Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

CASELAW ON IDENTITY THEFT

April, 2007

CIPPIC Working Paper No. 4 (ID Theft Series)

www.cippic.ca

CIPPIC Identity Theft Working Paper Series

This series of working papers, researched in 2006, is designed to provide relevant and useful information to public and private sector organizations struggling with the growing problem of identity theft and fraud. It is funded by a grant from the Ontario Research Network on Electronic Commerce (ORNEC), a consortium of private sector organizations, government agencies, and academic institutions. These working papers are part of a broader ORNEC research project on identity theft, involving researchers from multiple disciplines and four post-secondary institutions. For more information on the ORNEC project, see www.ornec.ca .

Senior Researcher: Wendy Parkes
Research Assistant: Thomas Legault
Project Director: Philippa Lawson

Suggested Citation:
CIPPIC (2007), "Caselaw on Identity Theft", CIPPIC Working Paper No.4 (ID Theft Series), April 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic.

Working Paper Series:
No.1: Identity Theft: Introduction and Background
No.2: Techniques of Identity Theft
No.3: Legislative Approaches to Identity Theft
No.3A: Canadian Legislation Relevant to Identity Theft: Annotated Review
No.3B: United States Legislation Relevant to Identity Theft: Annotated Review
No.3C: Australian, French, and U.K. Legislation Relevant to Identity Theft: Annotated Review
No.4: Caselaw on Identity Theft
No.5: Enforcement of Identity Theft Laws
No.6: Policy Approaches to Identity Theft
No.7: Identity Theft: Bibliography

CIPPIC

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) was established at the Faculty of Law, University of Ottawa, in 2003. CIPPIC's mission is to fill voids in law and public policy formation on issues arising from the use of new technologies. The clinic provides undergraduate and graduate law students with a hands-on educational experience in public interest research and advocacy, while fulfilling its mission of contributing effectively to the development of law and policy on emerging issues.

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
57 Louis Pasteur, Ottawa, ON K1N 6N5
tel: 613-562-5800 x2553
fax: 613-562-5417
www.cippic.ca

EXECUTIVE SUMMARY

This paper presents an inventory and analysis of identity theft caselaw in Canada and the U.S. as of December 2006. It covers criminal, civil, and administrative cases in both countries. For Canada, relevant findings of the Federal Privacy Commissioner are analyzed. For the U.S., decisions of Federal Trade Commission cases are discussed. Briefs of all cases referred to in this Working Paper are included in Appendices (one with Canadian cases; the other with U.S. cases). Most cases involve criminal prosecutions focusing on fraudulent uses of stolen personal information. Sentences tend to be mild, especially when compared with those in the U.S. Identity theft has not figured directly in many civil or administrative cases in Canada.

NOTE RE: TERMINOLOGY

The term "identity theft" as used in this Working Paper series refers broadly to the combination of unauthorized collection and fraudulent use of someone else's personal information. It thus encompasses a number of activities, including collection of personal information (which may or may not be undertaken in an illegal manner), creation of false identity documents, and fraudulent use of the personal information. Many commentators have pointed out that the term "identity theft" is commonly used to mean "identity fraud" and that the concepts of "theft" and "fraud" should be separated. While we have attempted to separate these concepts, we use the term "identity theft" in the broader sense described above. The issue of terminology is discussed further in the first paper of the Identity Theft Working Paper series.

TABLE OF CONTENTS

Page

1. INTRODUCTION

This paper reviews identity theft caselaw in Canada and the United States as of December 2006. The review covers thirty three Canadian criminal cases, seven civil cases, two judicial reviews and five Privacy Commissioner investigations under the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*").[1]

Due to the large number of U.S. federal and state identity theft cases, only a selection of cases is included. Three Federal Trade Commission cases, twenty two appellate criminal cases, four civil cases and three administrative law cases are reviewed.

Table 1 categorizes the Canadian and U.S. cases by the identity theft technique used. Appendices A and B contain case briefs of the Canadian and American cases respectively. Security breach cases in both countries are discussed CIPPIC's White Paper on "Approaches to Security Breach Notification", which was released in January 2007.

2. CANADIAN CASELAW

2.1. Criminal Cases

As noted in the "Introduction and Background" Working Paper, identity theft is sometimes considered a relatively new phenomenon. But, in fact, it has existed in various forms for quite some time. The offences used to charge identity thieves have existed in statutes, such as the *Criminal Code*,[2] for many years. Many cases in the past deal with what would today be viewed as "identity theft," even if that term was not used in the judgment.[3]

More recently, the term "identity theft" has started to appear in Canadian decisions. Generally speaking, however, the Canadian courts have been slow to acknowledge that the cases being decided are "identity theft" prosecutions. This is no doubt due to the fact that in Canadian law, there is no specific offence of "identity theft." This contrasts with the U.S. where many statutes exist, at both the federal and state levels, dealing specifically with identity theft.[4]

Most of the criminal cases reviewed deal with the unlawful uses of personal information, such as fraud and the unlawful use of credit cards. The only case dealing with the

---

[1] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5, online: <http://laws.justice.gc.ca/en/P-8.6/> [*PIPEDA*].
[2] *Criminal Code*, R.S.C., 1985, c.C-46, online : <http://laws.justice.gc.ca/en/C-46/>.
[3] One difference between the past and the present was mentioned by the court in the Canadian case of *R. v. Harris*, [2004] B.C.J. No. 2847, 2004 BCPC 532 (Prov. Ct. (Crim. Div.)) [*Harris*]. The court indicated that in centuries past, identity theft amounted to a capital crime, subject to significant penalties. Today, by contrast, for a typical personation offence, an identity thief faces a maximum of a few years in jail.
[4] The legislative framework for identity theft in Canada and the U.S. are reviewed in the Working Paper in this series entitled "Legislative Approaches to Identity Theft."

collection phase of identity theft, albeit indirectly, is the 1988 Supreme Court case of *R. v. Stewart.*[5] Here, the court held that obtaining confidential information without taking its physical medium, such as a sheet of paper, is not theft under s. 283(1) of the *Criminal Code*. The result is that unless personal information is used to commit an offence, its mere possession is completely legal.

The problem with the legality of possessing personal information is exemplified by cases such as the 2004 British Columbia case, *R. v. Harris.*[6] Harris was in possession of a notebook containing 39 MasterCard accounts whose numbers did not belong to him. Harris was not charged with an offence as he had not as yet used these credit card accounts.

In another British Columbia case, *R. v. McNeil,*[7] the accused possessed a variety of personal information, including a driver's licence, health card, address, home phone number, date of birth, cell phone number, bank and line of credit balances. However, McNeil was charged only with possession of a homemade mail key.

A similar situation is described in the 2004 Ontario case, *Bongeli v. Citibank Canada*.[8] Bongeli was in possession of personal information belonging to a number of individuals. He was only charged, however, with breach of trust.

2.1.1. Common Traits

The criminal cases analyzed have traits in common. First, in most cases, the accused pled guilty to the charges. This suggests that charges are laid and prosecuted only when the prosecutors and police are reasonably certain of obtaining convictions. Very few convictions are appealed, which seems to confirm this suspicion.

A further common characteristic is the reliance on mail theft to obtain personally identifiable information about victims. This was the situation in the 2004 Alberta case of *R. v. Bradley,*[9] and in three British Columbia cases: *R. v. McNeil,*[10] *R. v. Tonks,*[11] and *R. v. Adamkewich.*[12]

In many cases, the accused presented false identification to law enforcement officials at the time of arrest. This was the situation in *R. v. Bradley,*[13] *R. v. Jubbal,*[14] *R. v. Taft,*[15] and *R. v. Rafuse*.[16]

---

[5] *R. v. Stewart*, [1988] 1 S.C.R. 963 [*Stewart*].
[6] *Harris*, *supra* note 3.
[7] *R. v. McNeil*, [2006] B.C.J. NO. 187, 2006 BCPC 32 (C.A.) [*McNeil*].
[8] *Bongeli v. Citibank Canada*, [2004] O.J. No. 3272 (Ont. Sup. Ct. (Civ. Div.)) [*Bongeli*].
[9] *R. v. Bradley*, [2004] A.J. No. 1278, 2004 ABCA 362 (Alta. C.A.) [*Bradley*].
[10] *McNeil*, *supra* note 7.
[11] *R. v. Tonks*, [2003] B.C.J. No. 3042, 2003 BCPC 475 (Prov. Ct. (Crim. Div.)) [*Tonks*].
[12] *R. v. Adamkewich*, 1990 CanLII 1006 (B.C. C.A.) [*Adamkewich*].
[13] *Bradley*, *supra* note 9.
[14] *R. v. Jubbal*, [2004] B.C.J. No. 2207, 2004 BCPC 389 (Prov. Ct. (Crim. Div.)) [*Jubbal*].

A few cases also involved a breach of trust by an employee. As the caselaw shows, insider abuse can happen at all levels of an organization. For example, in the 2005 British Columbia case of *R. v. P.T.*,[17] P.T. was a bank branch manager who had obtained loans in the name of different clients. Breach of trust was also noted in cases where employees skimmed cards and forged or stole passports. In one of the PIPEDA cases, the Privacy Commissioner noted that no security system, no matter how sophisticated, can prevent determined insiders.

Finally, the sentences handed down are generally mild, especially for first time offenders. The reasoning of the courts has been that the crimes did not involve violence.

2.1.2. Policy Considerations

In a number of cases, the court raised policy considerations relating to identity theft in its reasons. Some judges recognized that identity theft victimizes not only the businesses or organizations being defrauded, but also every person in the community who holds a valid credit card and who could be subject to interest rate increases as a result of the fraud. Some courts also noted that identity theft is a growing problem that threatens the integrity and stability of the economic order on which we all rely. One judge commented that identity theft will ultimately result in a lack of faith in the postal system and in the validity of driver's licences and identification documents.

Courts have sometimes acknowledged the problems identity theft victims face when their identity is abused. For example, victims must expend time and effort to have fraudulent use removed from their record. At minimum, they are usually inconvenienced by the identity theft. One judge referred to: "the myriad of problems identity theft causes for law abiding citizens."[18]

Where insiders commit identity theft, courts have noted and denounced this breach of trust.

2.1.3. Sentencing

(i) *Sentencing Principles*

Many of the cases analyzed refer to the following sentencing principles in their reasons:

- the need for general deterrence and public denunciation to let like-minded individuals know that custodial sentences will result from this type of activity;

---

[15] *R. v. Taft*, [2003] B.C.J. No. 3042, 2003 BCPC 475 (C.A.) [*Taft*].
[16] *R. v. Rafuse*, [2004] S.J. No. 787, 2004 SKCA 161 (Sask. C.A.) [*Rafuse*].
[17] *R. v. P.T.*, 2005 BCPC 55 (Prov. Ct. (Crim. Div.)) [*P.T.*].
[18] *R. v. R.W.*, [2006] B.C.J. No. 830 (Prov. Ct. (Crim. Div.)), 2006 BCPC 154 [*R.W.*].

- the need for specific deterrence to ensure that the accused will understand that this type of behaviour is not tolerated; and
- public protection, which is broader than mere protection from serious bodily harm or the risk of the accused re-offending.

(ii) *Aggravating Factors*

Many of the cases analyzed refer to the following as aggravating factors:

- a high amount of the fraud;
- the degree of premeditation;
- that the fraud was perpetrated by an organized group;
- a high degree of sophistication;
- a related criminal record and continued involvement in crime;
- breach of trust;
- a lack of restitution;
- the offender being on bail or probation;
- the use of documents obtained by identity theft and the use of others' identities;
- a significant amount of time over which the scheme is carried out;
- a lack of cooperation with law enforcement; and
- the motive for the fraud being "greed" rather than "need."

(iii) *Mitigating Factors*

Many of the cases analyzed refer to the following as mitigating factors:

- an early guilty plea;
- a lack of a criminal record;
- any efforts towards restitution;
- an offender's employment or possibility of employment;
- any volunteer work;
- the young age of the accused;
- cooperation with law enforcement; and
- being the provider for the family.

2.1.4. Online Identity Theft

The present analysis revealed some British Columbia cases where identity theft was committed using the internet. Such cases, which can affect great numbers of businesses and individuals and which can inflict large losses, are expected to occur more frequently as the sophistication of identity thieves increases.

In *R. v. Taft*,[19] Taft set up a website offering to sell false identification. A warranted search of his premises revealed over 300 unfilled orders from around the world for false identification. The search also revealed that 200 applications had been filed, providing Taft with almost $19,000. This case represents a good example of how the internet can help identity thieves. Taft had also conducted a phishing scheme involving employment advertising.

R. v. Bower[20] concerned the sentencing of an eBay fraudster. The sentencing judge noted: "[i]nterestingly enough, a great deal of effort has been put forward doing Quicklaw research to see if there are any sentencing cases reported through Quicklaw dealing with this type of internet fraud, and even after a diligent search, not one reported case could be found."

R. v. Hall[21] is another online identity theft case. The accused challenged the admissibility of evidence produced automatically by computers. The court held that evidence produced automatically by computers during the normal course of business was sufficiently reliable to be admitted. This ruling is important as most cases dealing with online identity theft will involve evidence such as web server logs and transaction logs, which are all electronically generated. However, investigators obtaining this evidence must be careful in the way it is extracted, especially when only certain portions of logs are presented.

2.1.5. Identity Consolidation – "Breeding"

Many of the cases analysed involved obtaining false identification, which was then used to create or obtain additional documents. This process is known as "identity breeding."

In 2004 Alberta case of *R. v. Bradley*,[22] the accused produced forged driver's licences and social insurance cards. In *R. v. A. (M.L.)*,[23] the accused used false identification documents to try to open a bank account. In *R. v. Cox*,[24] Cox bred new identification by legally changing his name and applying for a new SIN number. In *R. v. Thiel*,[25] Thiel used an identification document in the complainant's name to obtain another document in his own name.

In the 2004 Saskatchewan case of *R. v. Rafuse*,[26] Rafuse did not actually breed identification, but used identification that had been lost three years previously.

---

[19] *Taft*, *supra* note 15.
[20] *R. v. Bower*, [2001] B.C.J. No. 2451, 2001 BCPC 314 (Prov. Ct.) [*Bower*].
[21] *R. v. Hall*, 1998 CanLII 3955 (B.C. S.C. (T.D.)) [*Hall*].
[22] *Bradley*, *supra* note 9.
[23] *R. v. A. (M.L.)*, [2000] A.J. No. 1282, 2000 ABQB 785 (Alta. Q.B.) [*A. (M.L.)*].
[24] *R. v. Cox*, [2003] A.J. No. 152, 2003 QBPC 9, (Alta Prov. Ct. (Crim. Div.)) [*Cox*].
[25] *R. v. Thiel*, [2005] A.J. No. 698, 2005 ABPC 149 (Alta. Prov. Ct. (Crim. Div.)) [*Thiel*].
[26] *Rafuse*, *supra* note 16.

