvrir une fraude éventuelle. Voici quelques exemples d'anomalies:

- Un numéro d'assurance social ayant déjà servi à une demande frauduleuse
- Un numéro d'assurance social retiré
- Un Numéro d'assurance social invalide
- Une adresse de facturation ayant déjà servi à une demande frauduleuse
- Une adresse de facturation associée à une boîte postale
- Une adresse de facturation associée à un centre de détention
- Un numéro de téléphone associé à un téléphone public
- Un numéro de téléphone associé à un téléphone portable
- Un numéro de téléphone ayant déjà servi une demande frauduleuse

- Une date de naissance erronée

2.1.2 La sécurisation des paiements par carte de crédit

L'ampleur des pertes attribuables aux fraudes prépayées a incité l'entreprise à s'attaquer de front à ce nouveau problème au cours des derniers trimestres de l'année 2000. En effet, les premières stratégies réactives ont été élaborées dès l'année suivante, en 2001, pour contrer ces fraudes aux proportions inquiétantes. Ces mesures avaient pour but de renforcer la sécurisation des paiements par cartes de crédit, dont les faiblesses ont été exposées au point 1.1.2. Les cinq premières mesures se résument comme suit :

1- Le nombre maximal de recharges hebdomadaires a été établi à trois;

2- La somme maximale hebdomadaire des recharges a été établie à 150 $;

3- La somme maximale par recharge téléphonique a été établie à 75 $;

4- Le montant maximal du solde de crédit téléphonique, au moment où une recharge est effectuée, ne peut dépasser à 125 $;

5- Une liste noire des cartes de crédit ayant déjà servi à des recharges frauduleuses auprès de l'entreprise a été établie. Les cartes de crédit ainsi répertoriées étaient automatiquement bloquées pour toute tentative de recharges téléphoniques.

Phase 1 : Service de vérification d'adresse (SVA)

Les escrocs par carte de crédit, nous l'avons déjà mentionné au point 1.1.2, se sont ajustés aux premières mesures de précaution prises par l'entreprise étudiée. Ceux-ci ont en effet adopté des comportements plus prudents afin d'éviter de se faire repérer par les dispositifs de sécurité. Dans le but de réduire davantage les risques de fraude reliés à l'utilisation des cartes de crédit pour le rechargement à distance des cartes prépayées, un système de sécurisation en trois phases a été mis en place vers la fin de l'année 2001. Au cours de la première phase, l'entreprise étudiée s'est munie d'un système de sécurisation des paiements par cartes de crédit qui exige l'enregistrement d'une seule carte de crédit par téléphone mobile, et ce, avant son utilisation. Préalablement à l'enregistrement d'une carte de crédit, un système appelé " Service de vérification d'adresse " compare les données relatives à l'abonné (nom et adresse de facturation du détenteur de la carte de crédit fournie

pour le paiement de produits et services) à celles contenues dans la base de données d'une agence nationale de crédit. À l'instar du système d'enquête de crédit, cette mesure de vérification consiste en des croisements de l'information. D'une part, elle permet de vérifier que l'utilisateur de la carte connaît le nom, l'adresse de facturation et la date d'expiration de la carte de crédit. D'autre part, cette vérification permet d'éviter que des personnes reçoivent des factures pour des biens ou des services qu'elles n'ont jamais demandés ou achetés. Ainsi, s'il y a disparité entre l'information fournie par le client et celle contenue dans la base de données de l'agence de crédit nationale, l'enregistrement de la carte de crédit est refusé et elle ne peut donc être utilisée auprès de l'entreprise étudiée.

Le SVA comportait toutefois des lacunes : il ne permettait pas d'éviter les fraudes commises par des gens en possession des coordonnées des victimes de cartes de crédit (noms, adresses) ainsi que des dates d'expiration des cartes. A l'opposé, à l'usage, l'entreprise a réalisé que ce dispositif génère en moyenne un taux de rejet de 12 % de clients voulant légitimement se servir de leurs propres cartes de crédit. Trois raisons principales expliquent les refus de demandes légitimes.

1- Les changements d'adresse non communiqués à la banque;

2- L'absence du ou de(s) nom(s) du (des) cotitulaire(s) d'une carte crédit conjointe ou commerciale dans le système de vérification d'adresse;

3- L'absence de données au sujet des cartes de crédit récentes dans la base de données du système de vérification d'adresse de l'agence nationale de crédit.

Pour éviter de rejeter les titulaires légitimes n'ayant pas satisfait aux exigences du SVA, le Service de la fraude effectue une vérification supplémentaire. En effet, il communique de façon systématique avec la banque ou l'institution financière émettrice de la carte de crédit de chaque client refusé afin de vérifier l'exactitude du nom et de l'adresse de facturation du titulaire de la carte de crédit. S'il y a confirmation de l'information fournie, la carte de crédit déclarée par le client pourra subséquemment être enregistrée et utilisée. Dans le cas contraire, l'enregistrement de la carte de crédit ne peut se faire. Le client doit alors fournir une autre carte de crédit ou faire l'achat des produits sans-fil ou de recharges téléphoniques prépayées dans un point de vente.

Phase 2 : Code de vérification de la carte (CVC)

Depuis le mois d'octobre 2002, l'entreprise ne se contente plus de recourir au Service de vérification d'adresse (SVA). Dans le but d'améliorer davantage la sécurité des paiements par cartes de crédit, elle exige des renseignements supplémentaires de ses clients. Ainsi, les abonnés désireux d'utiliser une carte de crédit pour obtenir des produits sans-fil doivent non seulement fournir le numéro de leurs cartes de crédit et les dates d'expiration, mais également le code de vérification de carte (CVC). Ainsi, si le client fournit ce code de trois ou quatre chiffres inscrit à l'endos de la carte de crédit, il est plus probable encore que la carte de crédit soit utilisée par son titulaire authentique ou du moins que ce dernier soit en possession physique de la carte. S'il est incapable de donner ce numéro, l'enregistrement de la carte de crédit pour les recharges téléphoniques à distance ne se fait pas.

Phase 3 : Système de protection de listes noires

L'entreprise a ajouté une dernière protection à son système de vérification des cartes de crédit à la fin de l'année 2002. En effet, son système interconnecté à un réseau informatique d'une agence de crédit nationale effectue une recherche dans la liste noire. Le système de protection refuse automatiquement la requête d'un abonné qui tente d'utiliser une carte de crédit enregistrée dans cette base soit pour avoir été l'objet d'un vol, soit pour avoir été l'instrument d'une fraude chez un détaillant, où que ce soit dans le monde.

2.2 LE DÉPISTAGE DE LA COMMISSION DES FRAUDES

Les pages suivantes traitent de la façon dont le personnel de l'entreprise parvient à dépister la fraude (2.2) ainsi que des activités d'intervention à l'égard d'un comportement potentiellement à risque ou typique de fraude (2.3). Il convient de mentionner que les parties 2.2 et 2.3 relèvent de nos observations. Les perceptions des personnes interviewées seront présentées à la section 2.4.

La mission du Service de la fraude est de réduire les pertes en matière de fraude, notamment par l'élaboration et la mise en place de stratégies de prévention et de détection. L'expertise du personnel lui permet également d'agir à titre de conseiller et de faire des

recommandations générales auprès des divers responsables des équipes multidisciplinaires. La fonction première du Service de la fraude est toutefois de détecter rapidement l'utilisation potentiellement frauduleuse des services téléphoniques et de déployer des interventions afin de minimiser les pertes. Le dépistage s'effectue à l'aide d'un système de détection des risques, soit pour l'essentiel un registre des activités des abonnés du réseau (ou *CDR*, de l'anglais *Call Detail Report*). Ce registre, disponible en temps quasi réel (*near real time*), contient l'historique de toutes les activités des usagers de l'entreprise pour une période donnée (environ 45 jours) en ce qui a trait :

1- Aux coordonnées des appels entrants et sortants (heure, date, durée, nombre, etc.);

2- À l'utilisation des services personnalisés (messagerie texte, messagerie fax, Internet mobile, etc.).

La première fonctionnalité du système consiste à identifier et à signaler par une alarme les usagers qui présentent une activité typique ou potentiellement à risque de fraude. Il s'agit de l'utilisation des services sans fil en dehors des normes préétablies par le Service de la fraude. Les méthodes de gestion de risques sont déterminées intuitivement et selon les modèles de fraude antérieurs relevés par le Service de la fraude, sans outils de calcul de risques. Voici à titre d'exemple, deux catégories de comportements déclenchant une alarme :

1- Commission d'une activité typique de fraude

2- Activité téléphonique dont le volume (nombre ou durée) dépasse un certain seuil d'alerte.

Pour ce qui est des cas de la première catégorie, une seule activité téléphonique peut être signalée par le système de détection, indépendamment de sa durée. Voici quelques exemples d'activités typiques qui seront signalées par le système de détection et soumises pour vérification au personnel du Service de la fraude :

- Appel interurbain lancé vers des villes à risques (*HotCity)*
- Appel lancé vers des numéros de téléphone à risques (*HotList*)
- Utilisation d'un appareil en mode itinérance dans un pays à risques (*HotCountry*)

- Utilisation d'un appareil ayant déjà fait l'objet d'usage frauduleux (*HotIMEI*[13])

Dans la deuxième catégorie, l'activité téléphonique est filtrée et signalée par le système de détection quand elle atteint ou dépasse un seuil préétabli (*threshold*) de durée d'appels ou de nombre d'appels. En voici deux exemples :

1- Un usager qui effectue plus de 100 appels par jour, alors que le système interne génère une alarme réactive à partir de 100 appels, sera repéré par le système de détection.

2- Un abonné qui lance un appel interurbain ou outre-mer d'une durée supérieure à une heure pour un seuil préétabli de 60 minutes éveillera des soupçons auprès du personnel de dépistage de la fraude, car un tel appel occasionne des frais supplémentaires pour l'entreprise[14] et pour l'usager.

Tout comme la nature des comportements à risques, les seuils des alarmes réactives peuvent être ajustés en fonction des caractéristiques de la fraude de façon à rendre cette alarme plus ou moins sensible. Dans certains cas, un seul appel téléphonique peut déclencher plus d'une alarme. Par exemple, si un abonné utilise un appareil ayant déjà servi à une demande de souscription frauduleuse (*Hot IMEI* = première alarme) pour effectuer un appel dans une ville à risques (*Hotcity* = deuxième alarme), deux alarmes distinctes seront déclenchées. Chaque alarme signale un coefficient de risque distinct. Plus le coefficient est élevé, plus l'abonné présente une probabilité statistique élevée d'avoir fait une demande de souscription frauduleuse. Quand deux ou plusieurs alarmes sont déclenchées simultanément, les coefficients de risque de fraude sont additionnés pour établir un score cumulatif des risques. Nous constaterons au paragraphe suivant qu'il existe deux types de scores.

---

[13] Les fraudeurs peuvent réutiliser les appareils ayant déjà faits l'objet de fraude parce qu'il est techniquement possible de les utiliser de nouveau. Il suffit simplement de remplacer la carte à puce (SIM) par une autre pour que l'appareil (IMEI) soit réutilisable. Une alarme a donc été créée en vue d'identifier rapidement les récidivistes qui se reconnectent au réseau avec un appareil qui a déjà servi à une demande de souscription frauduleuse. Comme l'utilisation d'un portable n'est pas immédiatement bloquée dès sa réutilisation sur le réseau, en dépit de l'alarme générée, il incombe à l'équipe de détection des fraudes d'authentifier l'identité de l'abonné du service cellulaire et de bloquer, le cas échéant, l'utilisation de la ligne obtenue frauduleusement.

[14] L'entreprise étudiée est facturée par une entreprise de télécommunications qui fournit des communications de longues distances nationales ou internationales à partir du portable. Sprint Canada et Téléglobe en sont deux exemples.

La deuxième fonctionnalité du système de détection consiste à établir un score des risques définis par l'addition des coefficients des alarmes au cours d'une période donnée. Par exemple, un appel interurbain lancé dans une ville à risques comme New York peut avoir un coefficient de risque de 1, alors qu'un autre appel lancé à partir d'un appareil ayant déjà servi une demande de souscription frauduleuse peut avoir un coefficient de 10. Comme la même activité (ou le même appel) génère deux alarmes, le score total sera de 11, soit l'addition des coefficients des deux alarmes (1 + 10). Il existe deux catégories de scores émis par le système de détection, soit le score récent (*Recent Score*) et le score total (*Total Score*). Le score récent se mesure dans le temps quasi réel, (*near real time*) par rapport aux comportements des utilisateurs sur le réseau puisqu'il est calculé approximativement aux 12 heures. Quant au score total, il est calculé sur une période beaucoup plus longue, généralement de 30 jours. Quel que soit le type de score, celui-ci est constamment recalculé pour les périodes choisies par la responsable du Service de la fraude.