Several British Columbia cases involve "identity breeding." In *R. v. McNeil*,[27] McNeil had a driver's licence in the name of another with his picture on it. In *R. v. Jubbal*,[28] the accused used both stolen and false documents to commit fraud. In *R. v. R.W.*,[29] *W.* produced an Alberta's driver's licence in the name of another person but with *W.* 's picture on it, along with a fake SIN card as supporting documentation.

In *R. v. Boyle*,[30] Boyle acquired a birth certificate in the name of Kovic and used that certificate to get a Social Insurance Number and a B.C. identification card. He then used these documents to obtain a learner's driver's licence in the name of Kovic. In *R. v. Black*,[31] Black obtained birth certificates and Social Insurance Numbers in the names of deceased individuals. In *R. v. Taft*,[32] Taft used his photograph to apply for identification in the name of job applicants who had responded to his ad. A search of his apartment revealed he had completed 200 applications for identification documents, which he then sold over the internet.

In *R. v. Adamkewich*,[33] Adamkewich used a victim's personal information to obtain a driver's licence in the victim's name but with his own photograph. After losing the first driver's licence, Adamkewich obtained an interim driver's licence to replace the lost one.

Apparently, it remains relatively easy to breed fraudulent identification documents in Canada. Moreover, with advances in technology, creating false documents is becoming relatively inexpensive and does not require a great deal of expertise. Many of the above cases are only two to three years old, perhaps reflecting the increased use of forgery and identity breeding as a method of choice by identity thieves. More cases of this type can be expected in the future.

Most forms of "identity consolidation" or "breeding" are offences under the *Criminal Code*. The offence of forgery (s. 366) covers cases where documents are altered and cases where an application for a document includes false elements, such as the name of another individual with one's picture. Forgery is an offence even if a document was actually produced by an innocent agent, as described in the 1990 British Columbia case of *R. v. Berryman*.[34] Berryman was found guilty of forgery, even though an innocent agent at the passport office "made" the forged passport.

However, applying for a document under false pretences is not a *Criminal Code* offence as long as the document itself is not materially altered. For example, it would not be an offence to apply for a replacement SIN card in the name of another.

---

[27] *McNeil*, *supra* note 7.
[28] *Jubbal*, *supra* note 14.
[29] *R.W.*, *supra* note 18.
[30] *R. v. Boyle*, [2005] B.C.J. No. 2501, 2005 BCCA 537 [*Boyle*].
[31] *R. v. Black*, 1993 CanLII 346 (B.C. C.A.) [*Black*].
[32] *Taft*, *supra* note 15.
[33] *Adamkewich*, *supra* note 12.
[34] *R. v. Berryman*, [1990] B.C.J. No. 1689 (C.A.) [*Berryman*].

2.2. Civil Cases

Our research uncovered few civil cases involving identity theft. Most such cases concern a victim suing an identity thief for damages suffered as a result of the theft. The dearth of cases likely reflects a number of factors, including difficulty identifying the thief, or where the thief is known to the plaintiff, a desire not to sue. Moreover, litigation is expensive, time consuming, and worthwhile only where the victim has suffered significant uncompensated losses. As noted in the CIPPIC White Paper, "Approaches to Security Breach Notification," it can be difficult to recover intangible damages, such as emotional stress and loss of reputation. It may become easier to claim such intangible damages as identity theft gains increasing recognition by the courts, and especially if the *Criminal Code* is amended to include a specific offence of identity theft.

2.2.1. Conversion of Personal Information

In the 2005 Saskatchewan case of *Haug v. Saskatchewan Corrections and Public Safety*,[35] the court analysed the possibility of pleading the tort of conversion in regard to the misappropriation of personal information. At paragraph 43, the judge said:

> I concluded with considerable hesitation that information of a personal nature maintained by a government agency concerning the plaintiff could possibly constitute a chattel or item of personal property akin to software or other intangible property capable of being copyrighted and that any unauthorized use thereof might constitute the tort of conversion.

This approach is very different to that taken by the Supreme Court in *R. v Stewart*[36] where the court held that personal information was not chattel in the context of the *Criminal Code*. Will the courts adopt a more expansive approach in the future? Only time will tell if this tort can be pleaded against identity thieves.

2.2.2. Financial Institutions

In the 2005 Quebec case of *Craig v. Independent Order of Foresters*,[37] the court held that organizations that manage investments must treat their clients like a prudent financial institution would, even if the organization is not a financial institution *per se*.

In *Craig*, an identity thief forged the plaintiff's signature to withdraw funds from an account. By not authenticating the plaintiff's signature before releasing funds from his account, Foresters breached its duty to Craig. However, the identity thief's actions were found to constitute an intervening act, which severed the casual link between the breach of duty and the loss, such that Foresters was not liable.

---

[35] *Haug v. Saskatchewan Corrections and Public Safety*, [2005] S.J. No. 287, 2005 SKQB 172 [*Haug*].
[36] *Stewart*, *supra* note 3.
[37] *Craig v. Independent Order of Foresters*, [2005] Q.J. No. 1387 (Qc. C.Q. (Civ. Div.)) [*Craig*].

If other courts follow this decision, victims of identity theft who lose investments as a result of the negligent authentication procedures of a financial organization may have nowhere to turn for compensation. However, other courts have been inclined to find liability as long as the intervening act was foreseeable. In the 1985 New Brunswick case of *Williams v. Saint John (City)*, for example, the court stated at paragraph 32 that: "[i]t is enough to fix liability if one could foresee in a general way the sort of thing that happened."[38]

Older cases support the reasoning in *Williams.* In the 1935 U.K. case of *Haynes v. Harwood*, the court observed that: "[i]f what is relied upon as *novus actus interveniens* [an intervening act] is the very kind of thing which is likely to happen if the want of care which is alleged takes place, the principle embodied in the maxim is no defence ..."[39] In the 1969 case of *C. Czarnikow Ltd. v. Koufas*, the court stated that: "…the tortfeasor is liable for any damage which he can reasonably foresee may happen as a result of the breach, however unlikely it may be, unless it can be brushed aside as far fetched."[40]

2.2.3. Consumer Reporting Agencies

The 2003 Ontario case of *Haskett v. Equifax Canada Inc*.[41] established that consumer reporting agencies have a duty of care towards consumers about whom they keep credit files. It also confirmed that individuals can sue for negligence even if the *Consumer Reporting Act*[42] offers other legal remedies. This is important because these statutory remedies do not include damages.

Another Ontario case, *Clark v. Scotiabank*,[43] followed the decision in *Haskett.* It also extended the duty of care to organizations such as banks, which report information to consumer reporting agencies. The court held that such organizations must also take care not to report erroneous information to consumer reporting agencies.

2.2.4. Collection Agencies

Collection agencies can be held liable for abusive collection practices under the *Collection Agencies Act*. [44] Only the Director, as defined under the *Ministry of Consumer and Business Services Act*, [45] can bring actions against collection agencies that contravene the statute.

---

[38] *Williams v. St. John (City)* [1985] N.B.J. No. 93 (C.A.) [*Williams*].
[39] *Haynes v. Harwood*, [1935] 1 K.B. 146 at para. 156 [*Haynes*].
[40] *C. Czarnikow Ltd. v. Koufas*, [1969] 1 A.C. 350 at para. 422 [*Czarnikow*].
[41] *Haskett v. Equifax Canada Inc.*, [2003] O.J. No. 771 (Ont. C.A.) [*Haskett*].
[42] *Consumer Reporting Act*, R.S.O. 1990, c. C.33, online: <http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90c33_e.htm>.
[43] *Clark v. Scotiabank*, [2004] O.J. No. 2615 (Ont. Sup. Ct. (Civ. Div.)) [*Clark*].
[44] *Collection Agencies Act*, R.S.O. 1990, c. C.14., online: <http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90c14_e.htm>.
[45] *Ministry of Consumer and Business Services Act*, R.S.O. 1990, c. M.21, online: <http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90m21_e.htm>.

In *Anderson v. Excel Collection Services Ltd.*[46], Excel was found negligent because of the nature and frequency of its calls. However, on appeal the damage award was overturned because Anderson did not provide any evidence of psychiatric or medical problems caused by Excel's conduct. Without such evidence, the court found that damages for mental distress could not be awarded.

This high standard for awarding damages gives collection agencies considerable latitude to engage in disruptive practices towards debtors who are victims of identity theft.

2.3. Administrative Cases

The two administrative cases treated in this paper both deal with the deportation of individuals who had committed the offence of personation contrary to s. 403(a) of the *Criminal Code*. In the 2005 case of *Arinze v. Canada (Solicitor General)*,[47] the Federal Court held that committing personation offences and identity theft was sufficient to determine that was Arinze a danger to the public, and therefore deportable, pursuant to p. 115(2)(a) of the *Immigration and Refugee Protection Act*.[48] Arinze submitted that his acts of identity theft and personation were insufficient to classify him as a danger to the public as they were no more than "minor economic offences." This was rejected, upholding the Minister's decision based on relevant factors including the nature and frequency of the crimes committed and their serious effect on the Canadian public.

2.4. PIPEDA Investigations

There are few identity theft investigations under *PIPEDA*. Those briefed in this Paper illustrate the failure of many businesses to comply with the privacy protection provisions of this and related provincial legislation.[49] In its White Paper "Approaches to Security Breach Notification," CIPPIC examines investigations by the federal Privacy Commissioner and her Alberta and British Columbia counterparts into the failure of organizations to notify individuals whose personal information is at risk as a result of a security breach.

2.4.1. Lack of Proper Authentication

In the 2005 Privacy Commissioner investigation, *Former employer changed account information of Air Canada frequent flyer member*,[50] Air Canada changed a former employee's frequent flyer account information at the request of another person without verifying that person's identity. Weak authentication procedures were found to violate

---

[46] *Anderson v. Excel Collection Services Ltd.*, [2005] O.J. No. 4195 (Ont. Sup. Ct. (Civ. Div.) [*Anderson*].
[47] *Arinze v. Canada (Solicitor General)*, 2005 FC 1547 (TD) [*Arinze*].
[48] *Immigration and Refugee Protection Act*, R.S.C. 2001, c. 27, online: < http://laws.justice.gc.ca/en/ShowTdm/cs/I-2.5>.
[49] See CIPPIC report, "Compliance with Canadian Data Protection Laws" (Ottawa: CIPPIC, 2006), online: <www.cippic.ca>.
[50] *PIPEDA* Case Summary #292, *Former employer changed account information of Air Canada frequent flyer member*, 2005 CanLII 15494 (P.C.C.).

Principle 4.7 of *PIPEDA*, which requires organizations to employ "security safeguards appropriate to the sensitivity of the information." The failure of an organization to follow proper authentication procedures can contribute to identity theft. In this case, the caller could possibly have obtained all the personal information held in the complainant's account and used it to engage in identity fraud.

2.4.2. Lack of Adequate Computer Security

In the 2003 Privacy Commissioner investigation, *Bank leaves computer logged on in public area; customer obtains sensitive personal account information without password*,[51] a publicly available computer in the bank allowed the complainant to obtain his own sensitive personal account information without a password. This computer could also have provided access to other clients' highly sensitive personal financial information. Clearly, an identity thief could have acquired this information. The bank was found to have contravened Principle 4.7 of *PIPEDA*. This investigation demonstrates the risks associated with holding personal information in computerized records. Under *PIPEDA*, computers and network resources must be adequately secured to reduce the risk of unauthorized access to personal information.

2.4.3. Insider Abuse

The potential for insider abuse is a consideration for any organization that collects personal information. As discussed in the first Working Paper in this series, "Identity Theft: Introduction and Background," a significant proportion of identity theft occurs as a result of unauthorized activity by employees, who gain access to customers' personal information. To limit the risk posed by insider abuse, organizations need to carefully screen job applicants and ensure proper supervision of employees.

In the 2003 Privacy Commissioner investigation, *Bank employee uses customer's information to commit fraud)*,[52] a bank employee used a customer's personal information to commit fraud. The Commissioner noted that no security system, however sophisticated and effective, may ever completely eliminate the possibility insider abuse.

2.4.4. Difficulty of Withdrawing Consent

The 2003 Privacy Commissioner investigation, *Customer withdraws consent but continues to receive promotional material*,[53] provides a good example of how difficult it can be to withdraw consent, especially for pre-approved credit card or loan offers. Financial institutions market these products aggressively and widely, even though they can pose a significant risk of identity theft if the offers include personal information.

---

[51] *PIPEDA* Case Summary #177, *Bank leaves computer logged on in public area; customer obtains sensitive personal account information without password*, 2003 CanLII 38271 (P.C.C.).
[52] *PIPEDA* Case Summary #121, *Bank employee uses customer's information to commit fraud*, 2003 CanLII 33645 (P.C.C.).
[53] *PIPEDA* Case Summary #116, *Customer withdraws consent but continues to receive promotional materials*, 2003 CanLII 42249 (P.C.C.).

The complainant had written to her bank twice, saying that she wanted to opt out of receiving promotional material. Nevertheless, seven months later, she received another solicitation for a credit card from the same bank. This investigation illustrates the problem of using an "opt-out" regime instead of an "opt-in" one. It has become the norm for businesses to assume consent for future solicitations unless the consumer opts-out of such situations. Opting-out may require a level of effort and awareness that most consumers do not have.

3. COMPARATIVE ANALYSIS OF UNITED STATES AND CANADIAN CASELAW

3.1. Introduction

Given the enormous volume of U.S. jurisprudence available at both federal and state levels, the U.S. caselaw in this Working Paper is limited to the 11 Circuit courts and the District of Columbia Circuit court. The analysis begins with a discussion of Federal Trade Commission enforcement actions. Selected criminal, civil and administrative cases are then discussed.

3.2. Federal Trade Commission (FTC)

The majority of FTC investigations result in a settlement, without going to court. We review three that were litigated. All concern software manufacturers distributing some form of malware, such as spyware applications. None deals directly with identity theft. However, malicious software is often implicated in identity theft. It may exploit vulnerabilities in operating systems such as Windows, so as to permit an identity thief to control another computer remotely and secretly. Such programs are readily available online and require little technical knowledge to operate.

3.3. Criminal Cases

Canadian and U.S. criminal cases involving identity thieves have some common elements. The first is the high percentage of cases in which the defendant pleads guilty. This suggests that law enforcement agencies press charges only when they have a very strong case. Also, a high proportion of the reported cases involve appeals of a sentence or of a restitution order, perhaps reflecting the type or level of cases that tend to be reported.

As in Canada, identity consolidation and breeding of forged identification documents are prevalent in the United States. Three U.S. cases, *United States v. Oates*,[54] *United States v. Montejo*[55] and *United States v. Melendrez*,[56] deal with the issue of using one's name, or a fictitious name, in conjunction with another person's identification numbers. In *Montejo*,

[54] *United States v. Oates*, No. 04-4018 (8th Cir., 3 Nov 2005) [*Oates*].
[55] *United States v. Montejo*, No. 05-4143 (4th Cir., 29 Mar 2006) [*Montejo*].
[56] *United States v. Melendrez*, No. 03-30221 (9th Cir., 9 Nov 2004) [*Melendrez*].

the numbers were fabricated but were nonetheless assigned. In each of these cases, it was found that associating a Social Security Number with a wrong name cannot be prosecuted for conviction under 18 U.S.C. § 1028A(a)(1) because the criminal had not severed the SSNs from the names of their true owners.

Identity theft resulting from insider abuse is also a major problem in the United States. In the cases selected for review, insiders at the United States Postal Service, SBC Communications, Fleet Bank and the United States Navy used their positions to commit identity theft. One would expect these institutions to have strong protections to prevent this type of activity. If insider abuse can occur within such large institutions, it can presumably also happen in smaller ones.

Canadian and U.S. criminal cases differ in one important respect. Sentences for identity theft crimes are harsher in the U.S. and restitution is imposed more often than in Canada. Sentencing guidelines appear to be the main reason why sentences are higher in the U.S. These guidelines use a point-based system of enhancements and mitigating factors which leaves less discretion with the court. Restitution is imposed more often in the U.S. as a result of the *Mandatory Victim Restitution Act*, which requires a court to order a defendant to make restitution to the victim of an offence involving fraud or deceit.[57]

3.4. Civil Cases

Three of the four U.S. civil cases selected for review deal with the aftermath of identity theft. As our review is limited to cases at the appellate level, it is not clear whether U.S. victims tend to take legal action more often than do their Canadian counterparts. However, the literature suggests that, proportionally, there is a much higher degree of identity theft-related litigation in the U.S. than in Canada.

The 2001 case, *TRW Inc. v. Andrews*,[58] established that when a consumer report agency wrongfully discloses information from one's credit record, the limitation period for bringing an action begins to run when the credit record is disclosed rather than when the individual discovers the harm that resulted from the disclosure. The court reasoned that since some of the liability arose when the disclosure occurred, the limitation period began to run at that point.

Sherman v. United States Department of the Army[59] demonstrates the risk of identity theft posed by the release of records requested under the *Freedom of Information Act*.[60] The requested records were computerized and contained information on awards given by the Army. These records contained the SSNs of the soldiers who had received the awards. The Army refused to disclose the records unless Sherman paid a prohibitive amount to

---

[57] *Mandatory Victim Restitution Act*, 18 U.S.C. § 3663A (1996), online: <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00003663---A000-.html>.
[58] *TRW Inc. v. Andrews*, No. 00-1045 (Sup. Ct., 13 Nov 2001) [*TRW*].
[59] *Sherman v. United States Department of the Army*, No. 00-20401 (5th Cir., 7 Mar 2001) [*Sherman*].
[60] *Freedom of Information Act*, 5 U.S.C. § 552, As Amended by Public Law No 104-231, 110 Stat.3048.

get the SSNs redacted. The court found that an individual maintained a substantial informational privacy right to limit the disclosure of his or her SSN and reduce the risk of identity theft.

In *Hallock, Ferncliff Assoc., Inc. v. Bonner*,[61] a search warrant was executed against a victim of identity theft. Hallock's computer equipment was seized and when it was returned, he discovered that the equipment was damaged and totally unusable. Hallock was unsuccessful in his suit against the government for damages. This case illustrates the difficulty of obtaining damages for the consequences of identity theft, even when they are easily quantifiable.

3.5. Administrative Cases

As in Canada, issues around identity theft play a role in U.S. administrative decisions, particularly in immigration matters.

In the 2005 case of *Murtuza v. Gonzales (Attorney General)*,[62] Murtuza argued before the Board of Immigration Appeals that he had not received notice of a hearing because he had been the victim of identity theft. The court was not convinced, concluding that no one else would want to use Murtaza's identity on such an application. The court found that even if the application were successful, the only one who would benefit would be Murtaza.

In *Sokolov v. Gonzales (Attorney General)*,[63] Sokolov was denied asylum. The immigration judge denied his application because of his implausible explanation of a recent conviction for financial identity theft. The Court of Appeal dismissed the petition for review for want of jurisdiction.

The 1999 case, *Ferm v. United States Trustee*,[64] concerned the risk of identity theft stemming from the presence of personal information in court records. Ferm helped individuals file applications with the Bankruptcy Court. When he assisted someone, he was required to provide his SSN, which then ended up in the public record. Ferm requested an exemption from this requirement based on his fear of identity theft. The court ruled that information privacy "is not absolute; rather it is a conditional right which may be infringed upon a showing of proper governmental interest." The court also held that the dire consequences of identity theft must be considered relative to the low probability of its occurrence. It concluded the government had a sufficiently important legislative purpose, mainly the Bankruptcy Code's "public access" provision, to require disclosure of Ferm's SSN in the court records.

---

[61] *Hallock, Ferncliff Assoc., Inc., v. Bonner*, No. 03-6221 (2nd Cir., 22 Oct 2004) [*Hallock*].
[62] *Murtuza v. Gonzales (Attorney General)*, No. 04-2718 (7th Cir., 28 Oct 2005).
[63] *Sokolov v. Gonzales (Attorney General)*, No. 04-3218 (7th Cir., 24 Mar 2006).
[64] *Ferm v. United States Trustee*, No. 97-16653 (9th Cir., 7 Oct 1999).

4. RELATIONSHIP BETWEEN IDENTITY THEFT TECHNIQUES AND CASES

The following tables list various identity theft techniques and cross reference them with the Canadian and U.S. cases reviewed in this Paper. They show that a wide range of techniques have been used in the various cases, and that insider theft is a more common source of identity theft in both countries. Forgery and opening new accounts using personal information wrongly acquired are also common techniques. No U.S. cases dealt with the physical theft of personal information, though this is certainly a problem in the U.S. as it is in Canada.

4.1. Acquisition techniques

Technique	Canadian Cases	U.S. Cases
Purchasing Stolen Personal Information	– *R. v. Naqvi*	
Physical Theft of Personal Information	– *R. v. Thiel* – *R. v. Jubbal* – *R. v. Rafuse* – *R. v. Weir* – *R. v. Adamkewich*	
Identity Consolidation – "Breeding"	– *R. v. Black* – *R. v. Taft* – *R. v. Adamkewich*	– *United States v. McNeil* – *United States v. Melendrez* – *United States v. Sample*
Change of Address	– *Bongeli v. Citibank Canada*	
Skimming (Magnetic Strip Duplication)	– *R. v. Naqvi* – *R. v. Mayer* – *R. v. Rodrigue*	
Mail Theft	– *R. v. Bradley* – *R. v. McNeil* – *R. v. Tonks*	– *United States v. Yagar* – *United States v. Peterson* – *United States v. Grant*
Dumpster Diving		
Phishing	– *R. v. Taft* (Offline)	
Pharming		
DNS Cache Poisoning		
Spyware, Malware and Viruses		
Internet Searches and Google Hacking		

Exploiting Computer Systems Security Vulnerabilities (Cracking)	– *R. v. Lavoie*	
Wardriving (Drive-By Identity Theft)		
Insider Abuse	– *R.. v. P.T.* – *R.. v. Berryman* – *R.. v. Thomas* – *R.. v. Adamkewich* – *R. v. Hall* – *Craig c. Independent Order of Foresters* – *Bongeli v. Citibank Canada* – *Bank employee uses customer's information to commit fraud*	– *United States v. Bush* – *United States v. Havens* – *United States v. Newsome* – *United States v. Vieke* – *United States v. Peyton* – *United States v. Sample* – *United States v. Green* – *TRW Inc. v. Andrews* – *United States v. Rand* – *Westra v. Credit Control of Pinellas*
Government Kiosks and Records		– *United States v. Klopf*
Acquiring Used Computer Equipment		
Mortgage Fraud		
Obtaining Credit Reports on Victims		– *United States v. Bush*
Reshipping		
Bogus Employment Schemes	– *R. v. Taft*	
Social Engineering		
Tombstone Theft	– *R. v. Boyle* – *R. v. Reith* – *R. v. Black*	– *United States v. Bush*
Contests and Surveys		
Legal Name Change and SIN Fraud	– *R. v. Cox* – *R. v. Thomas*	

4.2. Unlawful uses

Technique	**Canadian Cases**	**U.S. Cases**
Selling Personally	– *R. v. Naqvi*	

Identifiable Information	– *R. v. Lavoie* – *R. v. Taft*	
Creating Forgeries	– *R. v. Bradley* – *R. v. Naqvi* – *R. v. Jubbal* – *R. v. R.W.* – *R. v. Boyle* – *R. v. Harris* – *R. v. Weir* – *R. v. Mayer* – *R. v. Berryman* – *R. v. Taft* – *R. v. Rodrigue*	– *United States v. Mejìa-Barba* – *United States v. Bush* – *United States v. Newsome* – *United States v. Banks* – *United States v. McNeil* – *United States v. Montejo* – *United States v. Peterson* – *United States v. Klopf* – *United States v. Grant*
Taking Over Existing Accounts	– *R. v. Bradley* – *R. v. Thiel* – *R. v. Naqvi* – *R. v. Harris* – *R. v. A. (M.L.)* – *R. v. Weir* – *R. v. Tonks* – *R. v. Rodrigue* – *Craig c. Independent Order of Foresters* – *Bank employee uses customer's information to commit fraud*	– *United States v. Newsome*
Opening New Accounts	– *R. v. Olotu* – *R. v. Jubbal* – *R. v. R.W.* – *R. v. Richard* – *R. v. A. (M.L.)* – *R. v. P.T.* – *R. v. Thomas* – *R. v. Taft* – *R. v. Adamkewich* – *R. v. Hall*	– *United States v. Bush* – *United States v. Collier* – *United States v. Havens* – *United States v. Banks* – *United States v. Vieke* – *United States v. McNeil* – *United States v. Peyton* – *United States v. Klopf* – *United States v. Sample* – *United States v. Stovall* – *United States v. Williams* – *United States v. Karro* – *United States v. Oates* – *United States v. Green* – *TRW Inc. v. Andrews* – *United States v. Rand* – *Westra v. Credit Control of Pinellas,*

Ordering Goods Online Using a Drop-Site		
Secure Employment		– *United States v. Mejìa-Barba* – United States v. Montejo
Obtaining a Passport	– *R. v. Berryman*	
Obtaining government benefits	– *R. v. Reith* – *R. V. Cox* – *R. v. Black* – *R. v. Thomas*	– *United States v. Collier* – *United States v. Williams*
Obtaining Health Services		– *United States v. Sample*
Service Account Hijacking		
Making Long Distance Calls		
Concealment	– *R. v. Bradley* – *R. v. Jubbal* – *R. v. Rafuse* – *R. v. Adamkewich*	– *United States v. Mejìa-Barba* – *United States v. Banks*
Taking Over Insurance Policies		
Submitting Fraudulent Tax Returns		– *United States v. McNeil*
Filing for Bankruptcy		

5. CONCLUSIONS

This review of Canadian caselaw reveals that most identity theft cases concern credit and debit card fraud. Courts are starting to recognize that identity theft is an emerging social and policy issue, but their hands are tied by the legal framework within which they operate.

There are relatively fewer reported identity theft cases in Canada than in the U.S. This is no doubt a reflection of the fact that the U.S. has many identity theft laws at both the federal and state levels and a significantly larger population. In both countries, sentences given to convicted identity thieves tend to be light compared to other economic crimes. Thus, the deterrent effect of criminal convictions is questionable. Civil cases are few in number, perhaps because of the high cost of litigation and the difficulty of identifying identity thieves.

This could change if the *Criminal Code* were amended to include specific identity theft offences, if other statutes were amended to include civil causes of action for security breaches and other wrongs associated with identity theft, and if the common law develops in ways that provide individual victims with more incentive and opportunity to pursue civil redress in the courts.

APPENDIX A - CANADIAN CASE BRIEFS

Criminal Cases

R. v. Stewart, [1988] 1 S.C.R. 963

Procedural Background

Stewart was charged with counselling to commit Fraud, Theft and Mischief. He was acquitted in the Ontario High Court of Justice (1982), 38 O.R. (2d) 84. The Crown successfully appealed the acquittal (1983), 42 O.R. (2d) 225. Stewart appealed to the Supreme Court.

Facts

The appellant, Wayne John Stewart, a self-employed consultant, was hired by somebody he assumed to be acting for the union to obtain the names and addresses of the employees. He offered a security guard at the hotel a fee to obtain this information. The appellant did not want a physical and tangible object such as list of names printed. All that the appellant requested was the "information".

Legal Issue(s)

1. Does obtaining without authorization the confidential information, by copying the document or memorizing its content, constitute theft under s. 283(1) of the *Criminal Code*?
2. Would the appropriation of the information have amounted to fraud contrary to s. 338(1) of the *Criminal Code*?

Holding

The appeal was allowed and the acquittals restored. The appellant did not commit either theft or fraud.

Statement of Rule

Confidential information is not property for the purposes of s. 283 of the *Code*. The appropriation of the confidential information did not constitute fraud since the hotel would not have been defrauded of money or of any economic advantage.

Reasoning

Theft

The wording of s. 283 restricts the meaning of "anything" in two ways. First, whether tangible or intangible, "anything" must be of a nature such that it can be the subject of a proprietary right. Second, the property must be capable of being taken or converted in a manner that results in the deprivation of the victim.

The Court of Appeal did not properly consider the *actus reus* required for committing the offence, that is a taking or a conversion. One cannot be deprived of confidentiality, because one cannot own confidentiality. One enjoys it.

Fraud

It is conceded that there was no intention on the part of the hotel to deal in a commercial way with the confidential information. Although the appellant would have received some money for the information, the court could not see how the hotel suffered the requisite dishonest deprivation.

The proof of a risk of prejudice to the economic interests of the victim is sufficient evidence of the deprivation; actual economic loss is not essential.

Policy
The criminalization of certain types of conduct should not be done lightly. If the unauthorized appropriation of confidential information were to become a criminal offence, there would be far reaching consequences that the courts are not in a position to contemplate.

R. v. Hamilton, [2005] 2 S.C.R. 432

Procedural Background
Mr. Hamilton was charged under s. 464(a) in four separate counts, with counselling the commission of indictable offences that were not in fact committed.

The trial judge was not satisfied that Mr. Hamilton had acted with the requisite *mens rea*, or culpable intent, and she therefore acquitted him on all four counts. The Court of Appeal for Alberta dismissed the Crown's appeal. The Crown appealed to the Supreme Court on the issue of *mens rea*.

Facts
Luther Hamilton offered for sale through the internet access to a "credit card number generator" — in terms that extolled its use for fraudulent purposes. As part of the same package of "Top Secret" files, he also offered for sale bomb "recipes" and information on how to commit burglaries.

Legal Issue(s)
1. Did Hamilton have the necessary *mens rea*?

Holding
The appeal was allowed in part.

Decision
The appeal was allowed by the count for counselling fraud and a new trial was ordered on that count. The appeal in relation to the three remaining counts was dismissed.

Reasoning
The *mens rea* consists in nothing less than an accompanying *intent* or *conscious disregard of the substantial and unjustified risk inherent in the counselling*: that is, it must be shown that the accused either intended that the offence counselled be committed, or knowingly counselled the commission of the offence while aware of the unjustified risk that the offence counselled was in fact likely to be committed as a result of the accused's conduct.