Afin d'enrichir le système ou de l'actualiser, le gestionnaire du Service de la fraude peut y apporter des ajouts, des modifications ou des suppression en regard des activités typiques de fraude. Une mise à jour des critères peut être justifiée pour déceler les nouveaux modes opératoires des fraudeurs mis en évidence par le personnel du Service de la fraude. En vue d'optimiser l'efficacité du système de détection, les analystes de la fraude sont tenus de faire connaître à la personne qui gère le Service de la fraude les nouveaux modes opératoires de fraude. Sur la base des appels lancés par des usagers ayant souscrit frauduleusement à des services de télécommunications sans fil, il est possible, grâce au *CDR* ou à la facture, de dégager certaines similitudes entre les modes opératoires frauduleux. Par exemple, les plus évidentes sont le nombre et la durée anormalement élevés des appels frauduleux. Dégager des observations requiert toutefois beaucoup d'effort de la part du personnel de la fraude puisque la collecte des renseignements se fait manuellement.

La troisième fonctionnalité du système de détection est la transmission au Service de la fraude de certaines informations sur les usagers qui présentent un risque accru d'utilisation frauduleuse des services sans fil. En effet, depuis son poste d'ordinateur, chaque employé du Service de la fraude peut consulter, par le biais d'une interface graphique de type Web, les comptes d'utilisateurs pour lesquels une alarme réactive a été déclenchée. Le but est de

détecter le plus rapidement possible le plus grand nombre d'activités frauduleuses sur le réseau. De façon générale, le traitement des comptes à vérifier est effectué selon un ordre de priorité des risques, soit par ordre décroissant des scores de prédiction de la fraude, de manière à identifier d'abord les probabilités statistiques les plus élevées en matière de fraude. Comme la figure 1 l'indique, parmi les informations disponibles sur les usagers qui présentent une activité typique de fraude, il y a leurs numéros de téléphone et leurs numéros de compte. Ces deux informations sont nécessaires pour parvenir à retrouver le client dans le système de facturation de l'entreprise. Le Service de la fraude reçoit en outre comme informations, la date de mise en service du service téléphonique et le détail des alarmes.

Figure 1 : Exemple d'affichage d'un compte signalé par le système de détection

Numéros de téléphone	Numéros de compte facturation	Date d'activation	Détails des alarmes déclenchées	Score récent de prédiction de la fraude (12 h)	Score total (30 jours)
514-999-1010	123456	2004-01-01	*HotCity* = 1	11	500
			HotImei = 10		

2.3 LES INTERVENTIONS À L'ÉGARD D'UNE FRAUDE PRÉSUMÉE

Grâce aux techniques de dépistages informatiques, le système surveille et signale automatiquement les activités douteuses qui ont généré une alarme en vue d'une vérification plus approfondie. Le personnel du Service de la fraude doit cependant faire preuve d'une grande vigilance étant donné que le signalement d'un compte suspect ne concerne pas toujours une fraude. La présente partie, qui ne se veut pas totalement exhaustive, explique schématiquement comment le personnel authentifie l'identité d'un usager qui éveille des soupçons de fraude. Nous verrons que le premier stade consiste à s'assurer qu'un abonné n'utilise pas de faux renseignements personnels pour dissimuler sa véritable identité et pour accéder ainsi aux services téléphoniques. S'il y a repérage d'incohérences ou d'anomalies des renseignements fournis, le deuxième stade consiste à suspendre temporairement la ligne téléphonique de l'abonné dans le but de vérifier avec plus de rigueur son identité. Enfin, en cas de fraude, le dernier stade consiste à procéder à la résiliation permanente des services téléphoniques.

2.3.1 L'authentification des renseignements et le repérage des incohérences des renseignements personnels

Afin de respecter la Loi sur la protection des renseignements personnels et les documents électroniques dans le secteur privé, chaque entreprise ne doit collecter les renseignements concernant ses clients qu'à des fins légitimes de commerce, par exemple pour procéder à une enquête de solvabilité. Quant aux requérants de crédit, ils ne sont pas dans l'obligation de fournir leur numéro d'assurance social pour l'enquête de crédit, ni même dans le cadre du processus d'authentification, qui permet de s'assurer que le nouveau client n'a pas fait de fausse déclaration, c'est-à-dire qu'il porte bien le nom qu'il prétend avoir, qu'il est le détenteur des renseignements personnels qu'il fournit et qu'il habite ou travaille effectivement à l'endroit dont il a donné l'adresse de facturation. L'authentification de l'identité de la clientèle est d'autant plus importante lorsqu'il en va de demandes d'accès aux options non incluses dans la tarification du forfait avec abonnement. Les critères du Service de la fraude servant à établir l'authenticité d'une demande d'ouverture de service téléphonique s'appuient essentiellement sur trois sources :

1- les coordonnées postales et téléphoniques;

2- les renseignements personnels issus des données de l'agence de crédit (numéro d'assurance social, date de naissance, adresse, etc.);

3- les renseignements obtenus auprès des sociétés émettrices de cartes de crédit, le cas échéant.

À la première étape d'authentification, un logiciel permettant de vérifier la cohérence des coordonnées postales et téléphoniques des abonnés est mis à la disposition du personnel du Service de la fraude. Ce logiciel fourni par une entreprise[15] externe comporte un annuaire téléphonique informatisé mis à jour mensuellement. Il contient toutes les inscriptions résidentielles et commerciales provenant des éditeurs d'annuaires téléphoniques au Canada. Pour déterminer si une personne est répertoriée dans l'annuaire, les critères de recherche ou d'interrogation sont nombreux. Les options de recherche peuvent se faire par nom de famille, adresse, ville, code postal ou numéro de téléphone. En effet, les options de recherche permettent la combinaison de plusieurs critères. Or, certaines lacunes compromettent ou

[15] Il s'agit d'une entreprise qui offre des engins de recherche rapides des annuaires téléphoniques.

rendent difficile l'authentification de l'identité des clients. Premièrement, il peut arriver que le nouveau client porte bien le nom qu'il prétend avoir et qu'il habite ou travaille effectivement à l'endroit dont il a donné l'adresse, sans toutefois être répertorié dans l'annuaire. Il arrive en effet souvent que le numéro de téléphone résidentiel soit répertorié sous le nom d'un seul des membres de la famille. Deuxièmement, certains numéros valides ne sont tout simplement pas répertoriés, notamment les numéros de téléphone cellulaires et les numéros de téléphone résidentiels confidentiels. Troisièmement, en ce qui concerne la majorité des adresses des immeubles, celles-ci sont souvent incomplètes, de sorte que les numéros d'appartement ne sont pas répertoriés. Quatrièmement, certaines adresses sont incomplètes ou non disponibles dans les régions rurales (ex. : absence de numéro civique ou de nom de rue). Pour pallier ces lacunes, le Service de la fraude peut appeler au numéro de téléphone résidentiel (ou commercial) fourni lors de la souscription. L'incohérence des coordonnées (numéro de téléphone hors service ou le fait que l'abonné ne soit pas connu au numéro) ne prouve pas forcément qu'il y a eu fraude lors de la souscription. A cet égard, il peut se commettre des erreurs de frappe de la part du personnel du centre d'appels au moment de la demande de souscription.

À la deuxième étape, l'authenticité de l'identité d'un abonné peut également se faire par la comparaison systématique entre les renseignements personnels recueillis au moment de l'abonnement (son numéro d'assurance social, son numéro de carte de crédit, sa date de naissance, son adresse, etc.) et les renseignements inscrits dans la base de données de l'agence de crédit. Nous avons déjà précisé sous 1.1.1.2 que certaines informations sont signalées par une " alerte d'anomalie " dans le but de permettre le repérage rapide les discordances existant entre les renseignements fournis par le requérant et ceux figurant dans la banque de données de l'agence de crédit. À l'interne, l'accès à ces alertes n'est donné qu'au Service de la fraude.

À la troisième étape d'authentification, nombreux sont les abonnés qui préfèrent fournir leur numéro de carte de crédit au lieu de leur numéro d'assurance social pour procéder à l'enquête de solvabilité. Du côté de l'entreprise étudiée, les procédures d'authentification des titulaires de cartes de crédit ne peuvent se faire qu'auprès des institutions financières. L'entreprise étudiée doit communiquer par téléphone ou par écrit

avec les sociétés émettrices de cartes de crédit relativement aux abonnés du sans fil qui ont fait l'objet d'une enquête de crédit. Ce faisant, elle parvient à confirmer ou infirmer les quelques renseignements personnels qu'elle a obtenus de l'abonné et qu'elle souhaite vérifier (le nom et le prénom du titulaire de compte, son adresse de même que son numéro de téléphone résidentiel). Mais les sociétés émettrices de cartes de crédit, également assujetties à la Loi sur la protection des renseignements personnels et les documents électroniques, ne peuvent divulguer des renseignements personnels, comme la date de naissance ou l'adresse postale, relatifs aux titulaires de cartes de crédit aux personnes qui représentent le Service de la fraude d'une entreprise. La majorité de leurs pratiques sont uniformes et strictes, de sorte qu'aucune demande téléphonique ou par correspondance ne permet l'accès aux renseignements personnels des titulaires de cartes de crédit. Conséquemment, trouver de l'information fiable (en totalité ou en partie) en cas d'inexactitude s'avère complexe. Comme elles veulent protéger la vie privée de leurs titulaires, rares sont les institutions prêtes à faciliter sa tâche d'authentification à une entreprise ou à un commerçant. Les quelques occasions où le personnel de l'entreprise étudiée a pu obtenir des renseignements concernaient des comptes de cartes de crédit déjà désactivées pour fraude.

2.3.2 **L'interruption temporaire ou permanente des services téléphoniques**

Lors du processus d'authentification, le personnel doit faire preuve d'une grande vigilance pour éviter de suspendre indûment un service téléphonique et ainsi causer un préjudice à un usager. En effet, comme nous l'avons souligné, des erreurs administratives de la part de l'entreprise étudiée peuvent se glisser au moment de l'abonnement et rendre plus difficiles certains aspects de l'authentification. Ainsi, avant de passer à l'étape de la suspension de l'abonnement téléphonique, le Service de la fraude doit tenter de communiquer avec la clientèle en cause pour effectuer une authentification plus exhaustive.

C'est sur les bases de nombreux indices que le Service de la fraude peut se fonder pour décider de l'interruption d'une ligne téléphonique. Voici quelques indices susceptibles de justifier la suspension du service sans fil :

- l'adresse de facturation est inexistante, incomplète ou le client n'y est pas connu;

- le numéro de téléphone est erroné, hors service ou le client n'y est pas connu;
- le client est incapable de valider certains renseignements contenus dans sa fiche de crédit (date de naissance, adresse, employeur);
- la personne dont l'identité a été empruntée confirme qu'elle n'a jamais fait une demande de service téléphonique;
- les organismes externes (banques, bureaux de crédit, police, opérateurs sans fil) établissent que l'identité d'un tiers a fait l'objet d'une souscription frauduleuse.

La procédure d'interruption met fin à l'utilisation des services de communications et, elle prévoit que tous les appels émanant de la ligne suspendue soient systématiquement redirigés au Service de la fraude pour authentification. Ainsi, au moment où un usager tente de lancer un appel, il sera immédiatement mis en communication avec le Service de la fraude. Ensuite, l'abonné dont les services téléphoniques mobiles ont été interrompus doit faire la preuve de son identité afin d'obtenir le rétablissement du service sans fil. Il est parfaitement libre de refuser, mais, ce faisant, il s'expose fortement à la résiliation de son compte. En revanche, par respect pour les abonnés, c'est le principe du bon sens de la part du Service de la fraude qui prévaut pour l'interruption temporaire ou permanent de l'abonnement des clients. Comme nous l'avons déjà mentionné, la suspension téléphonique est généralement précédée d'une enquête qui comprend le processus d'authentification et le repérage des incohérences. Les membres du Service de la fraude ont reçu une formation leur permettant d'authentifier les renseignements et de s'assurer qu'ils parlent bel et bien avec le vrai requérant. Généralement, le degré d'authentification de l'identité d'un abonné varie selon la nature des incohérences ou le degré de risques que présente l'usager. L'authentification d'un abonné peut s'accomplir:

- par téléphone, si les employés du Service de la fraude estiment qu'il y a eu des erreurs administratives et que les coordonnées postales et téléphoniques ont été authentifiées.
- par télécopieur, si le client est incapable de fournir certains renseignements personnels permettant d'établir son identité (date de naissance, adresse, numéro de téléphone, numéro d'assurance social)
- en succursale avec des pièces justificatives, s'il a été établi qu'un tiers a été victime de souscription frauduleuse. L'information ayant permis de le faire peut provenir de la victime elle-même ou des organismes externes (police, banque, opérateurs sans fil, etc.)