The trial judge acquitted Mr. Hamilton on the charge of counselling fraud because she had "a doubt that Mr. Hamilton had subjective intent to counsel fraud".

> His motivation was monetary, and he sought to pique the curiosity of readers who might acquire the information in the same way that he was initially attracted to the

> information. Further, he struck me as utterly unsophisticated and naïve to the point that he cannot be said to have been wilfully blind or reckless.

The trial judge acquitted Mr. Hamilton on this count because his motivation was mercenary as opposed to malevolent; this was an error of law.

In most criminal trials, the mental element, the *mens rea* with which the court is concerned, relates to "intent", i.e. the exercise of a free will to use particular means to produce a particular result, rather than with "motive", i.e. that which precedes and induces the exercise of the will. The mental element of a crime ordinarily involves no reference to motive.

R. v. Bradley, [2004] A.J. No. 1278, 2004 ABCA 362 (Alta. C.A.)

Procedural Background
Bradley entered guilty pleas to 15 counts and appealed his sentence of four and half years.

Facts
Bradley stole credit cards from the postal service in Toronto before they reached the legitimate card holder. Bradley used these cards to make purchases. While making some of the purchases, he was recorded on security video tapes. In support of his use of the cards, he produced forged driver's licences and Social Insurance cards. At the time of his arrest, Bradley gave a fake name and provided forged documentation to the police.

Legal Issue(s)
1. Did the sentencing judge err in principle when she placed emphasis on Bradley's involvement with organized crime?
2. If the sentencing judge erred, what is the appropriate sentence?

Holding
The appeal is dismissed.

Decision
The evidence did not support the involvement to organized crime; Bradley only admitted the facts necessary to support the charges. The sentence imposed was fit and proper.

Reasoning
The court recognized the serious implications of identity theft for the victims defrauded but also for the victims being impersonated. The court found the fraud to be substantial, organized and sophisticated. The court also considered the appellant's related record and his continued involvement in crime. Considering these factors, the court found the sentence to be appropriate.

R. v. A. (M.L.), [2000] A.J. No. 1282, 2000 ABQB 785 (Alta. Q.B.)

Procedural Background
M.L.A. was charged of various offences including unlawful use of a credit card that he knew was obtained by the commission of an offence (s. 342(1)(c)), uttering a forged document (2. 368(1)(a)), personation with intent (s. 403(a)), fraud (s. 380(1)(b)), assault with a weapon (s.

267(a)), assaulting a police officer (s. 270(1)(a)), assaulting a police officer with intent to resist arrest (s. 270(1)(b)), two counts of possession of a credit card that was obtained by the commission of an offence (s. 342(1)(c)), and possession of property obtained by crime (s. 355(b)). Bail was originally denied in Provincial Court. This was an application by M.L.A. for judicial interim release.

Facts

On or about May 1, 2000 M.L.A. used a credit card he knew was obtained by the commission of an offence. On August 31, 2000, M.L.A. attempted to open a bank account using a false identity. The bank teller was suspicious and alerted police. The police tried to arrest M.L.A. while he was trying to enter a vehicle. The vehicle sped away while M.L.A. was partially inside and an officer was holding on to M.L.A. Both M.L.A. and the driver were able to get away. The bank was not financially harmed. On October 3 and 5, 2000 M.L.A. tried to change a counterfeit bill at a pub. The accused was on probation, as part of a suspended sentence, for a guilty plea entered for charges of unlawful use of a credit card at the time of the present offences.

Legal Issue(s)

1. Is continued detention of M.L.A. justified?

Holding

The application for interim release was dismissed.

Decision

The judge concluded that it would be inappropriate to grant judicial interim release for the accused.

Statement of Rule

An important consideration for ordering the continued detention based on p. 510(10)(b), is whether the accused is already on bail or probation at the time of the offence.

Reasoning

There are three grounds for which continued detention can be ordered. The court found that the Crown's case on the second ground is the strongest as the accused has failed to comply with a probation order and tried to flee from apprehension by police. On the same basis, ground one is also met.

The court then looked at ground three and indicated that the protection of the public encompasses a broader goal than merely protection from serious bodily harm. It also notes that areas of public concern are not limited to criminal acts where there is a defined victim and that in all the circumstances of these offences, the public at large suffers greatly from the perpetration of fraud and use of counterfeit currency and documents. The judge also considers that the strength of the prosecution's case is noteworthy when considering the perception of the justice system in the eyes of the public. Based on these observations, the tertiary ground is also met.

R. v. Lukian [2003] A.J. No. 1495, 2003 ABQB 989 (Alta. Q.B.)

Procedural Background

L. had pled guilty to one count of conspiracy to commit fraud and seven counts of Fraud. This case concerned his sentencing.

Facts

L. obtained several credit cards numbers from the Internet. The credit card accounts belonged to various individuals in the United States. He used these cards to buy merchandise, including computers, digital cameras, and high end sunglasses. The total value of the merchandise was $15,016.68 USD.

The merchandise was shipped to Sanders, a friend of L., in North Dakota. Sanders was instructed to re-package the items bought and re-ship them to Berg, another accomplice, in Edmonton. Sanders was also instructed to declare the items shipped as having minimal value ($50 to $70). The defendant admitted to Sanders that he was using credit card numbers he hacked off the Internet to make the purchases.

Searches by the R.C.M.P. revealed several emails detailing his attempts to get new credit cards. They also found lists of credit card numbers, with their credit limits, balances, expiry dates and the names and addresses of the credit card holders. Some purchases were made using an email address that belonged to the defendant.

Legal Issue(s)

What is the appropriate sentence?

Decision

L. was sentenced to a conditional sentence of 18 months to be served in the community, followed by 12 months of probation. He was ordered to complete 240 hours of community service work. A restitution order in the amount of $5000.00 was made. The defendant was barred from using the Internet and using computer equipment at his residence. A Victim Fine Surcharge of $800.00 was also imposed.

Reasoning

The judge considered the fact that L.'s guilty plea saved time and money to the justice system. The judge also considered that L. had ground to gain when it came to acceptance of responsibility. The sentencing judge concluded that L. was the leader of the scheme. The judge also found that his was not a situation involving a breach of trust or taking advantage of vulnerable victims. It was not a case of organized crime.

The judge considered that the defendant gained a little bit of party time, some money, and some computer equipment while losing most of his education. He had probably ended his ability to be qualified in positions of trust, and his objective of being realtor probably had no great prospects. The judge found that he paid a tremendous price for a fairly trivial amount of gain and only a very passing sense of success.

The judge then considered the principles of denunciation and of general deterrence. The judge noted that failure to deter can also demoralize the law-abiding. The judge also noted that deterrence of people across the world, who misuse the internet, is beyond the scope of his authority. The judge was persuaded that a non-lenient conditional sentence order was not inappropriate for this particular case.

R. v. Cox, [2003] A.J. No. 152, 2003 ABPC 9 (Alta. Prov. Ct. (Crim. Div.))

Procedural Background
Cox pleaded guilty to unlawfully receiving employment insurance benefits totalling $5,788.00. This is his sentencing.

Facts
Cox was 42 years of age and was a resident of Calgary. He resided in a common-law relationship and had two children. He was gainfully employed and earned approximately $20,000 annually.

Cox, using SIN No. 628 327 413 worked for Allied Tool Ltd. between Nov. 3, 1997 and Feb. 9, 1999. Shortly after, he applied for employment insurance benefits. He collected benefits between February and October 1999. At the same time, he was working for RYOCI Canada Inc. under the name Taylor.

On July 14, he applied for and obtained SIN No. 656 627 775 and provided that number to RYOCI . After being laid off, he collected further EI benefits between September 9 and 22, 2001. On August 15, 2001 using SIN No. 628 327 413, he commenced employment with the Cowboys Night Club and worked there for a period, including between September 9 and 22, 2001. Between his SIN applications, Cox made a formal application to change his name from Robert Gordon Cox to Robert Gordon Taylor.

Legal Issue(s)
1. What is a fit sentence?

Decision
The judge sentenced Cox to a global term of imprisonment of 30 days to be served on weekends. Cox is also on probation during the week and for a period of two years after his release. In the Probation Order, the judge ordered restitution, in the amount of $5,788.00 payable in $250 monthly instalments, 30 hours of community service and a charitable donation of $300. The judge also made a stand alone Restitution Order in the amount of $5,788.00 that may be obviated with the compliance with the Probation Order.

Reasoning
The judge considered the following aggravating factors, namely that: 1) The accused had a criminal record; 2) although the offences were welfare offences, they all involved some degree of "moral blameworthiness"; 3) The offences were planned and deliberate; 4) The offences involved three distinct frauds being committed using separate identities; 5) The accused was discovered in the commission of the offences; 6) The total benefits received were neither small or insignificant; 7) There had been no restitution; 8) The offences involved "greed" and "gambling problem" as opposed to "need"; and 9) the accused does not have difficulty finding new employment.

As mitigating circumstances the judge considered that: 1) The accused had tendered a guilty plea, although not a timely one; 2) Some of his prior convictions were old and there were gaps in his record; 3) the accused was the sole supporter of his wife and two children; and 4) the accused was gainfully employed at the time of sentencing.

R. v. Weir, [2000] A.J. No. 527, 2000 ABPC 62 (Alta. Prov. Ct. (Crim. Div.))

Procedural Background
Weir admitted to breaching the terms of a conditional order. He pleaded guilty to committing several offences both before and after the imposition of the conditional sentence. This is his sentencing.

Facts
Mr. Weir pleaded guilty and obtained a conditional sentence for a number of offences including, amongst others, theft under $5,000.00 (s. 334(b)); two counts of failure to appear (s. 145(5)); possession of stolen property under $5,000.00 (s. 355(b)); one count of possession of a credit card obtained by the commission of an offence in Canada (342(1)(c)); personation with intent (s. 403(a)); uttering a forged document (s. 368(1)(a)); two counts of break and enter and theft (s. 348(1)(b); theft over $5,000.00 (s. 334(a)); possession of stolen property over $5,000.00 (s. 355(a)). Mr. Weir was sentenced to a conditional sentence of two years less one day plus 18 months probation.

While bound by the conditional sentence order Mr. Weir committed the following offences, amongst others: failure to attend court (s. 145(5)), failure to attend court (s. 145(2)(a)); failure to attend court (s. 145(2)); theft of a motor vehicle exceeding $5,000.00 (s. 344(a)).

Mr. Weir pleaded guilty to the following offences prior to the commencement of the conditional sentence order: two counts of possession of stolen property under $5,000.00. At the time of hearing, Mr. Weir had served 6 weeks of pre-trial custody, had entered early guilty pleas and had 17 months left on his conditional sentence. The breach of the conditional sentence was in failing to reside where directed and in ignoring his curfew.

Legal Issue(s)
1. What actions should be taken in regards to the breach of the conditional sentence? Should the conditional sentence be suspended and the offender directed to serve the unexpired portion?
2. What are the appropriate sentences for the new offences?

Decision
Considering the totality principle and the circumstances of Mr. Weir, the judge suspended the conditional sentence and directed the accused to serve the 14 months remaining in the conditional sentence to be followed by the same probation as imposed after the conditional sentence. As for the new offences, the judge imposed 6 months incarceration consecutive to the 14 months.

Statement of Rule
A presumption exists that an offender must serve the remainder of a conditional sentence in jail when he breaches a conditional sentence order

Reasoning
The Crown submitted that the accused should serve the remainder of the conditional sentence and be sentenced to further consecutive time for the new offences. Defence counsel submitted that sending Mr. Weir to jail for the remainder of the time would amount to more time than if he had been sent to jail initially. Defence counsel submitted that this was contrary to the totality principle.

The court then analysed *R. v. Proulx*, 2000 S.C.C. 5 in which a presumption is established that an offender serve the remainder of a conditional sentence in jail when he breaches a conditional sentence order. This presumption helps to distinguish conditional sentences from probation by making the consequences of a breach of condition more severe.

The judge then analyzed this presumption and found that if the length of a sentence actually served in jail may be too short if it were a sentence served in the community, and will thereby fail the proportionality test, then it follows that the length of conditional sentence may be too long if it were a sentence served within a jail, and it will again fail the proportionality test. The judge concluded that whether such a straight conversion, from conditional sentence to imprisonment, is appropriate will depend on the circumstances of the offender, the offence, and the amount of time left to be served.

The judge also considered that the requirement to serve the remainder in jail can be seen as the price to pay for breaching conditions under which an offender is placed. According to the court, the difficulty with this argument is that it results in imposing a separate punishment for the breach, and thereby treats the breach as though it were a separate offence. Breach of probation is a separate criminal offence but breach of a conditional sentence is not.

R. v. Thiel, [2005] A.J. No. 698, 2005 ABPC 149 (Alta. Prov. Ct. (Crim. Div.))

Procedural Background

Mr. Thiel pleaded guilty to 8 *Criminal Code* offences including, personation (s. 403(a)), possession of stolen property (s. 355(b)), uttering (s. 368(1)(a) and fraud under $5,000 (s. 380(1)(b)). This was Thiel's sentencing.

Facts

On March 7, 2005 Mr. Thiel used an identification document in the complainant's name to obtain another document in his name. Armed with these documents and the complainant's social insurance card, the accused impersonated the complainant to carry out a series of frauds by which he obtained $5,600.00. The documents used included an Edmonton Police Service witness statement filed by the complainant relative to his stolen property.

Mr. Thiel already had 131 criminal convictions, of which 90 are for similar offences. The last sentence handed down to Mr. Thiel was to be served in the community, under the terms of a Conditional Sentence Order. Mr. Thiel submitted a letter of commendation and offered to make restitution in the event he was given a Conditional Sentence.

Legal Issue(s)

1. What is the appropriate sentence?

Decision

The judge sentenced Mr. Thiel to four and a half years and made two compensation Orders to direct the accused to give restitution to the financial institution defrauded ($5600) and to the victim ($1300) who had been personated.

Reasoning
The accused's criminal record has 13 entries demonstrating his inability to abide by court orders. This was coupled with the fact that the offences were committed while he was on Probation and out on bail.

The court also considered four aggravating factors: 1) The nature of the offences in Mr. Thiel's criminal record and their unremittingness; 2) The fact that no restitution was made; 3) The fact that the offences were committed while the accused was on Probation and out on bail; and 4) The commission of these offences by means of de facto 'identity theft' of the complainant.

The judge found that committing identity theft in order to aid in the commission of other offences heightens the seriousness of the offence.

R. v. Naqvi, [2005] A.J. No. 1593, 2005 ABPC 339 (Alta. Prov. Ct. (Crim. Div.))

Procedural Background
Naqvi pleaded guilty to skimming debit and credit cards to sell the card information contrary to s. 342.(3) of the *Criminal Code*. This case concerned Naqvi's sentencing.

Facts
Mr. Naqvi was given a skimming device by a high school acquaintance. In August 2004, over a period of 12 days, Naqvi skimmed 117 debit or credit cards. In December 2004, over a short period of time, he skimmed another 60 cards.