Si l'usager refuse de se conformer à l'obligation de faire la preuve de son identité, la ligne demeure suspendue. Passé un délai raisonnable, les abonnés s'exposent fortement à la résiliation de leur ligne téléphonique. Finalement, à la suite d'une résiliation de l'abonnement avec facture, l'appareil ayant servi à une demande de souscription frauduleuse est automatiquement inscrit au fichier de la " liste grise ". Ce faisant, le système de détection est en mesure de repérer immédiatement les récidivistes qui tentent de contracter un nouvel abonnement avec un appareil ayant déjà servi à une demande de souscription frauduleuse.

Par ailleurs, dans le cadre du processus d'authentification et de la suspension de la ligne des usagers, parallèlement à son enquête, l'équipe de la fraude peut mener des recherches simultanées ou en parallèle afin de localiser les victimes de vol d'identité qui seraient au Canada. Cette démarche a pour but de confirmer qu'il s'agit bien d'une demande de souscription frauduleuse et d'informer les victimes de vol d'identité de l'usurpation de leurs renseignements personnels. Souvent, ces victimes ignorent qu'un tiers a utilisé leurs renseignements personnels. D'autres victimes révèlent avoir déjà fait les frais de supposition de personne auprès d'entreprises qui fournissent du crédit (télécommunication, cartes de crédit, magasins, etc.). Notons toutefois que, pour diverses raisons, il arrive que le personnel de la fraude ne réussisse pas à retracer le titulaire légitime des renseignements personnels (ou la supposée victime); c'est notamment le cas quand :

- elle n'est pas répertoriée dans l'annuaire téléphonique informatisé;
- elle ne figure pas dans la base de données de l'agence de crédit;
- les institutions refusent de divulguer les coordonnées postales et téléphoniques de la présumée victime.

2.3.3 **L'absence de réactions formelles**

Une fois que la fraude a été mise au jour, l'entreprise étudiée procède simplement à la résiliation du service téléphonique sans fil et absorbe les pertes imputables à la fraude. Malgré l'existence de certaines infractions dans le Code criminel canadien, que nous avons vues au chapitre 1 (point 2.2), l'entreprise renonce à porter plainte auprès des autorités chargées de l'application des lois. La responsable du Service de la fraude confirme par ailleurs que l'entreprise ne prend pas l'ampleur monétaire de la fraude en considération pour

décider ou non de porter plainte à la police. L'absence de réactions pénales s'explique principalement par le problème de l'insuffisance des éléments de preuve, laquelle compromet d'éventuelles poursuites pénales. Par exemple, la tâche d'identification des auteurs ou des escrocs est pratiquement impossible. Il faut rappeler, à cet égard, que lors de demandes de souscription en ligne, l'entreprise ne relève pas les adresses IP (Internet Protocole[16]) des internautes si bien que le Service de la fraude n'en a pas connaissance. Il y a un problème analogue en ce qui a trait aux demandes de souscription réalisées en centres d'appels. Pour faire leurs demandes d'abonnement, les fraudeurs peuvent utiliser n'importe quelle ligne de téléphone (numéro local ou sans frais) car l'entreprise ne s'est pas dotée de dispositifs permettant de déterminer la provenance des appels de ses clients (date, lieu, heure, etc.) A l'instar des demandes en ligne, les souscriptions réalisées au téléphone peuvent provenir de n'importe quel endroit du monde.

Compte tenu des difficultés qu'elle rencontre pour faire la preuve des fraudes subies, l'entreprise nous semble même incapable de satisfaire aux règles de preuve en cour civile, où il s'agit pourtant de présenter une preuve selon la balance des probabilités (51%). Et sur le terrain de la poursuite criminelle, l'entreprise étudiée est *a fortiori* presque toujours dans l'impossibilité de produire une preuve hors de tout doute raisonnable.

2.4 LES PERCEPTIONS DES EMPLOYÉS

2.4.1 Quant à la prise de risques au moment de la souscription

Selon les propos recueillis, les employés voient dans le manque de rigueur et de contrôle lors de la demande de souscription une prise de risque considérable pour l'entreprise étudiée. Pour eux, il n'est pas étonnant que les escrocs exploitent à leur avantage certaines faiblesses de l'entreprise. Le premier facteur explicatif de la prise de risques provient des lacunes en matière de collecte de l'information, notamment à l'aide de pièces d'identité. En effet, ces lacunes posent un problème particulièrement délicat et soulèvent des commentaires de la part des analystes. D'abord, en ce qui trait à la suffisance des renseignements personnels

---

[16] " Protocole standard pour les transmissions dans Internet reposant sur la décomposition des messages en paquets autonomes et sur le système d'adresses uniques des nœuds : O'Leary et O'Leary, 2001 : 341 ".

qui sont recueillis aux fins de l'enquête de crédit, il existe une dissension parmi les employés. D'un côté, deux analystes se montrent soucieuses de la vie privée en faisant référence aux principes énoncés dans la Loi sur la protection des renseignements personnels et les documents électroniques, adoptée en janvier 2001. Elles ont donc le sentiment qu'il est impossible de circonscrire les risques qui sont pris. D'un autre côté, deux autres analyses sont plutôt d'avis qu'il y aurait possibilité de recueillir des renseignements supplémentaires au moment de la demande de souscription. Comme le font déjà les entreprises de cartes de crédit, l'entreprise pourrait demander à ses nouveaux clients leur second prénom ou le nom de jeune fille de leur mère. En outre, pour ce qui est des critères d'admissibilité, les exigences de l'entreprise à l'étude suscitent le commentaire suivant :

> *" Un fraudeur a seulement besoin des renseignements personnels. Il n'a aucun contrat à signer, aucune pièce d'identité à montrer à qui que ce soit. C'est donc très facile pour cette personne-là d'avoir un service chez nous. [...] La porte est ouverte à n'importe qui. "*

Finalement, deux autres commentaires ont trait à l'identification formelle des usagers :

> *" Au téléphone, on n'a pas à s'identifier avec une pièce d'identité. Tout ce qu'il faut, c'est l'information [sur la victime] en tant que telle, sans nécessairement avoir la carte d'identité ou [une carte] avec photo. "*

> *" C'est facile, parce que les clients n'ont pas besoin de montrer des pièces d'identité. Ils n'ont pas besoin de se présenter en personne. C'est plus facile de faire une fraude par téléphone. Si tu te fais prendre, tu n'as simplement qu'à raccrocher. "*

Ce dernier commentaire signifie en clair que l'entreprise ne prend aucune mesure pour neutraliser un escroc après une tentative de fraude. L'entreprise n'enregistre aucune information sur les circonstances dans lesquelles les tentatives de fraude ont lieu (numéro d'assurance sociale utilisé, carte de crédit, adresse donnée, etc.). Il n'existe aucun dispositif permettant de répertorier les tentatives de souscriptions frauduleuses. Il nous est permis de nous demander si l'enregistrement systématique des tentatives infructueuses pourrait minimiser les risques de nouvelles tentatives ou les récidives de la part des fraudeurs agissant lors de la souscription. Une analyste est d'avis que le manque de rigueur de l'entreprise à

l'égard des tentatives de fraude envoie un message peu dissuasif aux fraudeurs : *" Tu as le droit de réessayer et réessayer, jusqu'à ce que tu l'aies. "*

Le second facteur explicatif de la prise de risque découle des lacunes du système d'enquête de crédit qui ont pour effet de discréditer les attestations de légitimité des demandes de souscription. Au centre de leurs préoccupations, les analystes ont souligné que l'entreprise n'est pas très bien protégée contre les demandes illicites de souscription en raison du peu d'efficacité du système de vérification de crédit. Un analyste du Service de la fraude a même qualifié le système d'enquête de crédit de " vraie passoire ". À ce sujet, nous avons retenu deux failles dont les escrocs tirent partie pour dissimuler leur véritable identité au moment de la demande de souscription.

La première faille qui paralyse la procédure d'authentification des abonnés est sans contredit le manque de fiabilité et d'exhaustivité des bases de données relatives aux fiches de crédit. Bien que la majorité des fiches de crédit soient assez complètes et exactes, d'autres, dans des proportions non négligeables, le sont beaucoup moins. Certaines fiches de crédit comportent beaucoup d'erreurs ou sont incomplètes, selon deux employés chargés de la détection.

La deuxième lacune du système d'enquête de crédit est qu'il ne permet de vérifier la cohérence des coordonnées postales et téléphoniques des abonnés potentiels. Or, certains escrocs du cellulaire recourent à un faux numéro ou à un numéro qui n'est pas en service lors de la demande de souscription. D'autres utilisent un numéro civique inexistant, un faux code postal ou un faux nom de rue comme point d'acheminement des factures.

Il en résulte de ces deux lacunes que le système d'enquête de crédit est incapable de reconnaître, à coup sûr, les demandes de souscription qui comportent des incohérences quant aux renseignements fournis par le requérant. À ce sujet, un analyste de dire :

> *" On remarque souvent qu'un compte frauduleux a pu être activé même si le nom n'est pas semblable [au nom réel] ou que la date de naissance n'est pas semblable [à la vraie date de naissance]. [...] On peut réussir à activer un téléphone sans que le numéro d'assurance social, la date de naissance et le nom soient tous corrects [véritables]. "*

Les lacunes précitées nous semblent s'expliquer par la finalité du système d'enquête de crédit. Selon une analyste de la fraude, ce système est davantage destiné à déceler les mauvais payeurs plutôt qu'à dépister les fraudeurs ayant réussi à subtiliser des renseignements personnels d'un tiers :

> *" Le but du système d'enquête de crédit n'est pas d'identifier les fraudeurs. [...] C'est simplement pour créer un compte et pour des processus de recouvrement. [...] Si le fraudeur a les bons renseignements, il n'a simplement qu'à rester calme lors de la demande de souscription par téléphone et il va passer l'enquête de crédit [...] Dans le fond, c'est une préparation. "*

2.4.2 **Quant au système de surveillance et de dépistage de la fraude**

Sur la base des propos recueillis lors des entretiens, le taux de dépistage des fraudes par le système de détection est disproportionné par rapport à l'important volume des comptes soumis à vérification. En d'autres termes, les employés du Service de la fraude perçoivent le dépistage de la fraude comme étant de plus en plus difficile et exigeant car ils doivent consacrer beaucoup de temps et d'efforts pour parvenir à mettre à jour un nombre restreint de fraudes. Toutes les personnes interrogées se sentent concernées par la piètre performance du système de détection qui signale, de surcroît, de nombreux faux cas de fraude. Selon les employés, le système de surveillance et de dépistage produit des " faux positifs " (ou faux cas de fraude) 98 ou 99 fois sur 100. Ces résultats signifient donc que les personnes chargées de détecter la fraude doivent passer au crible une centaine de comptes pour finalement détecter 1 ou 2 cas de fraude.

Pour expliquer leur piètre performance en matière de dépistage, l'ensemble des analystes révèle que de nombreuses alarmes réactives générées par le système de détection sont maintenant inutiles. En d'autres mots, le système est actuellement incapable de cibler les cas qui présentent le plus de risques de fraude. Les analystes chargés de la détection ont évoqué une autre source d'inquiétude, à savoir que les fraudeurs agissant lors de la souscription n'ont aucune difficulté à s'adapter et à déjouer le système de détection. Les lacunes en matière de déclenchement des alarmes ont été évoquées par deux analystes. Elles

relèvent notamment la facilité avec laquelle les fraudeurs échappent au dépistage de la fraude :

> *" Premièrement, tu n'utiliseras pas ton téléphone énormément. Tu ne fais pas trop d'appels aux États-Unis non plus. Si tu prends 200 minutes à ta première journée d'utilisation, tu vas apparaître sur les listes des abonnés présentant un score élevé de prédiction de la fraude, c'est officiel. "*

> *" Ils s'habituent. Ils savent quelle est la limite de nos seuils ou critères de déclenchement d'une alarme. Ils savent que s'ils génèrent plus que 100 minutes d'appel par jour, ça sort une alarme [...] Les alarmes ne sont pas si fiables que ça : avant, quand ça générait une alarme pour New York, c'était payant. Aujourd'hui, ça ne l'est plus [...] parce que les fraudeurs changent de comportement. "*

3. LES RÉSULTATS OBTENUS PAR L'ENTREPRISE AU REGARD DE LA SITUATION

3.1 LA FRAUDE AU FORFAIT PRÉPAYÉ ET AU FORFAIT MENSUEL

Les données statistiques sur les estimations et l'ampleur de la fraude indiquent que l'entreprise étudiée considère la lutte contre la fraude avec sérieux. D'ailleurs, le tableau 2 souligne que la situation actuelle est loin d'être alarmante, il présente un taux global de fraude de 0,12% pour la dernière année (2003). Il faut ajouter aussi que le taux global des fraudes de 0,12% demeure bien en deçà de la moyenne estimée entre 3% et 5% dans l'ensemble de l'industrie du sans-fil.

Par ailleurs, bien qu'il n'existe pas de chiffres précis sur les taux des fraudes au forfait mensuel, les taux de fraude globaux indiquent que l'entreprise est parvenue à lutter efficacement contre la fraude. Il faut cependant rappeler que ces chiffres doivent être considérés avec une grande précaution pour deux raisons essentielles. D'abord, le préjudice économique non recensé (chiffre noir) lié au forfait mensuel est important. Ensuite, comme nous le verrons plus loin sous 3.2, les instruments de mesure de l'ampleur des pertes liées aux fraudes sont peu fiables.

Les résultats de cette étude démontrent également que l'entreprise a empêché la presque totalité des fraudes commises en matière de forfait prépayé après la mise en place d'un système de sécurisation des paiements à distance (sans carte physique) pour l'achat de recharges téléphoniques prépayées. Nous évoquerons plus précisément au point 3.3 quels ont été les moyens mis en oeuvre depuis la fin de l'année 2000 par l'entreprise pour réduire au maximum les fraudes au forfait prépayé. De surcroît, les tableaux 3 et 4 révèlent tous les deux des diminutions significatives du nombre de fraudes au forfait prépayé et une baisse non négligeable des pertes moyennes engendrées par la fraude pour les années 2002/2003. Rappelons que ces chiffres sont assez fiables en raison du fait que les cas de fraude sont rapportés assez systématiquement par les victimes ou mis à jour par les employés de l'entreprise.

3.2 LA PRÉCARITÉ DES INSTRUMENTS DE MESURE

Chaque mois, l'entreprise compile des statistiques dans le but de mesurer l'ampleur des pertes liées aux fraudes dont elle a été victime. Le principal instrument de mesure des activités frauduleuses connues est fondé sur le manque à gagner par rapport aux estimations basées sur les factures à recouvrer; ce chiffre est produit par le système de facturation de l'entreprise. Ceci revient à dire que le calcul de l'ampleur de la fraude se fait uniquement en dollars. De plus, d'après nos observations, des limites d'ordre méthodologique relatives aux modes de comptage nous amènent à nous questionner sur la validité et la fiabilité des fraudes enregistrées par l'entreprise. Il convient de mentionner que la mesure des pertes frauduleuses en dollars est fort discutable en raison des politiques de facturation ou d'établissement des prix des services de téléphonie mobile. Dans un contexte de démocratisation de la téléphonie du sans fil, les forfaits deviennent de plus en plus avantageux[17]. Les données présentées par le Service de la fraude ne tiennent pas compte des baisses de tarif des services cellulaires au cours des dernières années. En raison de la baisse des prix des services sans-fil, nous pouvons difficilement apprécier l'évolution de la fraude au cours de la période étudiée et déterminer si

[17] À cet égard, bien que nous ne disposions pas de chiffres permettant d'apprécier la baisse des coûts des communications mobiles, nous avons observé de nombreuses innovations ayant entraîné des chutes de tarifs. Par exemple, au cours de l'exercice 2000, la tarification des communications sans fil s'établissait uniquement selon un taux fixe. Puis, en 2003, l'entreprise a élargi l'éventail des régimes tarifaires en offrant, notamment aux grands utilisateurs, la possibilité de choisir des tarifs plus avantageux. Un des forfaits qui a été introduit est le forfait illimité " soirs ou week-ends ".

la diminution des pertes dues à la fraude résulte effectivement de la politique anti-fraude de l'entreprise.

Un premier élément vient compromettre la possibilité de mesurer précisément l'ampleur de la fraude ; il a trait aux différents modes de tarification du forfait mensuel : les utilisateurs du sans-fil peuvent être facturés selon différents plans tarifaires (fixe, combiné, illimité) lors de la souscription. Certains clients souscrivent à la tarification fixe, comprenant des minutes d'utilisation incluses tandis que d'autres optent pour le tarif combiné qui réunit le tarif fixe et le tarif illimité. La facturation des services sans fil n'est pas fonction du volume et de la durée des appels ; elle s'établit sur des principes de tarification très variés.

Un autre élément compromet toute éventuelle comparaison entre les deux modes de souscription. En effet, il faut savoir qu'en ce qui concerne les forfaits mensuels, les minutes d'utilisation sont calculées à la seconde alors que les forfaits prépayés comportent une tarification à la minute. Par conséquent, il nous semble hasardeux de comparer les pertes liées à la fraude au forfait mensuel avec celles qui sont engendrées par la fraude au forfait prépayé.

En bref, pour obtenir des statistiques plus fiables sur le phénomène de la fraude, l'instrument de mesure devrait être fondé sur d'autres principes. Plutôt que de prendre en considération la tarification des services de téléphonie mobile qui manque d'uniformité, il vaudrait mieux fonder les estimations sur le volume des communications mobiles, soit sur leurs nombres et leurs durées en minutes. Ainsi, il serait possible de calculer avec de telles données quelle est la proportion de communications frauduleuses (en nombre et en durée).

3.3 DES MOYENS DE LUTTE EFFICACES POUR CONTRER LA FRAUDE AU FORFAIT PRÉPAYÉ

Cette étude démontre que l'entreprise semble avoir pris les moyens de lutte nécessaires pour contrer la fraude au forfait prépayé. Celle-ci a amplement diminué et a quasiment été enrayée grâce aux politiques anti-fraude de l'entreprise. L'entreprise a fait preuve d'une plus grande vigilance afin d'améliorer la sécurité et la fiabilité des paiements à distance pour les recharges téléphoniques prépayées. Comme nous l'avons déjà vu sous

2.1.2, la panoplie des moyens de lutte qui ont été mis en oeuvre dès le début de l'année 2001 afin de réduire les opportunités de fraude sont les suivants :

- la mise en place d'un système d'enregistrement des cartes de crédit avant leur utilisation;

- la mise en place de mécanismes d'authentification tels que SVA et CVC qui permettent de vérifier sur-le-champ la concordance des renseignements personnels fournis par les titulaires de cartes de crédit (nom, adresses, code de sécurité, date d'expiration), avant son enregistrement, avec les bases de données qui alimentent le SVA et le CVC;

- la mise en place d'un système de listes noires qui empêche systématiquement toute tentative d'enregistrement d'une carte de crédit à risque de fraude;

- la politique sur le nombre de recharges quotidien;

- la politique sur le solde maximum au moment d'effectuer une nouvelle recharge;

- la politique sur les types de cartes de crédit admissibles aux recharges

3.4 L'INSUFFISANCE DES MOYENS DE LUTTE POUR CONTRER LA FRAUDE AU FORFAIT MENSUEL

Il est évident que les fraudes liées au forfait mensuel ne représentent qu'une partie de l'ensemble des activités frauduleuses. L'entreprise étudiée présente une certaine vulnérabilité quant à ses moyens de lutter contre la fraude et de la dépister. Ces carences tiennent, d'une part, aux opportunités de fraude (1.1.1.1) que présentent, entre autres, les modes de souscription par téléphone et par Internet. D'autre part, elles découlent du processus d'évaluation de crédit qui est peu rigoureux (1.1.1.2). L'entreprise agit dans un contexte de hauts risques de fraudes qui lui permet difficilement d'identifier tous les fraudeurs souscrivant à un forfait mensuel. En outre, les entretiens réalisés avec le personnel du Service de la fraude et nos observations nous suggèrent la conclusion suivante : il y a insuffisance de moyens déployés contre la fraude au forfait mensuel. Dans la partie suivante, nous entendons faire la synthèse des principales failles que présente le système de détection

des fraudes et des préoccupations émises par l'ensemble de personnes interrogées dans le cadre de leurs activités de dépistage de la fraude. Sans être exhaustives, ces observations serviront de fondement à une première réflexion visant à définir une lutte plus efficace contre les demandes de souscription frauduleuses.

3.4.1 **Difficultés liées au dépistage de la fraude au forfait mensuel**

Cette étude a permis de constater que le système de détection de la fraude au forfait mensuel est loin d'être efficace. L'entreprise devrait vouer plus d'efforts au développement du dispositif de détection pour mieux cibler les usagers du forfait mensuel susceptibles de faire une demande de souscription frauduleuse. Entre autres, il faut trouver le moyen de faire une meilleure sélection des comptes d'usagers devant faire l'objet d'enquêtes. Pour l'instant, au vu du nombre considérable de "faux positifs" générés par le système de détection de la fraude, il est impossible au personnel du service de procéder à une vérification de chacun d'entre eux. Signalons d'entrée de jeu que l'entreprise ne possède pas les moyens technologiques nécessaires, en l'occurrence d'un système expert[18], permettant de mieux cibler les usagers faisant vraisemblablement une utilisation frauduleuse des services de téléphonie mobile.

Le travail de dépistage de la fraude au forfait mensuel est donc une tâche fastidieuse. C'est au jour le jour, sur le terrain, que le personnel découvre de nouveaux modes opératoires de fraude et les soumettent aux gestionnaires pour améliorer le système de détection. Le fait que les changements informatiques destinés à améliorer le système de détection tardent à venir (ils ne sont pas considérés comme prioritaires par la direction de l'entreprise) rend le travail de dépistage difficile. Pendant ce temps, avec la démocratisation des services de téléphonie mobile, il y a une augmentation croissante du nombre d'abonnés sur le réseau sans fil. Cet accroissement est naturellement accompagné d'une augmentation du trafic des communications sans fil et, par conséquent, d'une hausse du nombre d'alarmes signalant des usagers susceptibles d'avoir fait des demandes de souscription frauduleuses.

---

[18] Système de gestion de bases de connaissances qui imite le savoir d'experts humains entraînés dans un domaine particulier (O'Leary and O'Leary, 2001 : 340).

Poussés par le désir effréné d'obtenir une plus grande part du marché et de demeurer compétitif, les dirigeants de l'entreprise n'ont pas évalué à l'avance les changements technologiques qui s'imposaient dans le système de détection. Dès lors, il est urgent que le Service de la fraude se dote d'un système expert capable de générer moins de "faux positifs", en sélectionnant plus efficacement les critères d'identification des cas méritant investigation. Là, le recoupement ou l'appariement des informations nous paraît être un outil essentiel. La responsable du Service de la fraude se dit consciente des faiblesses inhérentes au système de dépistage et admet que le système de détection n'est pas au point. Elle a reconnu que dans un contexte concurrentiel difficile, les initiatives de vente et de marketing en vue d'augmenter le nombre d'abonnés ont la priorité sur le déploiement de ressources nouvelles pour lutter contre la fraude. La personne qui gère le Service de la fraude renchérit en ajoutant que l'entreprise a délibérément pris la décision d'écarter les requêtes de son département qui visaient à l'amélioration du système de détection au cours des années 2002 et 2003. En fait, les demandes du Service de la fraude en vue de l'amélioration du système anti-fraude n'ont jamais été considérées comme une priorité majeure par les dirigeants de l'entreprise. En dépit de cette politique, la responsable du Service de la fraude se montrait cependant rassurante en prétendant avoir élaboré un plan d'action réalisable aux fins d'aider les employés dans leurs efforts de détection. Elle dit en outre vouloir prendre en considération toutes les pistes de suggestions soumises par les principaux utilisateurs afin de rendre le système plus performant. Mais, en attendant, le dépistage de la fraude demeure encore très difficile puisque le plan d'action est toujours à un stade embryonnaire. Tant et aussi longtemps que des modifications concrètes ne seront pas apportées au système de détection de la fraude, il sera, selon nous, toujours plus difficile de dépister la fraude.

3.4.2 **Des tâches de validation exigeantes et non garanties**

En plus de la difficulté de dépister les fraudes au forfait mensuel, s'ajoutent celles de l'authentification des renseignements et du repérage des incohérences dans les renseignements personnels ayant trait à des comptes faisant l'objet de soupçons. En premier lieu, les renseignements permettant d'authentifier l'identité d'un abonné peuvent émaner de sources différentes qui ont chacune leurs lacunes, étant indépendantes les unes des autres et ne garantissant pas à coup sûr la validation des renseignements. Par exemple, l'une des

sources fournit les renseignements postaux et téléphoniques résidentiels et de commerce (nom, adresse, numéro de téléphone, etc.) ; d'autres opérateurs du sans fil fournissent des renseignements postaux et téléphoniques sur des abonnés cellulaires; une autre source fournit des fiches de crédit (renseignements personnels et de crédit) et une autre source encore confirme ou infirme des informations relatives aux titulaires de cartes de crédit. En second lieu, il faut souligner les lacunes et les inexactitudes que comportent les fiches de crédit provenant de l'agence de crédit, de même que les restrictions rigoureuses à l'accès aux renseignements personnels provenant, entre autres, des sociétés émettrices de cartes de crédit qui sont d'ailleurs aussi soumises à la Loi sur la protection des renseignements personnels et les documents électroniques. Enfin et en dernier lieu, en plus d'être exigeantes et pas toujours fructueuses, les tâches d'authentification auprès des abonnés du sans fil peuvent également être difficiles. D'une part, le personnel est conscient que rien ne lui permet de s'assurer de l'identité de la personne qui est au bout du fil, notamment quand il en va de fraudeurs professionnels. Cela dit, si un doute persiste au cours du processus d'authentification verbal, il peut y avoir demande d'identification formelle en succursale ou par écrit. Ce d'autant que tous les abonnés ne sont pas disposés à donner des renseignements personnels par téléphone sans connaître un tant soit peu la personne à qui ils s'adressent. Selon nos observations, les citoyens sont de plus en plus préoccupés et sensibilisés par la question du droit à la vie privée et de la protection des renseignements personnels. D'autre part, le personnel est également conscient du danger d'offusquer des clients honnêtes, importunés par la procédure d'authentification et de les inciter à se désabonner.