Naqvi sold the information to the high school acquaintance for $100.00 each realizing a profit of $17,700.00. Mr. Navqi took no part in the actual counterfeiting or use of counterfeited cards. The total loss incurred by the financial institutions was $117,188.00. Following apprehension, Naqvi cooperated with police.

Legal Issue(s)
1. What is the appropriate sentence?

Decision
Naqvi was sentenced to 18 months of imprisonment and ordered to pay restitution in the amount of $17,700.00 to the banks according to their proportion of the losses.

Reasoning
The sentencing judge agreed with the Crown that general deterrence and public denunciation in these circumstances are paramount considerations. The judge took into consideration the following aggravating factors: the accused was in a position of trust; the crime was sophisticated; it was a group enterprise; the commission of the crime put the reputation of businesses at risk; it was committed again and again over a period of 5 months at different locations; the offence of skimming is prevalent and growing; the victims are highly vulnerable; the crime is difficult to prevent, detect and investigate.

As far as mitigating factors go, the judge considered: the youth of the accused; his cooperation with police following his arrest; his early guilty plea; his share of the proceeds compared to others.

Mr. Navqi's counsel argued that he was only a minor participant. However, the judge said that was akin to describing a bank robber as a low level participant, and the driver in the gateway vehicle as the primary offender. The judge found that without the information gathered and distributed by Mr. Navqi the criminal enterprise would not have been possible. The judge was not satisfied that a conditional sentence would satisfy sentencing principles.

Policy

The judge concluded by explaining that the immediate victims are the seven financial institutions whose customers have been defrauded. The longer-term victims are those who use these institutions services and are subjected to interest rate increases.

R. v. Mayer, [2006] A.J. No. 324, 2006 ABPC 30 (Alta. Prov. Ct. (Crim. Div.))

Procedural Background

Mayer pled guilty to 28 charges of using forged debit cards and debit card data, and 1 charge of breach of recognizance.

Facts

Mr. Mayer was involved in a large debit card skimming, counterfeiting and fraud ring in Calgary from January 1, 2005 to July 21, 2005. Mayer's conduct resulted in a total loss of $45,703.00.

Mayer's fraud involved five different financial institutions, six businesses where the cards were skimmed and 34 different card holders. Some members of the ring travelled to Calgary and obtained employment for the sole purpose of skimming cards. At least 20 individuals were involved in making withdrawals from the accounts or purchasing money orders using the cards.

Mr. Mayer's offences were committed in June. At the time of the offences, Mr. Mayer was on release on charges relating to debit card fraud (s. 380(1)(b)) committed in Laval, Quebec. Mr. Mayer left Alberta without permission and went back to Montreal. As a result, he failed to report on August 31. He also appears on bank surveillance video, dated September 2, while he's committing a fraudulent transaction. At the time of that transaction, he was out on bail.

Legal Issue(s)

1. What is the appropriate sentence?

Decision

After credit for the pre-trial custody, the judge sentence Mr. Mayor to twelve months imprisonment concurrent to any other sentence.

Reasoning

The judge found that the evidence supported the conclusion that a Conditional Sentence Order would endanger the community. The accused did not have a criminal record but he plead guilty to a breach of his recognizance. The accused was also on judicial interim release when he committed this set of offences. The court concluded that the accused was not inclined to follow Court orders and that serving his sentence in the community would be a risk and would endanger the community.

The court rejected the argument of duress in the circumstances of this case. A gambling debt is neither an exceptional circumstance justifying the imposition of a non-custodial sentence, nor a mitigating factor warranting a lesser sentence that would otherwise be fit and proper. The accused voluntarily engaged in the offences and after being caught engaged in the same activity. The offences took place over a number of months, giving the accused plenty of time to seek help from authorities if the duress was real.

The court considered the following aggravating factors: 1) The nature of the criminal enterprise (identity theft of highest order); 2) that the accused was acting in association with a criminal organization; 3) the amount of the loss; 4) that the accused was one of the individuals who used the cards and used them over several months; 5) that investigating this type of activity is difficult and time consuming; and 6) the evidence of prevalence of this type of criminal activity.

The court considered the following mitigating factors: 1) that the accused had cooperated with police and had plead guilty in a timely way; 2) that the accused was a first offender; 3) that the accused had continued support from his family and still had a job open for him; 4) that the accused had spent 3 months pre-trial custody.

Policy

The judge concluded that a Conditional Sentence Order (CSO) would not be consistent with sentencing principles. A punitive as opposed to a restorative sentence is required. A CSO would not give the principles of denunciation and deterrence sufficient weight.

McVey v. United States of America, [1989] B.C.J. No. 2025 (B.C. C.A.)

Procedural Background

McVey appealed his extradition, which had been granted in *The United States v. Charles Julius McVey* (1988), 33 B.C.L.R. (2d) 28.

Facts

McVey agreed to obtain confidential information about a new computer developed by Saxpy Computer Corporation and to sell that information to Russians for the sum of $4 million USD.

McVey recruited Ivan Pierre Batinic, an employee of Saxpy, to obtain the information. Batinic proceeded to remove seven reels of computer tape from the Saxpy plant. Five of them were copied and the originals returned. Two of them were kept and blank tapes returned instead. Batinic also had the hardware design on 76 diskettes.

Legal Issue(s)

1. Is the conduct for which McVey is charged listed as a crime in both Canada and the United States?

Holding

The appeal was allowed.

Decision

The alleged scheme could not be said to defraud the public and thus did not fall within clause 27 of the Schedule of the Canada-U.S.A. Treaty (1976).

Statement of Rule
Defrauding the company of software information amounts to a deprivation of something of value to support a charge of fraud. When the party with the burden of proof adduces insufficient evidence of the foreign law, the Court applies the law of Canada.

Reasoning
The court looked at clause 27 of the Schedule and determined that the issue was whether an accused could be convicted in the United States of using the telephone in connection with a scheme to defraud the public when the evidence was that the scheme was aimed at one person, Saxpy. If an accused could not be convicted, the conduct is not a conduct included in clause 27.

The court then looked at the interpretation to give to the word public. The judge concluded that when the charge and evidence is confined to one person, a person could not be convicted in the United States of using the telephone in connection with a scheme to defraud the public. The charge would be dismissed as the crucial element "a scheme to deceive the public" is absent. Based on that conclusion, the judge held that the conduct alleged as a crime in the United States is not the conduct comprised in clause 27 of the Schedule of the Treaty.

It should be noted that the appeal was reversed in *McVey (Re); McVey v. United States of America*, [1992] 3 S.C.R. 475.

R. v. Adamkewich, 1990 CanLII 1006 (B.C. C.A.)

Procedural Background
Adamkewich pleaded guilty to two counts of fraud (s. 380) and one count of personation (s. 403). He was sentenced to 10 years of imprisonment and ordered to pay compensation in the amount of $17,600. He appealed his sentence

Facts
After arriving in Vancouver, Adamkewich moved in with Mr. Prevost. Adamkewich gained access to Prevost's personal information and used it to obtain bank credit cards and a driver's licence with his own photograph. When he was arrested, he had Prevost's B.C. birth certificate and health card which he had taken. Adamkewich had intercepted mail to take what he needed.

Adamkewich also had the identification of David Morrow. He used that name in connection with Heidi Biberhofer. Adamkewich defrauded Biberhofer of $17,862 CAD and $900 USD. They were to buy some properties together. Adamkewich also obtained a lease for a Ford Bronco under the name of Prevost.

The appellant, using Prevost driver's licence, eluded police in Washington. When he returned to British Columbia, he promptly got himself an interim driver's licence to replace the one left to the Washington Police.

The appellant had a lengthy record which contained some 47 charges of fraud.

Legal Issue(s)

1. Is the length of the sentence unfit and unduly harsh when compared with sentences passed for the same offence in similar circumstances?
2. Did the trial judge err in failing to consider the relevance of the expert evidence indicating the appellant is treatable, particularly at this stage of his life?
3. Did the trial judge err in not giving proper consideration to rehabilitation as against deterrence in circumstances where protection of the public was his primary concern?

Holding

The appeal was allowed.

Decision

The sentences were reduced to three years.

Reasoning

The court accepted the appellant's argument that the sentence was not fit and was unduly harsh based on the decisions presented by the appellant. The crimes were neither particularly sophisticated nor that complex. The sentencing judge in his reasons had not considered the principle of totality.

According the judge, the question is: does the appellant have any hope or possibility of being rehabilitated? The court considered the psychiatric evidence submitted and the appellant's situation, and concluded that the principle of rehabilitation ought to be considered along with the protection of the public.

R. v. Berryman, [1990] B.C.J. No. 1689 (B.C. C.A.)

Procedural Background

Berryman was acquitted on two counts of forging a passport contrary to s. 57(1)(a) of the *Criminal Code* and convicted of one count of making a written statement on a passport application form, which she knew to be false, for the purpose of procuring a passport, contrary to s. 57(2). The Crown appealed the acquittals.

Facts

Berryman was an employee of the Victoria Regional Passport Office of the Department of External Affairs. Berryman was a passport application examiner.

In July 1987, two forged passports were made and Berryman was knowingly and intentionally instrumental in their production. On each of the two occasions, she accepted the applications on which the passports were issued, knowing that the person from whom they were received was not the applicant. She falsely stated in writing, on the face of each application, that the applicant had produced proof of citizenship and identification. She marked the applications with a notation, which ensured that no check would be made of the guarantors, knowing that all of the information on the face of each application, including the declaration of the purported guarantors, was false.

The respondent was not the one who "made" the false documents. The forgeries were unwittingly produced by Miss Venturin, another employee of the office. Miss Venturin had no knowledge that the information in the applications was completely false.

Legal Issue(s)

1. Can a person be convicted of forgery, when the *actus reus* of that offence, the actual making of the false document, is performed by an innocent agent?
2. If so, does her conviction for making a false statement on a passport application form preclude her from also being convicted of forging the passport which was made in consequence of that false statement?
3. If the appeal is successful, can a conviction be substituted on each count rather than ordering a new trial?

Holding

The appeal is allowed, the verdicts of acquittal were set aside and convictions entered.

Decision

The trial judge erred in concluding the respondent could not be convicted because the passports were made by an innocent agent. Her conviction for making a false statement did not preclude her being found guilty of forgery. Convictions for the forgery offences were entered.

Statement of Rule

A person who commits an offence by means of an instrument "whose movements are regulated" by him, actually commits the offence himself.

Reasoning

In common law, the person who caused a felony to be committed by means of the act of an innocent agent, was considered to be the principal in the first degree. It must be demonstrated that the doctrine of innocent agency survived the codification of the criminal law.

The court held that a person who commits an offence by means of an instrument "whose movements are regulated" by him, actually commits the offence himself. The court concluded that s. 21(1)(a) of the *Criminal Code* is construed so as to give effect to the doctrine of innocent agency. Thus the trial judge erred in concluding the respondent could not be convicted because the passports were made by an innocent agent.

The court then rejected the respondent's argument that her conviction for making a false statement for the purpose of procuring a passport, should be a bar to her being further convicted of forging a passport. The court found the elements of the offences to be different.

The crux of the first offence lies in the making of a false or misleading statement for the purpose of procuring a passport. The offence is complete as soon as the statement is made with the requisite intent. Forging a passport, on the other hand, involves making a false document with one or more of the intents described in s. 366(1) of the *Criminal Code*. In each case, something quite different is "made".

The court also considered the other acts of the respondent which contributed to the forging. Notably, her notation on the face of the application which ensured no checks would be conducted.

The court also noted that the element of making a false document, which is essential to the charge of forgery, is completely absent from the charge of making a false statement.

The court held that her conviction of making a false statement does not preclude her . being found guilty of forgery. It was satisfied that an acquittal would not necessarily have been entered on counts one and two, notwithstanding the error of law made by the trial judge.

In order to enter verdicts of guilty, the court must ensure that all the findings necessary to support the convictions that were made. The court concluded there was nothing left to be tried or determined and the convictions could properly be entered.

R. v. Black, 1993 CanLII 346 (B.C. C.A.)

Procedural Background
Black was convicted of defrauding the Government of Canada of money of a value exceeding $1000 in violation of s. 380(1) of the *Criminal Code*. Black was sentenced to six years imprisonment. He appeals his sentence.

Facts
Black researched information on deceased persons fitting within a certain profile: death before 1964, in a different jurisdiction from birth, and eligible for the old age pension. He then assumed their identity to obtain lock boxes and rented post office boxes for delivery of cheques. Black also obtained birth certificates and/or Social Security Numbers to support the old age pension applications.

Black prepared old age pension applications which used a number of frequently recurring addresses. He attended the post boxes to pick up the cheques and made banking arrangements to cash the cheques.

At the time of his arrest, four cheques of a total value of $14,300 had been issued. The scheme had the potential to net $40,000 in a lump sum and monthly income of $3,500.
At the time of these acts, the appellant was before the court in Alberta for 25 similar offences.

Legal Issue(s)
1. Did the trial judge err by not taking into account the totality of sentences imposed in Alberta and British Columbia for offences of a similar nature?

Holding
The appeal was dismissed.

Decision
The court was not convinced that a sentence of six years was unfit in the circumstances described by the trial judge.

Reasoning
In this case, unlike in *R. v. Marinac* (10 May 1990) Vancouver Registry CA011878 (BC C.A.), there was no forfeiture of remission time and no increase in the total time to be served by this appellant.

The court rejected the defence counsel's argument that both the Alberta and British Columbia offences should be treated as one transaction. The court found that the Alberta transaction became an aggravating factor in this case. It had the effect of extending the record of fraud of the appellant and in illustrating that the sentence imposed in Alberta had no deterrent effect on the appellant's activities in British Columbia.

R. v. Boyle, [2005] B.C.J. No. 2501, 2005 BCCA 537 (B.C. C.A.)

Procedural Background
Boyle was convicted of fraudulently personating Daniel Richard Kovic, a deceased man, with intent to gain an advantage for himself, contrary to s. 403(a) of the *Criminal Code*. He appealed his conviction.

Facts
Mr. Boyle acquired a birth certificate in the name of Kovic and used that certificate to get a social insurance number and a B.C. identification card. He then used these documents to obtain a learner's driver's licence in the name of Kovic. He also obtained a bank account and a postal box using Kovic's identity.

Legal Issue(s)
1. Did the trial judge err in admitting as evidence Boyle's criminal record on the basis that its probative value was not outweighed by its prejudicial effect?
2. Did the Crown demonstrate that he used his false identity to gain any advantage he could not obtain under his own name?

Holding
The appeal was dismissed and the conviction sustained.

Decision
The evidence was admissible and its weight was a matter for the trial judge to decide. The fact that he came to the attention of the authorities before he was able to obtain any particular monetary or other advantage does not afford a defence to the charge of which he was convicted.

Reasoning
The trial judge found that the accused obtained the false identity to make his past disappear and thereby gained an advantage. The words 'gain advantage' could scarcely be more general in their scope. The trial judge held that the appellant had gained an advantage by being able to adopt a new identity. It was only required, to obtain a conviction, that the judge find that the appellant had the intent to gain an advantage by personating someone else.

R. v. Richard, [2005] B.C.J. No. 2438, 2005 BCCA 536 (B.C. C.A.)

Procedural Background
Richards was found guilty of one count of fraud over $5,000.00, contrary to s. 380(1)(a) of the *Criminal Code* and one count of personation with intent, contrary to s. 403(a) of the *Criminal Code*. He was sentenced to 10 months imprisonment. He sought leave to appeal the sentence.

Facts
Between December 8 and December 25, 2003, Richards obtained a $25,000.00 loan from Vancouver City Savings by passing himself as Russel Galovich. The funds were never recovered.

Legal Issue(s)
1. Would the sentence imposed have been considerably less if these offences had been dealt with at the time of an earlier sentencing?

Holding
The court dismissed the leave to appeal.

Decision
Mr. Richard's sentence was not demonstrably unfit.

Statement of Rule
Is the sentence in all of the circumstances demonstrably unfit?

Reasoning
The trial judge took into account the age of Mr. Richard (23), that he has a young family, and that he had employment available. However, he also took into account Mr. Richard's 30 prior convictions, which had occurred on an approximately yearly basis. These offences included personation and possession of stolen property.

The court recognized Mr. Richard's concerns that the charges were not processed in a timely fashion. However, what the court has to consider is whether the sentence in all of the circumstances is demonstrably unfit. It is not the court's role to impose a sentence it thinks was fit in the circumstances; that is not an option open to the court.

R. v. McNeil, [2006] B.C.J. No. 187, 2006 BCPC 32 (B.C. C.A.)

Procedural Background
Mr. McNeil pleaded guilty to the possession of a homemade mail key. This case deals with the sentencing of Mr. McNeil.

Facts
When Mr. McNeil was searched, he was in possession of two forged mail keys, many pieces of identification in the name of others and stolen mail, including credit cards.

The identification included driver's licences in the names of others. Mr. McNeil also had the driver's licence, Care Card and other identification of Mr. Shawn Coldwell. Mr. McNeil also had personal information on Mr. Lanny McVeigh including address, home phone number, date of birth, cell phone number, bank balance and line of credit. There was also evidence that Mr. McNeil was practising the signature of Mr. Lanny McVeigh. However, there was no evidence that Mr. McNeil used these items for his benefit.

Mr. McNeil had already gotten bail on another offence in which he was also found to be in possession of a driver's licence in the name of another with his picture on it. When these second offences were committed, the accused was on probation order and on bail.

Legal Issue(s)

1. What is the appropriate sentence?

Decision

The judge imposed a sentence of 18 months imprisonment.

Reasoning

The court found that a sentence other than a jail sentence would be completely inappropriate considering the number of offences, their nature and the persistent nature of the accused's offending. The court considered it appropriate to label the accused as a "regular offender" because the accused's drug addiction has brought him before the court on so many occasions for these types of offences.

Policy

In its reasons the court noted that if this kind of behaviour is not met sternly by the court, it will result in the public having a complete lack of faith in its mail system, the validity of the driver's licence and a lack or lessening of faith in the financial field and the validity of the documents that the public takes for granted and relies upon every day. It also underlined that these offences are identity-theft offences, which if not dealt with seriously will lead to a weakening of the whole social fabric that we all rely on.

R. v. Taft, [2003] B.C.J. No. 444, 2003 BCCA 104 (B.C. C.A.)

Procedural Background

Taft pleaded guilty to 25 counts of personation (s. 403); three counts of fraud (s. 380), three counts of uttering a forged document (s. 368); one count of obstructing a police officer (s. 129); seven counts of forgery (s. 366); one count of possession of property obtained by the commission of an offence (s. 354); one count of forging a passport (s. 57); and two counts of possession of a forged passport (s. 57). Taft was sentenced for 27 months, with three remaining after deducting his pre-trial custody.

On October 22, 2002, Taft pleaded guilty to one count of obstructing justice (s. 139) and four counts of uttering a forged document (s. 368); he was sentenced to 15 months imprisonment. Taft sought leave to appeal his sentences.

Facts

Between November 1998 and August 2000 Taft obtained personal information from individuals by advertising for construction manager jobs in the local newspaper. He sent letters to applicants saying that they had been short listed and needed to provide copies of identification documents. The appellant then, using his photograph, forged or applied for identification in the name of the job applicants. Using the identification, he opened bank accounts under their name and deposited forged cheques in the accounts. Between April 2, 2000 and June 14, 2000, Taft obtained almost $80,000.

In August 2000, bank personnel was suspicious With the police, they confronted Taft. While he was under investigation, he travelled to Montreal and setup a website using the assumed identities. The website was used to offer false identification. When Taft was arrested in Vancouver in July 2001, he provided three successive false names before the police established his identity using fingerprints.

The appellant had set up a number of false residences under the false identities. The search of his apartment revealed over 300 unfilled orders for false identification from all over the world. The search also revealed 200 applications that had been filled, providing Taft with almost $19,000.

During the proceeding on the first set of charges, Taft provided his lawyer with several copies of letters and certificates of completion of programs from the institution where he was held. Four of the letters were determined to be forgeries.

The first set of offences was committed while Taft was on supervised release for his Washington State offences.

Legal Issue(s)

1. Is the first sentence demonstrably unfit?
2. Is the second sentence demonstrably unfit?

Holding

Leave for appeal was denied.

Decision

In the judge's view, Taft had no basis for contesting his sentence, which the judge could only describe as lenient. The sentence of 15 months was entirely fitting for the cynical attempt to manipulate the courts.

R. v. Hall, 1998 CanLII 3955 (B.C. S.C. (T.D.))

Procedural Background

The defendants were charged with fraud (s. 380) and theft of telecommunication service (s. 326) and possession of devices used for the theft of telecommunication services (s. 327). This was an application to exclude evidence.

Facts

Nicole Walker, an employee of the Ministry of Environment, obtained and transferred personal information of fellow employees to Mark Hall. Hall passed this information to two other accomplices who worked for Radio Shack. The two Radio Shack employees used the personal information to fill out false applications for cellular service.

Nineteen "ghost" accounts were established using this scheme. The bills were sent to false addresses. The applications were made between December 1996 and April 1997.
The applications required a date of birth, SIN and a driver's licence number. However providing only a date of birth and SIN was sufficient to base a credit check.

The police contacted Rogers Cantel, which proceeded to an inquiry. The investigation produced evidence of credit applications and computerized billing records central to the Crown's case. Also produced were carbon copies of the forms filled out.

When a sale was completed, the sales agent would make an original and three carbon copies of the application for credit and cellular service.

Legal Issue(s)

1. Are computer records inadmissible under the *Canada Evidence Act* s. 30(10(a)(i) as generated in the course of an investigation?
2. Are the computer records inadmissible because they are not originals but copies, requiring the Crown to comply with *Canada Evidence Act* s. 30(3) and (4)?
3. Are the computer records admissible under the common law exception to the hearsay rule?
4. Are the computer records admissible as real evidence generated entirely by machine, without human intervention?
5. Are the Radio Shack records inadmissible as copies rather than originals?

Holding

The application was dismissed and the evidence admitted.

Decision

The computer printouts were admissible as they had not been produced as part of an investigation and were not copies. The evidence was also admissible under the common law hearsay exception. The evidence generated without human input was admissible. The carbon copies were admissible as originals.

Statement of Rule

Hearsay evidence is admissible based on the twin demands of necessity and reliability. Necessity is not based on necessity to the Crown's case, but rather on the necessity to establish a given fact. As for reliability, records made contemporaneously by someone having personal knowledge of the matters being recorded and under a duty to make the entry, should be received in evidence as *prima facie* proof of the facts stated therein.

Reasoning

Records made in the course of an investigation are inadmissible based on s. 30(10) of *Canada Evidence Act*. Their primary utility is in litigation and not in normal business operations. The judge distinguished this case from *R. v. Biasi* (No. 2) (1981), 66 C.C.C. (2d) 563 because, in that case, the police had made the logs. In this case, the investigators retrieved portions of pre-existing records which were not originally made with a view to criminal or civil legal proceedings but rather for ordinary business purposes. This is equivalent to a bank clerk that identifies a bank record from an account record. The information in question had been created before the investigation was contemplated. For these reasons, the evidence was admissible.

A computer record must be regarded as coming within the definition of a record "… document, paper, card … on or in which information is written, recorded, stored or reproduced, …" A computer screen printout does constitute a record of the information that was originally created. The argument that the printouts are not records because they are not permanent was rejected. The

argument that the printouts are merely copies was rejected. For these reasons, the printouts are admissible.

In *R. v. Sunila and Soleyman* (1986), 26 C.C.C. (3d) 331, it was held that computer records, generated during the course of an investigation and as such barred by s. 30(10)(a)(i) of the Canada Evidence Act, were nonetheless admissible under the common law requirements of *Ares v. Venner*, [1970] S.C.R. 608.

Hearsay evidence is admissible based on the twin demands of necessity and reliability. Necessity is not based on necessity to the Crown's case, but rather on the necessity to establish a given fact. The evidence is central to the entire enquiry yet the computer that created it cannot testify. Most large organizations have huge amounts of information retained as data with no tangible form. As for reliability, records made contemporaneously by someone having personal knowledge of the matters being recorded and under a duty to make the entry, should be received in evidence as *prima facie* proof of the facts stated therein. In this instance, the recorder of information, a passionless mechanical computer with no subjectivity, surpasses the requirement of "a person having personal knowledge."

The argument that the records were inadmissible as they were completely unreliable was rejected. The judge did find that there were some errors but also found that, by and large, the records are created and relied upon in the ordinary course of business and are thus reliable notwithstanding the errors in question.

The defence also contended that as a condition precedent, evidence from someone with knowledge and qualifications who can say that the computer system and the printouts are reliable is required. Such information is desirable but as long as there exist in evidence other *indicia* of reliability, a court may hear such evidence. The admitted technical ignorance of the investigators was not fatal.

Ultimately, Rogers Cantel's reliance on these records for conducting business ensured the reliability of those records. Computers are subject to error, but these problems to weight rather than admissibility. The court also noted that the usual fears of hearsay evidence, namely perception, memory, and credibility, are irrelevant to a computer generated record. The evidence was admissible under common law as it satisfied the "circumstantial guarantee of trustworthiness" stated in *R. v. Smith*, [1992] 2 S.C.R. 915.

The defence contended that even though there had been no human input, the computer generated records contain a certain number of obvious errors. The judge held that the very existence of Rogers Cantel is predicated upon their computer systems being accurate, save for the odd error. The evidence generated without human input is admissible.

Several Courts of Appeal have ruled that carbon copies are admissible as originals, even if they are not the top white copy. The objection is thus dismissed.

<u>Policy</u>

The law must be applied in accordance with the rapidly changing reality of today notwithstanding that it was drafted in the past.

R. v. Reith, [2003] B.C.J. No. 2227, 2003 BCSC 1454 (B.C. S.C. (T.D.))

Procedural Background
Reith pleaded guilty a charge of personation contrary to s. 403(a) of the *Criminal Code*. This was Reith's sentencing.

Facts
Ms. Reith was 56 of age, had a grade 9 education and suffered from alcoholism. Ms. Reith passed herself in the name of her dead sister to the Ministry of Human Resources, thereby collecting Social Assistance. In another trial, Ms. Reith was also found guilty of defrauding the Ministry of a sum in excess of $5,000.00. Ms. Reith received benefits under her own name and under her sister's name. She also misinformed the Ministry as to her status, which enabled her to get benefits.

Legal Issue(s)
1. What is the appropriate sentence?

Decision
The judge imposed a sentence of one year and a specific direction that Ms. Reith be assessed for alcoholism and appropriate treatment, followed by one year probation. The judge also made an order for restitution in the amount of $50,000.00.

Reasoning
The court considered the case *R. v. Sivard*, (1996) 109 C.C.C. (3d) 471 in which the factors to take into consideration in the sentencing of fraud offences are enumerated. They include 1) the nature and extent of the loss; 2) the degree of premeditation; 3) the accused's actions after the offence; 4) previous convictions; 5) personal benefits obtained by way of the offence; 6) the trust in the relationship between the victim and accused; and 7) the motivation underlying the offence.

The court found that there was premeditation and planning, that Ms. Reith was not in a position of trust; the benefits are the moneys obtained. The court notes that taking from the public fund must also be considered. The trial judge found the offence took over a significant period of time, involving numerous incidents of deceit. The trial judge also noted the criminal record for shoplifting, the fact that the amount was significant and the unlikelihood of the money being recovered. As mitigating factors, the judge considered she had pled guilty, that she had a 12-year old son who would need her help and that she had health problems.

The court found that this is not a case for a two-year sentence. It was a case that demanded imprisonment and that the sentence also provide the best chance of rehabilitation and treatment for Ms. Reith.

R. v. Thomas, [2002] B.C.J. No. 734, 2002 BCPC 113 (B.C. Prov. Ct. (Crim. Div.))

Procedural Background
Thomas was charged with eight counts of fraud contrary to s. 380(1)(a) of the *Criminal Code*. Thomas pled guilty to the charges. This case concerned her sentencing.

Facts

Between January 1, 1996 and March 30 of 1999 Thomas defrauded the Canadian Imperial Bank of Commerce, in regards to student loans, of an amount in excess of $5,000. Between January 1, 1996 and March 30 of 1999 Thomas defrauded the Province of British Columbia, in regards to student loans, of an amount in excess of $5,000. Between January 1, 1996 and March 30 of 1999 Thomas defrauded the Receiver General, in regards to student loans, of an amount in excess of $5,000. To conduct these frauds, Thomas obtained student loans using fifteen names other than her own. She obtained $130,135.00 and had obtained approval for another $62,050.00. She obtained the student loans by assuming fifteen names under which the applications were made. Six of those names were obtained by applying for and obtaining five legal name changes for her sister, Ankica Zupan, and making applications in these names. Another 9 names where adopted and used to process the applications.

Between November 24, 1996 and August 14, 1999 Thomas defrauded The Royal Bank of Canada of an amount in excess of $5,000. She obtained Visa Cards, using four assumed names, to make purchases. While employed as a summer legal researcher, she took letterhead from her employer and falsified a letter of reference misrepresenting the terms of her employment so that she could obtain a line of credit from Royal Bank. The total amount obtained using the two methods was $35,998.15.

Between April 10, 1997 and June 23, 1999 Thomas defrauded the Bank of Montreal of an amount in excess of $5,000. She falsified employment letters from the B.C. Society of Occupational Therapists that exaggerated her salary, to cause the bank to extend credit based on those misrepresentations. She also obtained identification from Dr. Mary Stephenson and opened bank accounts and credit cards in her name. When she had to attend personally, she wore a costume. The disguise was found in her residence when she was arrested. She obtained $32,525.41.

Between March 14, 1995 and December 31, 1999 Thomas defrauded Canada Trust. She obtained $55,740.66, of which $10,000 was obtained under Dr. Stephenson's name. On May 1, 1996 she declared personal bankruptcy and changed her name to Helen Thomas.