Il faut savoir en outre que, bien que l'entreprise possède des renseignements personnels issus des fiches de crédit fournies par une agence de crédit nationale (voir annexe 1), elle ne peut pas ouvertement en faire état dans ses échanges avec les abonnés. Rappelons à cet égard que la Loi sur les renseignements personnels et les documents électroniques prévoit que les entreprises doivent utiliser les renseignements relatifs aux clients aux seules fins pour lesquelles ces renseignements ont été recueillis. Par conséquent, même si les fiches de crédit peuvent contenir des renseignements sur la situation matrimoniale, le nom du (de la) conjoint(e), le nom de l'employeur, etc., il ne faut pas en parler avec le client puisque ces informations sont sans rapport direct avec sa solvabilité. Aussi, authentifier les clients par

leur état civil, le nom de leur conjoint(e), le nom de leur employeur, etc. peut constituer une intrusion dans leur vie privée. Bref, la tâche de validation reste délicate puisqu'il faut simultanément respecter la vie privée du client et lui montrer qu'on le fait, tout en vérifiant la véracité de ses propos et en recueillant de l'information personnelle à son sujet. En définitive, le Service de la fraude est donc confronté à plusieurs obstacles découlant d'une part, de l'augmentation du volume d'abonnés faisant l'objet de soupçons et d'autre part, de l'insuffisance des outils à disposition pour procéder à la vérification de l'identité des clients.

CHAPITRE 4 :
DISCUSSION ET CONCLUSION

4.1 LES TECHNIQUES DE PRÉVENTION SITUATIONNELLE

Au terme de la présente étude, il ressort que l'entreprise étudiée a comme principe de lutter contre la fraude en amont, soit dans le cadre de ses politiques organisationnelles de prévention et de réaction, plutôt qu'en aval, c'est-à-dire par des politiques de répression. Pour contrer la fraude, l'entreprise s'est dotée d'une politique générale qui met l'accent sur la réduction des occasions de commettre des activités frauduleuses dans le contexte de la prévention situationnelle. Il s'avère donc intéressant de jeter un regard sur les quatre axes évoqués dans la théorie de la prévention situationnelle de Clark (1997) et de les mettre en rapprochement avec ceux mis en place par l'entreprise et ceux qui ne l'ont pas été.

1- Rendre le passage à l'acte plus difficile :

Il y a certes eu un durcissement de la cible lié au service de télécommunications prépayées au cours de la période étudiée (2001-2003). Plus que jamais, l'accès au paiement par carte de crédit pour l'achat de recharges téléphoniques prépayées est contrôlé, bien qu'il soit difficile de dire si cette nouvelle pratique est connue des fraudeurs. En effet, nous avons vu que l'intérêt des escrocs pour les recharges téléphoniques prépayées s'est considérablement réduit depuis la mise en place d'une série de mesures de vérifications systématiques effectuées par le dispositif de sécurisation des cartes de crédit. En revanche, si le contrôle d'accès est plus que jamais renforcé dans le mode prépayé de souscription, nous verrons à la section suivante (4.2) que nous ne pouvons en dire autant du mode postpayé de souscription, en raison de la vulnérabilité à laquelle l'entreprise s'expose. Néanmoins, le durcissement de la cible de la fraude au forfait mensuel prend la forme d'une nouvelle politique d'authentification des abonnés désireux d'obtenir des services optionnels, politique mise en place à la suite d'importantes fraudes survenues au cours de l'été 1999. Cette mesure vise à rendre plus difficile la souscription mensuelle à un abonnement téléphonique à ceux

dont le but est de se prévaloir de services optionnels comme l'itinérance internationale ou les appels outre-mer.

2- Rendre le passage à l'acte plus risqué :

Tous les abonnés, que ce soit au forfait prépayé ou mensuel, font l'objet de surveillance par le biais d'un registre qui contient l'historique de toutes les activités des usagers. Ce registre alimente en temps quasi réel le dispositif de dépistage de la fraude, lequel alerte le personnel du Service de la fraude quand un abonné fait une utilisation suspecte des services de téléphonie mobile. Ensuite, les employés peuvent, à leur seule discrétion, procéder à l'authentification formelle ou informelle des abonnés. En revanche, nos observations de terrain ont déterminé jusqu'à quel point le dispositif de détection, l'instrument privilégié pour contrer la fraude, est inefficace pour identifier les utilisateurs du sans-fil qui font l'objet de soupçons. À ce titre, le passage à l'acte demeure encore relativement peu risqué.

3- Réduire les bénéfices escomptés du crime :

L'enthousiasme des fraudeurs aux recharges téléphoniques prépayées qui réussissent à déjouer le dispositif de sécurisation des cartes de crédit pourrait bien fléchir. En effet, les nouvelles règles qui limitent le nombre de recharges quotidiennes et hebdomadaires permises, le crédit téléphonique maximal ainsi que le type de cartes de crédit accepté ont pour effet de réduire les gains escomptés de la fraude au forfait prépayé.

Quant aux téléphones mobiles ayant déjà servi à faire une demande frauduleuse, quel que soit le forfait, ils sont maintenant systématiquement enregistrés dans une base de données (liste grise), de sorte que les récidivistes qui tentent de réutiliser ces appareils sont généralement repérés par le dispositif de détection.

4- Montrer le caractère répréhensible du délit en le rendant moins " excusable " :

La dénonciation n'est pas une procédure automatique mais relève de la victime elle-même. Cela dit, la victime d'un délit a le choix de signaler aux organismes de contrôle social l'acte répréhensible dont elle a été la cible. Le cas échéant, si les mécanismes de

contrôle social formel se mettent en place, certains principes généraux du système de justice pénale tels que la rétribution, la rééducation, la dissuasion individuelle et générale peuvent être mis en oeuvre (Cusson,1998).

Dans le cadre ce cette étude, nous avons vu que l'entreprise, quel que soit le type de fraude qu'elle subit, gère elle-même sa propre victimisation en choisissant délibérément de ne pas dénoncer officiellement la fraude. Cette politique de l'entreprise étudiée contraste avec le constat de l'auteur américain Delaney (1993), selon lequel les entreprises de télécommunications ont souvent recours aux organismes d'application de la loi pour mener des enquêtes et traduire en justice les malfaiteurs. Bien qu'il existe des dispositions du code criminel canadien qui permettent de réprimer la fraude en matière de télécommunications mobiles, il semble y avoir un important décalage entre les modes de réactions de l'entreprise et l'application des grands principes sur lesquels est fondée la justice criminelle. Ce choix fait que l'entreprise représente le maillon faible de la chaîne de répression en matière de lutte contre la fraude. Le non recours aux organismes de contrôle social entrave donc l'effet de dissuasion générale ou spécifique et contribue à discréditer l'impact du droit criminel.

Notre étude montre que l'entreprise étudiée, en plus de ne pas faire appel aux sanctions de type formel, n'inflige pas non plus de sanctions informelles qui pourraient appauvrir financièrement (amendes) le délinquant ou encore susciter la réprobation sociale vis-à-vis des tentatives ou des commissions de fraudes. Nous avons déjà d'ailleurs mentionné qu'une fois la fraude mise au jour, le seul désavantage des fraudeurs consiste à se voir imposer une suspension téléphonique des services de téléphonie mobile et l'enregistrement sur une liste grise de numéros de séries du numéro de l'appareil ayant servi à commettre une fraude. Or, ces mesures ne sont que peu dissuasives.

Pour conclure la réflexion sur les techniques de prévention situationnelle, mentionnons que Clark (1997) les juge prometteuses dans la mesure où les quatre axes de la prévention sont mis à contribution de façon parallèle et complémentaire. Il suffit de négliger un seul axe pour compromettre l'efficacité des mesures de prévention situationnelle. Jusqu'à présent, cette recherche a démontré, d'une part, que les techniques de prévention sont inégalement déployées selon le type de fraude et, d'autre part, qu'il y a une absence totale du

dernier axe qui a pour but de montrer le caractère répréhensible du délit. L'absence réelle de mesures de contrôle social formel et informel dénote la faiblesse défensive de l'entreprise. À ce sujet, Cusson (1998) dit qu'une cible est vulnérable si elle est attaquée par un délinquant qui ne sera pas directement l'objet de représailles ni de sanctions pénales. L'auteur ajoute que cette vulnérabilité contribue à augmenter le risque de victimisation (p. 106).

4.2 LA VULNÉRABILITÉ DE L'ENTREPRISE

À la lumière des principes de la théorie des opportunités, nous pouvons affirmer que l'entreprise facilite les conditions permettant que se produisent les activités frauduleuses. Mise à part la présence de fraudeurs potentiels, deux autres facteurs rendent possible la commission des fraudes au forfait mensuel, notamment en ce qui a trait à l'accessibilité à un service téléphonique : les occasions de fraudes et la faiblesse du système d'enquête de crédit.

D'abord, pour ce qui est des occasions de fraude, elles surviennent notamment lors de la demande de souscription à un forfait mensuel mais elles sont encouragées par la faiblesse de la dissuasion des tentatives frauduleuses de demande de souscription. Voici quatre éléments contribuant à cette faiblesse.

1- L'entreprise n'exige pas toujours des pièces justificatives pour s'assurer de l'identité des usagers ;

2- Les clients potentiels n'ont que très peu de renseignements à fournir au moment de souscrire aux services téléphoniques sans fil ;

3- L'entreprise ne prend aucune mesure pour neutraliser les fraudeurs après qu'ils ont commis une tentative infructueuse de fraude. L'entreprise ne relève aucunement l'information relative aux circonstances dans lesquelles les tentatives de fraude ont lieu (numéro d'assurance sociale utilisé, carte de crédit, adresse donnée, etc.). Les fraudeurs n'ont donc rien à craindre et s'en sortent en toute impunité;

4- L'entreprise ne prend aucune mesure en ce qui a trait à la localisation des requérants au moment de la demande de souscription. Lors des demandes en ligne, l'entreprise ne relève pas les adresses IP des internautes, si bien que le Service de la fraude

n'en est pas informé. Il en va de même en ce qui a trait aux demandes de souscription réalisées auprès des centres d'appels. En effet, pour faire leur demande d'abonnement, les fraudeurs peuvent utiliser n'importe quelle ligne de téléphone (numéro local ou numéro sans frais) car l'entreprise ne s'est pas dotée de mesures pour déterminer la provenance des appels de ses clients (date, lieu, heure, etc.) À l'instar des demandes en ligne, les souscriptions réalisées par téléphone peuvent provenir de n'importe quel endroit du monde.

Ensuite, il y a le caractère plus ou moins efficace des moyens de surveillance en matière d'enquête de crédit.

1- Même si le système d'enquête de crédit permet généralement de déterminer si l'abonné potentiel est un bon candidat au crédit, il ne permet pas toujours de vérifier la validité ou la véracité des renseignements fournis par le requérant.

2- Même si l'entreprise prétend coter les requérants selon leur probabilité d'insolvabilité, les observations montrent que durant certaines périodes, dans le but d'acquérir davantage d'abonnés, des exceptions aux critères usuels ont été faites. À titre d'exemple, certaines populations ciblées comme les requérants adultes de Westmount étaient systématiquement acceptés sans égard à leur évaluation de crédit.

3- Outre les exceptions en matière de solvabilité, dans un contexte d'accroissement de la base d'usagers au sans fil à tout prix, il y a également eu des exceptions des critères d'" avertissement de fraude ". Sous le couvert de l'anonymat, un membre du personnel de la fraude a révélé que l'entreprise a délibérément assoupli les conditions générales d'abonnement, de sorte que le système d'enquête de crédit faisait fi des critères d'" avertissement de fraude ", et ce, en raison du taux non négligeable de requérants qui étaient systématiquement refusés.

À la lumière de Cusson (1990 : 78), nous pouvons donc conclure à la vulnérabilité de l'entreprise, qui prend la forme de lacunes défensives de techniques en matière de prévention situationnelle, des grandes facilités d'accès à un service sans fil et de l'impunité qui découle de l'absence réelle de sanctions formelles et informelles. En conséquence, tous ces éléments favorisent l'exécution de délits, et l'ampleur de la vulnérabilité de l'entreprise

peut s'expliquer, en partie du moins, par la rationalité commerciale qui caractérise ses attitudes réactives.