Between November 12, 1992 and February 15, 1998 she defrauded the Government of Canada, Human Resources Development Canada. She obtained $56,663.00 by way of employment insurance fraud. The money was obtained using five bogus claims; three in the accused's former name Helene Zupan and two in her sister's name. To conduct this fraud, Thomas obtained and prepared false Records of Employment while working for KPS Plumbing.

Between May 22, 1996 and December 31, 1998 Thomas defrauded the Province of British Columbia, Ministry of Social Development and Economic Security. She obtained $5,581.00 by collecting welfare under the name Helene Zupan and failed to declare student loan money she had received as well as the fact she was in full time attendance in college and university. She also failed to declare that she was employed.

Legal Issue(s)

1. What is the proper sentence?

Decision

Thomas was sentenced to two years less one day for each count. The sentences were to be concurrent. Thomas was also sentenced to two years probation following the sentence. A restitution order was also made for restitution of the amounts taken to the respective entities.

Reasoning

The court considered the gravity of the offence and noted that the amount taken over six years was remarkable. Thomas netted an average of $50,000 annually. The court found that her motive was her own greed.

The court rejected the accused's pretension that the cycle that began and carried her further and further in the enterprise should be considered as a mitigating factor. The court found that this does not distinguish her from other offenders.

The court also noted that the frauds were all committed in situations where the members of the public are trusted to be honest in putting forth claims for entitlement to public funds. The accused not only breached that trust, she did so repeatedly, on a massive scale, and her schemes involved impressive amounts of money. She demonstrated a commitment and diligence that would be most commendable in a legitimate enterprise. Planning and premeditation aggravated the offence.

The court also noted that her financial situation would have permitted not much more than token reimbursement of the money she had taken, even though she had offered to undertake some programme of restitution. The court also noted that she did not have a criminal record.

The court took into consideration the following sentencing factors: 1) specific deterrence: the sentence imposed must take care to impress on the accused that such behaviour will not be tolerated; 2) protection of the public: the court concluded there is some danger she will re-offend; 3) rehabilitation: the court concluded her rehabilitation is probable and must be a consideration; 4) denunciation: the amount, the breach of trust and methodical nature of the frauds attract denunciation; 5) general deterrence: this case required a sentence that emphasized general deterrence.

The court concluded based on these factors that these offences will attract a sentence at a lower range. The court accepted both counsels' submissions requesting a sentence of two years less one day. However, the court concluded that a conditional sentence would endanger the safety of the community by encouraging others contemplating similar offences.

R. v. Tonks, [2003] B.C.J. No. 3042, 2003 BCPC 475 (B.C. Prov. Ct. (Crim. Div.))

Procedural Background

Tonks pleaded guilty to one count of fraud over $5,000 contrary to s. 380(1)(a) of the *Criminal Code*, three counts of being in possession a debit card knowing the property was obtained by the commission of an offence, contrary to s. 355, one count of being in the possession of a vehicle knowing the property was obtained by the commission of an offence, contrary to s. 355(B), and one count of being in possession of cheques, of a value of less then $5,000, knowing the property was obtained by the commission of an offence contrary to s. 355(a). This case concerned Tonk's sentencing.

Facts
Between October 30, 2002 and November 6, 2002 Tonks used three debit cards which were stolen from the mail. He received over $29,000 in cash and consumer goods. Tonks also made fake deposits using empty envelopes.

On June 15, 2003 the police arrested Tonks in a Toyota 4Runner. The ignition and passenger doors were damaged. While being booked the accused advised the police that he knew the vehicle was stolen but that he did not steal it.

On July 7, 2003, while on bail for the other offences, Tonks was a passenger in the car of Mr. Stacy, the co-accused. Stacy tried to cash a cheque stolen from the mail at a Money Mart. The Money Mart employee was suspicious and called the police. When the police arrested them, they found three cheques made out to the accused as the payee. The accused had already cashed a cheque worth $460.

Legal Issue(s)
1. What is the proper sentence?

Decision
Tonks was sentenced to ten and a half months of imprisonment followed by two years of probation. Restitution in the amount of 28,859.68 was a condition of the probation order.

Reasoning
The sentencing judge considered the accused's age of 21, the fact that his girlfriend was expecting twins, the fact that he had been offered a job upon his release and that he had accepted full responsibility and indicated that he planned to pay the monies back in time.

The judge then looked at the principles of denunciation and specific as well as general deterrence. The judge also noted that mail theft is becoming widespread and that personal financial information is targeted in that type of theft. The judge noted that Tonk's actions were deliberate, with personal financial gain as the motive.

The judge then considered a conditional sentence but concluded that based on the accused's non compliance with his bail terms and his not appearing in court on July 17th when he had been released a second time, Tonks could endanger the community. The judge also indicated that the conditional sentence would not have served the needs of denunciation and deterrence.

The judge concluded that in this case, the only effective way of impressing upon the accused the community's denunciation of his actions and of accomplishing general deterrence was to impose a custodial sentence.

R. v. Harris, [2004] B.C.J. No. 2847, 2004 BCPC 532 (B.C. Prov. Ct. (Crim. Div.))

Procedural Background
Jamie Grant Harris pleaded guilty to one count of possession of a motor vehicle of a value in excess of $5,000, knowing that that property was obtained by the commission in Canada of an offence; one count of possession of property obtained using a false credit card; one count of using

a false credit card; and one count of using a counterfeit mark. This case concerned Harris' sentencing.

Facts
Mr. Harris is 26, a recent father and has a limited criminal record ("not the worst this court has seen"). Mr. Harris was in the possession of a vehicle obtained by someone using a false credit card. Mr. Harris used false credit card to obtain clothing from a Bootlegger store and used a false credit card in a Trend store. Mr. Harris also used a counterfeit mark on a British Columbia driver's licence which had his photograph and the name of C.S.D.

Legal Issue(s)
1. What is appropriate sentence?

Decision
Mr. Harris was sentenced to thirteen months. Factoring in the pre-trial custody, Mr. Harris will serve five months. He also sentenced Mr. Harris to twelve months of probation after his release.

Reasoning
In this case, the judge notes that in the past identity theft amounted to a capital crime and that this is a reflection of our history which makes these kind of offences some of our more serious offences.

The judge also found that Mr. Harris was involved in a concerted effort to recreate or impose his identity upon the identity of someone else. The judge also notes that the victim of the identity theft committed by Mr. Harris will have to take some time and effort to have the fraudulent use of this name taken off his record and restored.

The judge was also concerned by Mr. Harris's possession of a notebook containing 39 MasterCard accounts for which the numbers did not belong to Mr. Harris. According to the judge, this indicated some planning on the part of Mr. Harris.

The judge then looked at sentencing principles and found the issue of deterrence to be a primary matter. The court recognized the need to protect the ability of the public to carry on commerce in a safe and orderly fashion and to tell those who disrupt that commerce that a custodial sentence is the likely result. The judge also considered the following factors Mr. Harris's age, circumstances and pre-trial custody.

Policy
The sentencing judge also noted that there is a need to protect the ability of the public to carry on commerce in a safe and orderly fashion, and at the same time there is a need to tell those who want to disrupt that commerce by using fraudulent means that a custodial sentence for those who engage in that activity is the likely result.

R. v. Jubbal, [2004] B.C.J. No. 2207, 2004 BCPC 389 (B.C. Prov. Ct. (Crim. Div.))

Procedural Background
Jubbal and Gosal pleaded guilty to fraud contrary to s. 380(1) and 463 of the *Criminal Code*. This case concerned their sentencing.

Facts
The defendants used both stolen and false documents to defraud Prospera Credit Union of $17,000.00. When the defendants were arrested, they provided false information to the police and were, attempting to secure a second loan from another financial institution by the same means.

Mr. Gosal had been convicted twice of possession of stolen property under $5,000. Ms. Jubbal had no prior convictions but was acquitted of a number of charges.

Legal Issue(s)
1. What is the appropriate sentence for Gosal?
2. What is the appropriate sentence for Jubbal?

Decision
Mr. Gosal was sentenced to nine months imprisonment and two years of probation with conditions over the mandatory conditions. Ms. Jubbal was sentenced to four months in jail and two years probation with the same conditions as Mr. Gosal. Finally, the court ordered restitution to be made in the amount of $17,000.00.

Reasoning
The court found the defendants were engaged in a scheme which required a great deal of planning, premeditation and deception. In reaching the appropriate sentence, the judge took into account the circumstances of the offence, the circumstances of the defendants, the submission of counsel, portions of the Pre-Sentence Reports, case-law and the brief statement provided by each defendant.

The court considered the significance of the period of time over which the scheme was carried out. The judge noted that this time provided the defendants a number of opportunities to abandon the scheme. Another aggravating factor was the use of documents obtained by identity theft. The judge also considered as aggravating the fact that they were in the process of committing the scheme a second time. Also taken into account were the uncooperativeness of Mr. Gosal, his prior convictions and Ms. Jubbal's lack of a prior criminal record.

The court found that in the present case the need for denunciation and deterrence was great and pressing and concluded that a Conditional Sentence Order would not be a fit sentence for either Mr. Gosal or Ms. Jubbal.

Policy
In his reasons, the judge noted that identity theft is a growing problem which could ultimately threaten the integrity and stability of the economic order on which we all depend.

R. v. P.T., 2005 BCPC 55 (B.C. Prov. Ct. (Crim. Div.))

Procedural Background
P.T. pled guilty to fraud over $5,000.00 in violation of s. 380(1)(a) of the *Criminal Code*. This is P.T.'s sentencing.

Facts

Starting in 1986 P.T. made unsuccessful investments which lead her into financial difficulties. P.T. was the branch manager of the bank. As a result, P.T. created fictitious loans which she intended to pay back. Unfortunately, the loans did not resolve the situation and she had to continue creating loans in an effort to stay afloat. This practice is known as kiting in the banking industry.

The fictitious loans where created in the names of some of the bank's clients. Some of them had negative experiences when they applied for credit elsewhere. The losses are approximately $1.57 million, of which about $100,000 was given back in restitution.

Legal Issue(s)

1. What is the appropriate sentence?

Decision

The judge was satisfied that a jail sentence in the lower range is appropriate and sentenced P.T. to three years of imprisonment.

Reasoning

The court found that the offence was a serious one which involved a huge sum of money defrauded over a long period of time by someone in a position of trust.

The court considered the following mitigating factors: 1) the guilty plea and the expressed intention to plead guilty when the fraud was discovered; 2) the sincere expression of remorse; 3) lifetime achievement of good works both before and after the fraud; 4) lack of a criminal record; 5) treatable psychiatric issues; and 6) efforts towards restitution.

The court then considered the following as aggravating factors: 1) the sum of money; 2) the high level of breach of trust; 3) the length of time and the number of loans (87); 4) the sophistication; 5) the use of customers' identities; and 6) the lack of real restitution, given that the money was lost in the stock market. The court did not consider the fact that a bank was the victim as a mitigating factor.

P.T. had completed approximately 1200 hours of community services with three organizations. The judge was satisfied that she had gone a long way towards making reparation to the community. The judge is also satisfied that P.T. does not need further deterrence, thus rehabilitation has been largely achieved.

Policy

The judge also concluded that the sentence must denounce on behalf of society the abhorrent breach of trust committed by P.T. The sentence aims at deterring others in positions of trust.

R. v. R.W., [2006] B.C.J. No. 830, 2006 BCPC 154 (B.C. Prov. Ct. (Crim. Div.))

Procedural Background
R.W. pled guilty to one count of using a forged or falsified credit card knowing that it was obtained by the commission of an offence in Canada; and three counts of defrauding by deceit, falsehood or other fraudulent means. This case concerned R.W.'s sentencing.

Facts
Mr. R.W. produced an Alberta's driver's licence in the name of Jason Scott with his picture on it and a fake social insurance card as supporting documentation. He then utilized fake or fraudulent Visa credit cards to obtain or attempt to obtain merchandise from several West Vancouver merchants, including a Radio Shack store, a London Drugs store, a Lens and Shutter store and a Sunglasses Hut store. The total value of the merchandise obtained was under $5000 but in excess of $4000.

Legal Issue(s)
1. What is appropriate sentence?

Decision
Mr. W. was sentenced to a fine of $2,000.00 and a twelve month probationary period.

Reasoning
In arriving at the appropriate sentence, the judge considered the submissions of counsel; the sophistication involved; the myriad of problems identity theft causes for law abiding citizens; the minimal likelihood of recidivism as shown by a psychological report; a victim impact statement; a job offer received by Mr. R.W.

The court found the following aggravating factors: a man with no prior convictions willingly involved himself in the offence which indicated a serious lack of moral turpitude; Mr. R.W. sought to benefit financially; he did not provide information to the police about others involved.

The judge found that on the facts Mr. R.W. was a determined scam artist and that the persistence of his criminal conduct raises suspicions about exactly just what he did know and how much he was involved in these frauds.

As mitigating factors, the court noted that Mr. R.W. was involved in commendable volunteer community work and that he had creatively found employment. The court also noted that Mr. R.W. had pleaded guilty.

The judge found that neither a conditional jail sentence nor a conditional discharge would be appropriate in this case. A conditional jail sentence would be excessive and a conditional discharge would not be in the public interest because of the nature of the crime, the sophistication involved and the accused's involvement in it. In short, the aggravating factors far outweigh the mitigating factors.

Policy
In his reasons, the sentencing judge noted that Mr. R.W. became involved in identity theft and that each and every person in our community that holds a valid credit card is victimized by such conduct. The conduct complained of is definitely not a victimless crime.

The sentencing principles of denunciation and general deterrence mandate that the offender receive a criminal record for his conduct to bring home to him specifically, but more importantly to others in the community who may be like-minded, that there will be a penalty for this kind of action.

R. v. Olotu, [2004] M.J. No. 361, 2004 MBCA 146 (Man. C.A.)

Procedural Background
Olotu pleaded guilty to seven counts of fraudulent use of credit cards obtained by identity theft. The sentencing judge imposed a conditional sentence of two years less a day with strict conditions. The Crown appealed the conditional sentence.

Facts
Mr. Olotu was arrested in 2002 for credit card fraud and was released. He was subsequently arrested in April 2004 and had in his possession fraudulent credit card applications in the names of other individuals. He also had electronic equipment worth $11,000. Some of the equipment was linked back to purchases made by Mr. Olotu using the fraudulently obtained cards. The accused was on probation on other charges at the time of both offences.

Legal Issue(s)
1. Did the sentencing err in principle when he did not take into account the risk of the accused re-offending and the principle of denunciation?

Holding
The appeal is dismissed.

Decision
The sentencing judge did not commit an error of principle; the record indicates he took these two considerations into account.

Statement of Rule
It is incumbent upon a sentencing judge to consider and explain why a conditional sentence would or would not be consistent with the four factors enunciated in *R. v. Proulx*, [2000] 1 S.C.R. 61 at para. 46.

Reasoning
The reasons for decision must be understood in the complete context of the case, including the facts, exhibits files and submissions by counsel. Reasons of the sentencing judge emerge from his questions to counsel and his conditions. It would have been preferable if his reason had included some analysis on the issues of risk and principles.