4.3 LA RATIONALITÉ ET LES MOTIVATIONS DE L'ENTREPRISE

Au regard des moyens de lutte de l'entreprise, nous pouvons dire que ceux-ci ne s'inspirent pas des grands principes de droit criminel. L'attitude de l'entreprise étudiée ne s'inscrit pas dans une rationalité de justice puisqu'elle ne dénonce pas les atteintes aux valeurs qui sont défendues par le droit criminel. Pour appréhender les décisions et les bonnes raisons de l'acteur, rappelons brièvement qu'avec Boudon (2002), il convient d'examiner sa rationalité, ses croyances et le système d'interaction dans lequel il se trouve.

Premièrement, en ce qui a trait à la rationalité de l'entreprise en cause, elle est manifestement de type instrumental car elle relève de la logique du profit et de la rentabilité. Cette rationalité bien connue dans le monde économique est donc de type commercial. Elle repose sur le mandat de faire des bénéfices et de demeurer compétitif dans un marché où la concurrence est féroce. Les modes de réactions corporatives que suscite la fraude et qui ont été déployées dans cette étude semblent reposer sur le calcul entre, d'une part, les coûts engendrés pour recourir aux organismes de contrôle social et, d'autre part, la valeur du manque à gagner qui résulte des actes frauduleux. Nous pouvons aussi dire que l'absence totale de contrôle social de la part de l'entreprise en matière de fraude et plus spécifiquement l'absence de dénonciation s'explique, en partie, par le meilleur rendement (maximisation indirect des gains) qui découle de son silence. Dans le contexte des services du cellulaire, où il y a une course perpétuelle à l'accroissement de la part du marché, il est dans l'intérêt de l'entreprise de ne pas divulguer ni dénoncer la fraude, de peur d'alarmer les actionnaires, les investisseurs et les créanciers et de compromettre la fidélisation de ses abonnés.

Deuxièmement, selon Boudon (2002), il n'y a pas que leur rationalité qui détermine les décisions typiques des individus. Pour reconstruire les bonnes raisons des décisions prises par les acteurs, il faut aussi prendre en considération le type de système dans lequel ils se trouvent lorsqu'ils sont en interaction avec autrui. Les dirigeants de l'entreprise tiennent un rôle qui leur fait obligation de générer des profits pour l'entreprise. En effet, les actionnaires

et le conseil d'administration attendent des dirigeants de leur entreprise qu'ils fassent assez de profits pour que les actions prennent de la valeur et qu'elles procurent des dividendes aux actionnaires. Aussi, le rôle qu'assument les responsables du Service de la fraude n'est pas forcément compatible avec les priorités de la direction. Quand le Service de la fraude entend faire plus de dépenses que de profits, le rôle des responsables de la fraude s'avère incompatible avec celui que jouent les dirigeants. Et, dans ces cas-là, la logique de type économique l'emportera le plus souvent sur une logique de type de justice dans la mesure où les objectifs économiques ont préséance sur l'ambition de contribuer à ce que justice se fasse.

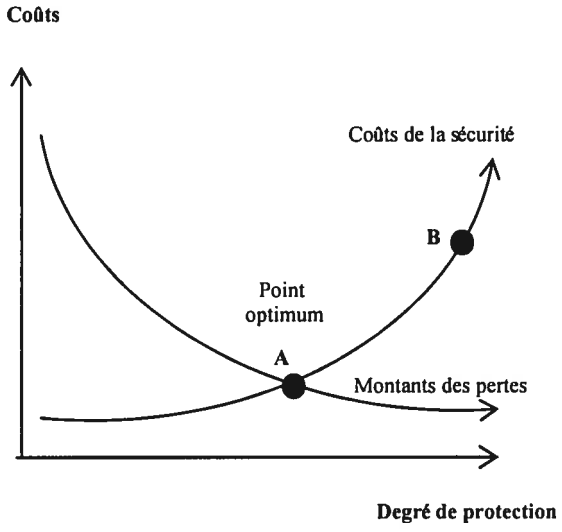
Si l'on part de l'idée que l'entreprise est plutôt régie par une logique de type économique que par une logique pénale, il nous échoit de nous demander, avec les théoriciens de l'analyse stratégique, si l'entreprise a fait de bons choix en matière de parades anti-fraudes tout en atteignant ses fins commerciales.

4.4 LES MOYENS STRATÉGIQUES POUR CONTRER LA FRAUDE

Pour comprendre la rationalité et les tactiques de l'entreprise, des liens peuvent être effectuées, en l'occurrence dans le domaine de la criminalité informatique. Une étude effectuée par Dufour (2002) nous permet d'évoquer des analogies avec la rationalité économique des entreprises de télécommunications face à la criminalité informatique. Du côté des moyens de prévention et de protection, qu'il s'agisse de contrer la délinquance informatique ou celle en matière de téléphonie mobile, les entreprises de télécommunications canadiennes semblentréagir de la même façon que l'entreprise à l'étude, soit de façon réactive et événementielle. Dans sa recherche portant sur les processus de sécurisation des entreprises de télécommunications vis-à-vis la criminalité informatique, Dufour en arrive à la conclusion que les entreprises qu'il a étudiées semblent conscientes des risques auxquels elles sont confrontées. Pour minimiser les pertes, elles mettent en place des dispositifs de sécurisation plutôt rationnels, bien que ceux-ci ne soient pas toujours très efficaces ni déployés de manière optimale. La sécurité informatique des entreprises tend de plus en plus vers une démarche préventive, en dépit du fait qu'elles agissent principalement de façon réactive et événementielle, c'est-à-dire en fonction des incidents déjà survenus.

Selon les théories de l'individualisme méthodologique et de l'analyse stratégique, il est attendu que l'entreprise, pour les fins qu'elle poursuit, adopte les tactiques qui lui semblent les meilleures. Cependant, d'après Rosé (1995) qui s'est également intéressé à la criminalité informatique, une des difficultés auxquelles les entreprises doivent faire face est le double défi de demeurer compétitives et rentables tout en maîtrisant la gestion des risques. De l'avis de l'auteur, qui s'intéresse notamment aux moyens déployés contre la criminalité informatique, ce qui constitue la base d'une démarche cohérente des moyens de prévention et de protection d'une entreprise repose sur la détermination de l'optimum de sécurité. À cela, l'auteur ajoute que pour contrer certaines activités délinquantes, il importe idéalement de trouver un équilibre entre les coûts de la sécurité et le montant des pertes. Le graphique de Rosé (ibid.) reproduit ci-dessous démontre que le point optimum (A) est atteint " lorsque le coût marginal d'un contrôle est égal à la perte marginale qu'il permet d'éviter " (ibid., p. 80). Au-delà du point B, l'auteur soutient que l'investissement en matière de sécurité n'est pas justifié car l'accroissement des contrôles a pour effet d'augmenter les coûts de la sécurité sans pour autant faire diminuer les pertes dans des proportions analogues.

Figure 2 : Détermination de l'optimum de sécurité



Source : Rosé (1995 : 79)

Selon les observations de terrain, l'entreprise a fait d'assez bons choix stratégiques pour trouver des parades anti-fraudes au forfait prépayé. Outre la politique de l'entreprise en matière de recharges prépayées, le dispositif de sécurisation des cartes de crédit a été renforcé au vu des comportements des fraudeurs, à tel point que la fraude au prépayé est presque éliminée. Il a été implanté à un moment où le taux de fraude au forfait prépayé atteignait la proportion de 9 % du chiffre d'affaires, alors que le taux acceptable établi par l'entreprise et l'industrie du sans-fil se situe entre 3 et 5 %. Selon une analyste interviewée, le dispositif de sécurisation a permis de faire diminuer plus de pertes imputables à la fraude au prépayé comparativement à son coût d'implantation.

En ce qui concerne la fraude au forfait mensuel, la situation n'est pas encore complètement maîtrisée. Bien que les outils de dépistage doivent être améliorés, les moyens technologiques tardent à venir. L'attitude des dirigeants de l'entreprise porte à se demander si la somme à investir pour améliorer le dispositif de détection risquerait de dépasser celle qu'ils pourraient épargner. Pour le moment, les taux de fraude au forfait mensuel sont très rassurants par rapport aux points de comparaison du marché du sans-fil. Il est aussi permis de croire que tant que la situation ne sera pas très grave et que le taux de fraude au forfait mensuel n'aura pas dépassé un seuil tolérable établi à 5 %, les moyens tarderont à venir.

Pour terminer, les observations de terrain permettent de dire que l'entreprise a fait de bons choix stratégiques à la suite de l'évaluation des coûts, des avantages et des risques en matière de fraude. Tout porte à croire également qu'il y a adéquation entre l'ampleur du phénomène de la fraude au sein de l'entreprise et la nature des moyens déployés pour la contrer. Or, même si elle a poursuivi ses objectifs commerciaux tout en luttant contre la fraude, il nous est difficile d'affirmer qu'elle a atteint ce point optimum de sécurité que définit Rosé. Pour atteindre ce point, l'entreprise doit disposer d'informations fiables quant à sa situation et être ne mesure de l'interpréter adéquatement. Or, comme l'affirme Boudon (2002), les acteurs disposent généralement d'informations imparfaites au moment de passer à l'action en dépit du fait qu'elles ont l'impression de prendre les meilleures décisions possible. Aussi, en l'occurrence, il y a évidemment lieu de nous demander si l'entreprise à l'étude disposait vraiment de toute l'information utile, notamment à propos de l'ampleur de

la fraude, et de toutes les compétences nécessaires pour parvenir à déterminer si elle a déjà atteint ce point optimum de sécurité au-delà duquel la rentabilité du dispositif irait en décroissant.

Compte tenu du fait que ce point d'équilibre, si tant est qu'il est atteint, est susceptible de se déplacer, notamment en raison de la capacité des fraudeurs à s'adapter aux mesures prises par l'entreprise aux fins d'assurer sa sécurité, et du fait que le vol d'identité est manifestement une activité criminelle qui continue à s'étendre, l'entreprise à l'étude aurait tort de relâcher ses efforts pour contrer la fraude. Aussi, les recommandations qui suivent proposent des actions concrètes de lutte contre la fraude que pourraient mettre en œuvre l'entreprise ainsi que les autorités publiques et privées.

4.5 CONCLUSION ET RECOMMANDATIONS

À la lumière de la théorie de la prévention situationnelle de Clark (1997), l'idéal, pour lutter efficacement contre la fraude, serait d'associer des méthodes de prévention, de détection et de répression. Comme il est peu probable que l'entreprise ait recours aux contrôles formels, il nous apparaît plus réaliste de suggérer qu'elle investisse dans les contrôles informels. De façon plus concrète, l'entreprise doit mettre en œuvre des moyens de prévention, de limitation des opportunités et de dépistage encore plus efficaces pour réduire les ardeurs des escrocs du sans-fil. Par exemple, à court terme, elle devrait :

1 - Se doter d'un système expert pour maximiser les probabilités d'identifier les usagers susceptibles de faire une demande de souscription frauduleuse.

En matière de détection, le taux de dépistage de la fraude est actuellement une préoccupation majeure puisqu'il est largement inférieur au volume des comptes soumis à vérification. Les employés du Service de la fraude perçoivent le dépistage de la fraude au forfait mensuel comme étant de plus en plus difficile et exigeant car ils doivent consacrer beaucoup de temps et d'effort pour mettre au jour un nombre très restreint de fraudes. Les analystes chargés de la détection ont évoqué une autre source d'inquiétude, à savoir que les fraudeurs n'ont aucune difficulté à s'adapter et à déjouer le système de détection. Tout indique qu'il y a lieu à apporter des améliorations susceptibles de faciliter le travail du personnel. À cet égard, un système expert pourrait réduire le nombre de cas non frauduleux qui sont soumis à vérification et augmenter le nombre de cas qui, bien qu'étant frauduleux, échappent à toute vérification. Autrement dit, un système expert permettrait de restreindre aussi bien le nombre de " faux positifs " que de " faux négatifs" et de faire la détection en temps réel, soit le plus vite possible après la mise en activation du service téléphonique.

Depuis la dernière décennie, divers domaines tels que de la médecine, la géologie, les sciences militaires, les assurances, etc., utilisent déjà ce type de système pour obtenir des conseils quant aux meilleures décisions à prendre. Le système se substitue alors à l'humain dans cette fonction de conseiller (O'Leary et O'Leary, 2001 : 64-65).

Premièrement, un système expert à l'usage du Service de la fraude permettrait de définir des modèles de fraude auxquels pourraient être comparés les modus operandi des abonnés sur le réseau sans fil dont il s'agit de savoir s'ils méritent ou non de faire l'objet d'une enquête. Entre autres, ce système pourrait, à partir du registre des appels téléphoniques des abonnés, identifier des éléments qui peuvent entrer dans la description des modus operandi de fraude : les numéros de téléphones les plus fréquemment appelés par les fraudeurs ou la localisation des endroits (adresses, quartiers, villes) à partir desquels les appels téléphoniques sont logés. Deuxièmement, le système expert serait en mesure de faire des profils d'utilisateurs frauduleux en retenant, d'une part, des caractéristiques individuelles comme l'âge et le sexe. D'autre part, le système pourrait mémoriser des informations quant à l'usage que fait ces individus des services téléphoniques. Par exemple, une dame âgée fait une demande de souscription à un service téléphonique comprenant un accès illimité de temps d'antenne les soirs et week-ends et des services personnalisés comme la messagerie texte, la messagerie fax, l'Internet mobile, etc. pourrait correspondre à un type connu d'utilisateurs frauduleux et faire l'objet d'une enquête.

En somme, un tel système conçu spécifiquement pour l'entreprise serait capable de s'adapter aux modèles de fraude qui sont en constante évolution, en mettant continuellement à jours les modus operandi de fraude et d'utilisateurs frauduleux auxquels il s'agit de mettre en parallèle les données nouvellement entrées dans le système. En identifiant les comportements d'usagers qui s'apparentent le plus à des cas de fraude, le travail de dépistage serait grandement amélioré.

Pour augmenter davantage la probabilité de détection, le système expert doit exploiter toutes les bases de données dont dispose actuellement l'entreprise sur ses utilisateurs et leurs comportements sur le réseau sans fil: registre des appels téléphoniques, registre des numéros de série des appareils, système de facturation, modèles d'utilisation légitimes, modèles d'utilisation frauduleuses, etc. De plus, il doit être alimenté par les trois bases de données du Service de la fraude qui fonctionnent présentement de façon indépendante. Ce sont les bases d'enquête de crédit, d'adresses postales et téléphonique et celles de l'agence de crédit. L'intégration de plusieurs sources de données permettrait aussi,

par le recoupement automatique des données, de réduire considérablement la lourdeur de la tâche d'authentification et de repérer très rapidement les incohérences entre les renseignements personnels fournis par le client et les bases de données utilisées par l'entreprise. Pour obtenir de bons scores de prédiction en matière de détection, il importe de s'assurer de la qualité et de la mise à jour régulière des données entrées dans le système expert. Ces données sont celles qui proviennent autant des cas de fraude que des cas qui ne sont pas de la fraude.

En attendant l'implantation d'un tel système, l'entreprise pourrait dans l'immédiat :

2 - Créer une banque de données centrale de renseignements personnels ayant déjà servi à des demandes de souscription frauduleuse et réduire l'accessibilité aux services.

Afin de renforcer sa capacité de prévenir la fraude, le Service de la fraude devrait établir un répertoire dans lequel il recenserait les renseignements nominatifs et personnels (numéro d'assurance social, numéro de carte de crédit, noms et coordonnées, etc.) de chaque cas de fraude. Le registre des noms et coordonnés ayant déjà servi à des demandes de souscription frauduleuse auprès de l'entreprise pourrait approvisionner le système d'enquête de crédit et, ultimement, le système expert.

La création d'une banque de données centrales au sein de l'entreprise exige toutefois des modifications législatives à la Loi sur la protection des renseignements personnels et les documents électroniques dans le secteur privé. L'obtention d'aménagements législatifs permettrait d'établir de nouvelles règles s'appliquant aux entreprises pour collecter et utiliser des renseignements personnels. Par exemple, pour assurer la confidentialité des renseignements personnels et faire en sorte qu'ils soient utilisés qu'aux seules fins de détection de fraude, l'accès à de tels renseignements pourrait être limité à un nombre restreint de personnes au sein du Service de la fraude de l'entreprise.

3 – Bloquer automatiquement l'utilisation des appareils portables ayant déjà servi à une demande frauduleuse de souscription.

L'entreprise sait que les récidivistes peuvent facilement se reconnecter au réseau sans fil en réutilisant le même portable. Il nous paraît inconcevable que l'entreprise ferme les yeux et permette la réutilisation de ces portables alors qu'elle possède les moyens techniques de les interdire sur son réseau. Bien que les numéros de série des appareils ayant déjà servi à une demande frauduleuse se retrouvent sur une liste grise et que les récidivistes soient généralement repérés par le système de détection, ils ne font alors que l'objet de vérifications. Ainsi, la réaction de l'entreprise devrait être plus coercitive afin d'envoyer un message dissuasif à certains récidivistes. Elle pourrait par exemple adopter une politique analogue à celle qui concerne les appareils perdus ou volés. En effet, pour mettre un frein au vol aux mobiles, l'entreprise bloque automatiquement l'accès au réseau aux portables de ses propres usagers qui les ont déclarés perdus ou volés (liste noire des IMEI).

Les deux premières propositions supposent donc le développement de meilleures compétences qui permettront de mieux appréhender et documenter le phénomène de la fraude. Dans cette optique, le développement de la recherche criminologique en matière de fraude dans le domaine des télécommunications sans-fil s'impose. D'ailleurs, l'entreprise pourrait ainsi disposer de renseignements plus fiables pour mieux parvenir à déterminer les modèles de fraude, les caractéristiques des fraudeurs, son ampleur et sa position par rapport au point optimum de sécurité. La troisième proposition repose sur un constat. Comme l'entreprise crée elle-même de nombreuses opportunités criminelles, elle devrait lutter davantage contre la fraude qu'elle suscite.

Plus largement et à plus long terme, compte tenu du fait que le vol d'identité est un phénomène assez répandu qui va en croissant, la recherche qui lui est consacrée pourrait être effectuée en étroite collaboration avec les autorités publiques et privées. Un mémoire du Protecteur du citoyen du Québec à la Commission de la culture rapportait, en septembre 1997, que le vol d'identité sera la fraude dominante du XXI^{e} siècle, les fraudeurs n'ayant besoin que de quelques renseignements sur chaque individu pour se créer une identité et

procéder ainsi à toutes sortes de transactions (Protecteur du citoyen, Page Web). De plus, la vérificatrice générale, Sheila Fraser, a fait des recommandations au gouvernement fédéral en octobre 2002 dans un rapport où elle se disait particulièrement préoccupée par la fraude reliée au vol d'identité. À son avis, la fraude par vol d'identité est une préoccupation croissante car elle sert de tremplin aux malfaiteurs ou aux organisations criminelles pour la commission d'infractions beaucoup plus graves (Cyberpresse, Page Web). À ce même sujet, un rapport spécial a été publié conjointement par le solliciteur général du Canada et le département de la Justice des États-Unis en mai 2003. Ce rapport, qui consistait en un avertissement public lancé aux consommateurs, avait pour objectif d'informer les Canadiens sur les types de fraudes reliées au vol d'identité, sur les méthodes employées par les fraudeurs ainsi que sur les moyens de se protéger (Sécurité publique et Protection civile Canada, Page Web). Cela dit, l'application de techniques de prévention situationnelle pourrait s'avérer encore plus efficace pour contrer la fraude si des partenariats publics, privés ou mixtes se développaient. Un problème vient aussi d'être mis en évidence : il s'agit du recensement des fraudes à la téléphonie mobile et des vols d'identité en général. Nous avons vu en effet que les problèmes méthodologiques viennent essentiellement du fait qu'il n'existe, pour l'heure, aucune procédure de déclaration uniforme ou de centralisation qui permette de disposer d'un observatoire statistique fiable, cohérent et constamment remis à jour.

Dans le cadre d'une stratégie globale de lutte contre le vol d'identité, nous proposons la création d'un organisme central canadien qui se chargerait de la centralisation et de la coordination des renseignements personnels ayant servi à des demandes frauduleuses. Cet organisme devrait ensuite informer lui-même les deux agences de crédit canadiennes afin qu'un " avertissement de fraude " soit inscrit dans le dossier de crédit des victimes de fraude. Cet avertissement permettrait de protéger non seulement la victime de vol d'identité mais aussi d'aviser les futurs prêteurs que cet individu s'est déjà déclaré victime.

Enfin, nous sommes d'avis que les malfaiteurs qui cachent leur véritable identité n'obtiennent pas que des services de télécommunications mobiles. Il y a fort à parier qu'ils commettent des activités similaires dans le but d'obtenir frauduleusement des permis de

conduire, des passeports, des cartes de crédit, des cartes d'assurance social, des cartes d'assurance-maladie, etc. De plus, nous avons quelques raisons de penser que les services de télécommunications sans fil ne font pas uniquement l' "objet" de crime mais qu'ils peuvent également être l'" instrument " de crimes plus graves encore comme le trafic de drogues, le trafic d'armes, le blanchiment d'argent, le télémarketing frauduleux, etc.

BIBLIOGRAPHIE

Association Canadienne des Télécommunications Sans fil (ACTS) : http://www.cwta.ca

Basset Telecom Solutions (2001). *Fraud Prevention and Detection Handbook*, Sundbyberg, Sweden.

Bernatchez, Eric (2000). " Pour qui sonne l'heure du prépayé? ", *La Presse*, 22 novembre, p. D4.

Beseler, Peter R. (1997). " Operation Cellmate ", *FBI Law Enforcement Bulletin*, vol. 66, no 4 (April), pp. 1-8.

Blackwell, Gerry (1999). " Meet The Fraud Busters ", *Wireless Telecom*, (Fourth Quarter), pp. 62-65.

Boudon, Raymond (2002). Les méthodes en sociologie, (avec R. Fillieule), Paris : Presses Universitaires de France (Que sais-je ?), 1969, 12e édition, 128 p.

Boudon, Raymond (2002a). " Théorie des choix rationnels ou individualisme méthodologique? ", in La théorie du choix rationnel contre les sciences sociales ? Bilan des débats contemporains, *Sociologie et Société*, vol. 34, no 1, pp. 9-34.

Briscoe, Suzanne (2001). *The problem of mobile phone theft*, New South Wales Bureau of Crime Statistics and Research, Sydney, 6 p.

Cellular Telephone Industry Association (CTIA), Wireless Telephone Fraud: http://www.ctia.org

Cherry, Paul (2001). " Cloned cell phones led to fraud ring cops ", *The Gazette*, 27 juillet, p. A3.

Clarke Ronald V. (1995). Les technologies de la prévention situationnelle, *Les Cahiers de la sécurité Intérieure,* no 21, pp. 101-113.

Clarke, Ronald V. (1997). Introduction, In Clarke, Ronald V. (ed.). *Situational Crime Prevention: Successful Case Studies* (2nd ed.), pp.1-43, Albany: Harrow and Heston.

Clarke, Ronald V; Kemper, Rick and Wyckoff, Laura, (2001). " Controlling Cell Phone Fraud in the US: Lessons for the UK " Foresight " Prevention Initiative ", *Security Journal*, vol. 14, no 1, pp. 7-22.

Code Criminel du Canada : http://lois.justice.gc.ca/fr/C-46/index.html

Cohen, Lawrence and Felson, Marcus (1979). " Social Change and Crime Rate Trends: A Routine Activity Approach ", *American Sociological Review*, no 44, 1979, pp. 588-608.

Collins, Simon (1999a). " Prepaid Vouchers: The Good, The Bad and The Ugly ", *Security and Fraud Newsletter*, (November), pp. 5-8.

Collins, Simon (1999b). " Case Study: Pre-paid – Panacea or Problem? ", *Security and Fraud Newsletter*, (February), pp. 9.

Committee of the Judiciary (1997). Cellular Telephone Fraud Hearing before The Subcommittee on Crime of the Committee on The Judiciary, House of Representatives, One Hundred and Fifth Congress, First session, September 11, 1997, Serial No 77. Washington, DC : US Government Printing Office: http://commdocs.house.gov/committees/judiciary/hju55946.000/hju55946_0f.htm

Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), Loi sur les télécommunications : http://www.crtc.gc.ca/frn/LEGAL/TELECOM.HTM

Cornish, Derek B. and Clarke, Ronald V. (1986). Introduction. In Cornish, Derek and Ronald Clarke (eds.). *The Reason Criminal,* pp. 1-16. New York: Springer-Verlag

Cousineau, Sophie, (1995). " Les escrocs du cellulaire étendent leurs tentacules. Bell Mobilité ne dessert plus ses abonnés dans certaines villes américaines ", *Le Soleil*, mardi 25 juillet, p. A1.

Cunningham, Norbert (1995). " Gare aux puces ", *Actualité-Justice*, vol. 10, no 4, pp. 6-8.

Cusson, Maurice (1989). Délinquants pourquoi? (Réédition). Montréal : Hurtubise HMH, 301 p.

Cusson, Maurice. (1990). Croissance et décroissance du crime. Paris : Presses Universitaires de France, 170 p.

Cusson, Maurice (1998). La Criminologie, Paris : Hachette (Les Fondamentaux), 160 p.

Cyberpresse (2002). " Cinq millions de cartes d'assurance sociale de trop", *Presse Canadienne*, mardi 8 octobre, : http://www.cyberpresse.ca/

De Calan, Jeanne (1995). " La prévention situationnelle en Angleterre : fondements, pratiques et enjeux. ", *Les Cahiers de la sécurité Intérieure*, no 21, 3 ème trimestre, pp. 143-157.

Delaney, Donald P. (1993). *Investigation Telecommunications Fraud in Criminal and Civil Investigation Handbook*, Part 6. Business-Oriented Crimes, pp. 35-1-35-8, 2nd ed., McGraw-Hill, New York: Grau, J.J (ed).

Deslauriers, Jean-Pierre et Kérisit, Michèle (1997). Le devis de recherche qualitative dans *La recherche qualitative : enjeux épistémologiques et méthodologiques* (Poupart et al.), Montréal : G. Morin Éd., pp. 212-249.

Dubowski, Stefan (2001). Technologie sans fil : le beau, le bon et le mauvais, Québec Micro, (juillet), pp. 8-10.

Dufour, Pascal (2002). Analyse des processus de sécurisation des entreprises de télécommunication québécoise face à la criminalité informatique, Montréal : Université de Montréal. Mémoire inédit.

Dupaul, Richard, (1995). " Fraude cellulaire : le phénomène est négligeable au Québec ", *La Presse*, jeudi 27 juillet, p. B7.

Ericsson: http://www.ericsson.fr

Grabosky, Peter N.; Smith, Russel G.; Wright, Paul (1996). " Crime and Telecommunications ", *Trends & Issues in Crime and Delinquency*, vol. 59, no 6, pp. 1-6.

Grabosky, Peter N. and Smith, Russel G. (1997). " Telecommunications and Crime: Regulatory Dilemmas ", *Law & Policy*, vol. 19, no 3, pp. 317-341.

Grabosky, Peter N.; Smith, Russel G.; Wright, Paul (1998). " Nouvelles technologies, nouveaux délits ", *Les Cahiers de la sécurité intérieure*, vol. 34, no 1, pp. 13-29.

GSMBOX (2000), " La fraude des Télécoms a atteint 22 billions de dollars par an" : http://fr.gsmbox.com/news/mobile_news/all/8255.gsmbox

Harvey, Claire, " Protégez-vous contre le vol d'identité ", *La Presse*, dimanche 8 avril 2001, p. A 13.

Hoad, Christopher D. (1996). *The Impact of Mobile Telephony upon the organization and practice of crime*. Loughborough University of Technology. United Kingdom : Not published.

Hoffman, Charles E. (2000). " La nouvelle ère de la convergence ", *Technologie canadienne*, (novembre), p. 10.

Jaccoud, Mylène et Mayer, Robert (1997). L'observation en situation et la recherche qualitative dans *La recherche qualitative : enjeux épistémologiques et méthodologiques* (Poupart et al.), Montréal : G. Morin Éd., pp. 212-249.

Janhevich, Derek E. (1998). " L'évolution de la nature des fraudes au Canada ", *Juristat*, vol.18, no 4, 16p. Ottawa : Statistiques Canada, Centre canadien de la statistique juridique.

KPMG Canada (1995). *1995 Police Chiefs Survey*. Peat Marwick Thorne – KMPG Investigation and Security Inc. Toronto.

Landry, Johanne (2001). " Cellulaire à tout faire... ", *Affaires Plus*, (mai), pp. 35-39.

Littman, Jonathan : The Fugitive Game; online with Kevin Mitnick: http://hpgx.net/willday/mitnick.html

McGregor, Scott (1998). " A Law Enforcement Perspective ", *La Gazette de la GRC*, vol. 63, (September/October), pp. 60-63.

Michelat, Guy (1975). " Sur l'utilisation de l'entretien non directif en sociologie ", *Revue française de sociologie*, vol. 16, pp. 229-247.

Microcell Télécommunications Inc. (1999). *Rapport Annuel 1999*.

Microcell Télécommunications Inc. (2001). " L'évolution du téléphone sans fil : d'hier à demain ", *Opus*, (novembre), p. 3.

Microcell Télécommunication Inc : L'ABC des SCP : http://www.microcell.ca/microcell/navigation.jsp?sectionID=9&subSectionID=154&pageContent=technoparc/glossaire.html&lang=fr

Microcell Télécommunications Inc, Microcell conclut un accord d'itinérance avec Mobilité Canada. http://www.microcell.ca/navigation.jsp?sectionID=2&pageContent=telecom/headlines.html&lang=fr&Div=TE&DocId=72&pge=1&caller=TE.jsp

Ministère de la Justice (1997). Rapport du groupe de travail Canada-États-Unis sur le télémarketing frauduleux. Ottawa : Approvisionnement et Services.

Mondoux, André (2000a). " Convergence des technologies : N'importe où, n'importe quand ! ", *Info-tech*, (octobre), pp. 36-38.

Mondoux, André (2000b). " La téléphonie cellulaire répond à l'appel ", *Info-tech*, (octobre), pp. 52-57.

Mucchielli, Alex (sous la direction de) (1996). Dictionnaire des méthodes qualitatives en sciences humaines et sociales. Paris: Masson et Armand Colin Éd.

Natarajan, Mangai; Clarke, Ronald V.; Jonhson, Bruce D. (1995). " Telephones as Facilitators of Drug Dealing: A Research Agenda ", *European Journal on Criminal Policy and Research*, vol. 3, no 3, pp.137-154.

Nortel Networks Fraud Solutions (2000). " Club Cerebrus swells its ranks ", *FraudVision*, (November), pp. 1-4.

O'Brien, John T. (1998). " Telecommunications Fraud – Opportunities for Techno-Criminals ", *FBI Law Enforcement Bulletin*, vol. 67, (May), pp.20-25.

Office of the Privacy Commissioner of Canada, " Identity Theft: What it is and what you can do about it " : http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp.

O'Leary, Timothy et O'Leary, Linda (2001). Éléments d'informatique, traduction de Computing Essentials, 4e ed., Montréal : Chenelière/McGraw-Hill.

Option consommateurs : http://www.option-consommateurs.org

PhoneBusters : http://www.phonebusters.com

Pires, Alvaro P. (1997). Échantillonnage et recherche qualitative: essai théorique et méthodologique in *La recherché qualitative: enjeux épistémologiques et méthodologiques*, (Poupart et al.), Montréal : G. Morin Éd., pp. 113-169.

Poupart, Jean (1997). L'entretien de type qualitatif : considérations épistémologiques, théoriques et méthodologiques in *La recherche qualitative: enjeux épistémologiques et méthodologiques* (Poupart et al.), Montréal : G. Morin Éd., pp.173-209.

Praesidium : " Fraud Risks For New Mobile Operators ": http://www Praesidium.co.uk

Protecteur du citoyen du Québec (1997). " Les cartes d'identité et la protection de la vie privée ", (septembre): http://www.protecteurducitoyen.qc.ca/fr/publications

Office of the Privacy Commissioner of Canada, " Identity Theft: What it is and what you can do about it " : http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp.

Ramsay, Charles-Albert (2000). " Le cellulaire commandité brouille les cartes dans le service prépayé ", *Les Affaires*, 16 décembre 2000, p. 5.

Reuters – La Presse, Le jeudi 14 mars 2002, Londres, " Les opérateurs de téléphonie 3G face aux risques de piratage " : http://www.cyberpresse.ca/reseau/internet/0203/int_102030076853.html

Richardson, Karen, " Le contour incertain des appareils de troisième génération ", *La Presse*, 12 décembre, 2000, p. D5.

Rico, José M. (1977). " Notes introductives à l'étude de la criminalité d'affaires ", *Criminologie*, vol. 10, no 1, pp. 8-28.

Rogers AT&T Communications sans fil – Salle de presse - Rogers AT&T Communications Sans Fil - Profil de l'entreprise : http://www.rogers.com/francais/corporate/newsroom/wireless/newsroom_profile.html

Rosé, Philippe (1995). *La criminalité informatique*, 2e éd. Paris : Presses universitaires de France, (Que sais-je ?).

Sécurité publique et Protection civile Canada : http://www.psepc.gc.ca/publications/policing/Identity_Theft_Consumers_f.asp

Sigrist, Gabriel (1999), " L'avenir du téléphone mobile, c'est l'image en direct ", *Le Temps* : http://www.letemps.ch/dossiers/telecom99/supplement/patte.html#Anchor-44867

Simmonds, Joe, (2000). " Microcell, Total Risk Management ", *Economic Data Network*, vol. 1, no 3, pp. 5-6.

Solicitor General Canada. " Public Advisory - Special Report for Consumers on Identity Theft " : http://www.sgc.gc.ca/publications/policing/Identity_Theft_Consumers_e.asp.

Smith, Russel G. (1996a). " Stealing telecommunications services ", *Trends & Issues in Crime and Delinquency*, vol. 54, no 6, pp. 1-6.

Smith, Russel G. (1996b). *Preventing mobile telephone crime*, Australian Institute of Criminology, Canberra, ACT, 10 p.

United State Sentencing Commision: http://www.ussc.gov/publicat/clonexs.PDF

ANNEXE 1

Les types de renseignements contenus dans la fiche de crédit d'un requérant et pris en compte par l'agence de crédit lors du processus d'évaluation de solvabilité :

Les dossiers de crédit des demandeurs de l'agence de crédit dont il est question dans cette recherche renferment les types de renseignements suivants sur les requérants. L'ensemble des renseignements fournis est alors pris en considération lors du processus d'évaluation de solvabilité, lequel se traduit par un pointage de trois chiffres (1 à 999).

RENSEIGNEMENTS

Seules les personnes ayant fait une demande de crédit ou de prêt sont répertoriées au sein de l'agence d'évaluation de crédit.

1. Renseignements nominatifs et renseignements personnels :
    a. Renseignements nominatifs actuels : nom, prénom (s);
    b. Renseignements nominatifs répertoriés antérieurement : nom (s) et prénoms;
    c. Renseignements personnels : numéro d'assurance sociale et date de naissance.

2. Coordonnées des sept dernières années :
    a. Adresse complète;
    b. Numéro de téléphone à la maison ou au bureau, ou les deux.

3. État civil, nom du conjoint (antérieur, actuel ou les deux)

4. Employeurs (actuel et antérieurs)

INFORMATION DE CRÉDIT

5. Date d'ouverture du fichier : indique la date de la première demande de crédit du requérant auprès des institutions financières, des sociétés émettrices de cartes de crédit, des grands magasins ou encore des entreprises qui font du crédit. Seuls les prêteurs qui rapportent les emprunts au sein de l'agence sont répertoriés dans la base de données de l'agence de crédit.

6. Types et historiques de crédit avec les institutions financières :
    a. Noms des prêteurs : Banque Nationale, Caisse Populaire, CIBC, Visa, Master Card, American Express, etc.;

b. Type de crédit : prêt hypothécaire, prêt automobile, ligne de crédit personnel, cartes de crédit , etc.;
c. Limites de crédit accordé (en dollars);
d. Soldes dus : indique le solde actuel;
e. Historique de paiement : indique si l'emprunteur effectue ses versements aux échéances.

7. Types et historiques de crédit avec les sociétés qui accordent du crédit
   a. Noms des prêteurs :
      i. Grands magasins : ex. : Sears, Brault et Martineau, Canadian Tire
      ii. Sociétés de crédit : ex. : Household Finances
      iii. Sociétés automobiles : ex. : Honda Canada Finances, Ford Canada etc.
      iv. Sociétés de télécommunications sans fil
   b. Limites de crédit accordé (en dollars);
   c. Soldes dus et calcul du taux d'endettement en pourcentage : indique le solde actuel et compare les sommes dues sur les limites de crédit de divers prêteurs;
   d. Historique de paiement : indique si l'emprunteur effectue ses versements aux échéances.

Aux yeux de certains prêteurs, faire plusieurs demandes de crédit sur une courte période de temps est perçu comme un signe des difficultés financières du requérant.

REGISTRES PUBLICS CIVILS ET RECOUVREMENT DES CRÉANCIERS

8. Jugements : indique si une décision a déjà été rendue par une autorité judiciaire dans une action ou une poursuite civile.
9. Recouvrements : indique les comptes en souffrance des créanciers. En plus des noms des créanciers, le solde, la date de la créance, le statut de la créance (payée ou non payée) apparaissent sur la fiche de crédit.

ALERTE OU AVERTISSEMENT DE FRAUDE À L'INTENTION DES PRÊTEURS :

10. L' " avertissement de fraude " ne concerne pas le demandeur lui-même, mais plutôt un tiers qui aurait subtilisé l'identité du demandeur. En d'autres termes, l'" avertissement " inséré dans le dossier de crédit du requérant indique aux prêteurs que ce dernier a déjà déclaré à l'agence de crédit avoir été victime de vol d'identité. L'avertissement émis par le système d'enquête de crédit a donc pour but d'inciter l'entreprise à communiquer avec le requérant afin d'authentifier sa demande d'ouverture de compte.