Policy
Given the workload and time pressures of provincial courts, their reasons need not be long or take into consideration every detail; an unrealistic high standard for such reasons is not required. Fundamentally, the approach taken is functional and practical one.

R. v. Okungbowa, [1991] O.J. No. 1692 (Ont. Ct. J. (Gen. Div.))

Procedural Background
Okungbowa was charged with personation and fraud exceeding $1,000 contrary to ss. 403(a) and 380 of the *Criminal Code*.

Facts
Kenneth Coker lost his wallet in 1988 and it was never recovered. From July 1989 to March 1990, Okungbowa deposited various cheques and made several withdrawals using the name of Kenneth Coker. Okungbowa was identified by different witnesses in different bank branches.

Legal Issue(s)
1. Did the Crown prove the offences beyond a reasonable doubt?

Holding
The accused was convicted of both charges.

Decision
The judge was satisfied beyond a reasonable doubt that Okungbowa did fraudulently personate Kenneth Coker with intent to gain an advantage for himself. The evidence established beyond a reasonable doubt that Okungbowa defrauded Royal Trust of monies in excess of $1,000.

Reasoning
The court considered the defence counsel statements about the great caution which must be exercised in relation to a prosecution which is based almost entirely on identification evidence. The judge considered that all eyewitness identification suffers from the natural frailty of human observation or human recollection which are both notoriously unreliable in this area.

The judge considered the irregularities with the identification evidence submitted by the defence and concluded that they do not require the trier of fact to reject the evidence outright as having been tainted.

The judge found as a fact that a video tape submitted in evidence confirms a witness's evidence as to the identity of the accused, who was in her Royal Trust branch on Saturday, July 29th 1989. The court rejected the accused's evidence that he did not represent himself as Kenneth Coker.

R. v. Blanas, [2004] O.J. No. 3982, 2004 ONCJ 212 (Ont. Ct. J. (Gen. Div.))

Procedural Background
Blanas was charged with two Criminal Code offences: Theft over $5,000 and Breach of Trust. There was also a charge under section 122(1)(c) of the *Immigration and Refugee Protection Act* (IRPA), R.S.C., 2001, c. 27. This was a preliminary inquiry to determine if Ms. Blanas would stand trial.

Facts
Ms. Blanas was employed as a production clerk at the Scarborough passport office. On June 21, 2002, five boxes of passports were stolen from the production room in the passport office at the end of the business day. The Passport Blank Control List (PBC) indicates Blanas made entries for the five boxes. Blanas placed the passports in the garage of another individual.

Legal Issue(s)
1. Is there sufficient evidence to order Ms. Blanas to stand trial?

Holding
The accused was ordered to stand trial.

Statement of Rule
A committal is required where there is any evidence upon which a reasonable jury, properly instructed, could convict. It is not a question of whether a properly instructed jury, acting reasonably, would infer guilt from the evidence adduced at the preliminary inquiry, only whether they could do so.

To rely on the doctrine of recent possession to prove the accused stole the property, the Crown must show 1) that the goods were recently stolen; and 2) that they were found in the possession of the accused. To establish constructive possession, the Crown must prove knowledge and control.

Reasoning
The court was satisfied Blanas had removed the passports and placed them in Allan Graham's garage. The judge was also convinced by the testimony of her co-workers that Blanas, by virtue for her employment as a production clerk had the requisite knowledge and opportunity to steal the passports. The altered entries on the PBC list further support the inference that Blanas stole the passports. The court was satisfied that the doctrine of recent possession applied.

The judge was convinced 1) that the blank passports entrusted to Blanas were valuable government assets and that she knew of the measures used to protect the passports; and 2) that Blanas derived a benefit from this breach of trust because of the potential sale value of the passports.

The judge accepted evidence that Blanas sold or distributed or dealt with at least one box of passports shortly after the theft. The judge also considered the definition of "traffic" in the *Controlled Drugs and Substances Act*, which includes the acts of selling, giving, delivering, transferring or transporting. A jury could conclude that by removing and placing the passports in the garage, Blanas was "dealing" in blank passports.

R. v. Renew Credit Services Canada Inc. et al., [2005] O.J. No. 5899, 2005 ONCJ 524 (Ont. Ct. J. (Gen. Div.))

Procedural Background
Renew Credit Services Canada Inc. and Sherri Graham were charged with the offence of operating as a credit repairer and requiring or accepting payment or security for payment, directly or indirectly, from a consumer without causing a material improvement to the consumer report,

credit information, file, personal information, credit record, credit history or credit rating of the said consumer, contrary to s. 13.1(1) of the *Consumer Reporting Act*, R.S.O. 1990, c. C-33 (the Act)

Renew Credit Services Canada Inc. and Sherri Graham were charged with operating as a credit repairer and failing to deliver to a consumer, a written contract containing information which met the requirements of s. 13.2(1)(a) of the Act as amended and its O. Reg 468/01 at s. 12, and thereby had committed an offence under s. 23(1) of the Act.

Renew Credit Services Canada Inc., Todd Alexander Gnish and Sherri Graham were charged with the offence of engaging in an unfair practice in relation to a consumer contrary to s. 17(2) of the *Business Practices Act*, R.S.O. 1990, c. B-18

Renew Credit Services Canada Inc., Todd Alexander Gnish and Sherri Graham were charged with the offence of carrying on the business of a collection agency without registration by the Registrar under the Act, contrary to s. 28(1) of the *Collection Agencies Act*, R.S.O., c. C-14.

Facts

November 20th, 2002 Derek Hardy met with a representative of Renew Credit Services. The representative asked him about his debts and they worked out a monthly payment plan to cover the debts. The monthly payment was established at $200.00 and payable directly to Renew Credit Services.

Mr. Hardy's understanding was that Renew Credit Services was going to consolidate his debts and would provide information as to where his money was going. This was all for the purpose of improving his credit rating.

Mr. Hardy provided post dated cheques and two money orders, each in the amount of $200.00, to Renew Credit Services. He received a letter saying he would receive a manual which he never got. He received no confirmation or proof from Renew Credit Services as to where his money was going, nor did Mr. Hardy receive any acknowledgment from his creditors.

On September 18th, 2003 he sent a letter to Renew Credit Services requesting his money back. At that date, they had cashed four cheques and the two money orders.

Legal Issue(s)

1. Are the defendants guilty of the offences?

Decision

The defendants are guilty of the four charges and convictions are registered.

Reasoning

The judge found Mr. Hardy's oral evidence to be credible. That evidence combined with the contract demonstrated clearly that Renew Credit Services had been acting as credit repairers. The trial judge was satisfied that the Crown had proven beyond a reasonable doubt the elements of the first offence.

Section 12 of the regulation lists items that must be contained in the contract. Section 12(f) requires that the statement set out in the Schedule be located on one page and in not less than 10

point type, in which the heading "your Rights under the *Consumer Reporting Act*" is not less than 12 point bold type. This statement was not embodied in the contract. The trial judge was satisfied that the Crown had proven beyond a reasonable doubt the elements of the second offence.

Mr. Hardy had understood that debt consolidation would improve his credit rating. The judge found it clear from the evidence that this had not occurred. Mr. Hardy had made a number of payments and there was no evidence that the defendants had done anything on his behalf as required by the contract. The judge found that Sherri Graham had been complicit in the commission of the offence. There was no evidence presented that she did not authorize, permit or acquiesce to the offence. The judge was also satisfied based on Mr. Hardy's evidence that he had spoken to "Todd" and that in these conversations Mr. Gnish made representations to the defendant which did not happen. These representations constituted an unfair practice. The trial judge was satisfied the Crown proved beyond a reasonable doubt the elements of the third offence.

The judge found that it was clear from the evidence that the defendants were not registered as required by s. 4(1) of the *Collection Agencies Act*. The trial judge was satisfied that the Crown had proven beyond a reasonable doubt the elements of the fourth offence.

R. v. Lavoie, 2000 IIJCan 14437 (Qc. C.Q.)

Procedural Background

Lavoie pleaded guilty to one count of possession of a computer password contrary to s. 342.1 (1)d) of the Criminal Code and one count of counselling another to fabricate an explosive substance contrary to ss. 464 and 82(1). This is his sentencing.

Facts

Lavoie, with the help of two friends, published web sites called "Corruption Addicts" and "Phaust Laboratories". The first site was used to promote "hacking" and "phreaking".

The first site was used to publish passwords to access government sites, military or telecommunication organisations' sites. Intrusions where detected at various institutions. However, it could not be proved that they had been committed by the accused. On the other hand, the proof demonstrated a coincidence in time between these intrusions and the period where this site was active.

The second site was used to publish a recipe to make a "pipe bomb" with step by step pictures. Chemicals were found in the Lavoie's room. A notice posted on the site also demonstrated that Lavoie knew the recipe could be used for terrorism.

Lavoie claimed that discovering the passwords was a pastime and not meant to cause damages. The proof demonstrated that the affected sites had to change their password and notify their clients. Lavoie had since obtained employment with a financial institution.

Legal Issue(s)

1. What is the appropriate sentence?

Decision
The accused was sentenced to twelve (12) months imprisonment for each count, to be served concurrently in the community. The accused was also to be on probation for one year after his sentence. The court also imposed forfeiture of all electronic equipment seized. The equipment which was still in working condition was to be donated to an educational institution of Lavoie's choice. A victim surcharge of $50 was also imposed.

Reasoning
The court held that it could not attribute much credibility to Lavoie's assertion that he had been acting in good faith when circumventing the security of the sites. It noted that the electronic infrastructure will be the theatre of more and more criminal activity. These considerations led the court to pronounce a term of imprisonment as even though the damages caused cannot be readily quantified it is certain that some damage exists.

The court found that the publication of bomb recipe has a subversive connotation which constitutes an extreme danger to society by multiplying the possibilities of someone fabricating this type of bomb. It held that the gravity of the conduct requires denunciation and deterrence to ensure society's security.

R. v. Rodrigue, 2005 IIJCan 22261 (Qc. C.Q.)

Procedural Background
Rodrigue pled guilty to charges of fraud under $5,000 (s. 380), attempted fraud (ss. 463d)(i) and s. 380), possession of credit cards knowing that they were obtained by the commission of an offence in Canada (s. 342(1)c)e)), possession of a device intended for use in forging or falsifying credit cards (s. 342.01), possession of computer passwords (s. 342.1(1)d)), and fraud over $5,000 (s. 380).

Facts
Using the internet, Rodrigue obtained blank magnetic strip cards which he used to create debit cards using the financial information of account holders.

By claiming to have lost his debit card, Rodrigue obtained real debit cards. He then used a skimmer to overwrite the information on the card and was able to obtain approximately $60,000.00 from his frauds.

Legal Issue(s)
1. What is the appropriate sentence?

Decision
Rodrigue was sentenced to an 18 month conditional sentence, and a 36 month suspended sentence. Rodrigue was further sentenced to 200 hours of community service and to 36 months probation. Rodrigue was also ordered to make restitution in the amount of $970.00.

Reasoning
Rodrigue was 21 years old and did not have a criminal record. He had pled guilty on his first appearance in court. The chance of recidivism seemed small. The psychologist determined that he did not have a delinquent personality.

A joint submission was made for a conditional sentence, probation, community service and restitution in the amount of $970.00.

R. v. Rafuse, [2004] S.J. No. 737, 2004 SKCA 161 (Sask. C.A.)

Procedural Background
Mr. Rafuse pled guilty to one count of possession of counterfeit money (s. 450(b)) and one count of personation with intent to gain an advantage (s. 403(a)). He was sentenced to twelve months imprisonment with and order for forfeiture on count one and six months consecutive on count two. Rafuse appealed his sentence.

Facts
On May 4, 2004, Rafuse was a passenger in a car driven by Junaid Altaf. The car was stopped by the R.C.M.P. who conducted a consent search of Rafuse. The officer discovered approximately 5 counterfeit Canadian $100 bills in Rafuse's wallet. The search of the vehicle revealed another $1000 in counterfeit bills hidden in a suitcase. Rafuse denied knowledge of the money in the suitcase.

At the time of his arrest, Mr. Rafuse identified himself as one Emad Borhot. Mr. Borhot had lost his wallet some three years prior to the offence of personation. Mr. Rafuse acknowledged his real identity only when fingerprint evidence was presented. Rafuse was on probation at the time of the offence.

Legal Issue(s)
1. Is the sentence demonstrably unfit?
2. Did the trial judge err by failing to give Rafuse credit for time spent on pre-trial remand?

Holding
The appeal is partially allowed.

Decision
The sentence on count one, possession of counterfeit money, was vacated and substituted for 6 months imprisonment. The sentence for count two, personation, was not demonstrably unfit.

Reasoning
The court looked at the range of similar offences and found the appellant to be at the lower end of the scale, particularly because nothing connects him to the production of the counterfeit money and because of the small amount in his possession.

The court found the sentence to be demonstrably unfit given the amount in his possession, his lack of involvement in the production and the amount of time spent on pre-trial remand.

Civil Cases

Haskett v. Equifax Canada Inc., [2003] O.J. No. 771 (Ont. C.A.) (Q.L.)

Procedural Background

The appellant brought action against Equifax Canada Inc., Trans Union of Canada inc. and, their American parent companies. The appellant sought to get class action certification. The appellant's actions were struck out in a motion under Rule 21.01(1)(b) of the Rules of Civil Procedure, R.R.O. 1990, Reg. 194 as disclosing no reasonable cause of action. The motion dealt with three theories of liability. The appellant appealed the motion but limited his claimed cause of action to negligence.

Facts

In 1990, the appellant was obliged to make a voluntary assignment in bankruptcy when third parties breached their financial obligations to him. Both prior to and after his bankruptcy and discharge in 1996, the appellant had met all his financial obligations.

Since his discharge, the appellant had applied for and had been denied credit despite his uninterrupted earnings in excess of $75,000.00 annually and the fact that he had met all his financial obligations.

Legal Issue(s)

1. Can the action proceed at this stage as a claim in negligence?
2. If so, can the action, as pleaded, proceed against the two respondent American parent corporations?

Holding

The order of the motions judge was set aside and the appeal partially allowed. The claim against the American parent companies was struck out of the pleading.

Decision

The motion judge erred in concluding that it was plain and obvious that the appellant has no cause of action against the respondents in negligence. The appellant was allowed to proceed with the action against the Canadian respondents as a claim in negligence.

Statement of Rule

If it is not plain and obvious that no duty of care can be recognized, the action can proceed and the issue will be determined at a trial.

In order to found liability by a parent corporation for the actions of a subsidiary, there typically must be both complete control, so that the subsidiary does not function independently. The subsidiary must have been incorporated for a fraudulent or improper purpose or be used by the parent company as a shield for improper activity.

Reasoning

On a Rule 21 motion, the court applies the Anns/Kamloops two-stage test for determining if a duty of care exists and will found a cause of action. If it is not plain and obvious that no duty of care can be recognized, the action can proceed and the issue will be determined at trial. In that context, the court may well recognize potential policy concerns but should be circumspect in

using those policy concerns to determine, without a Statement of Defence and without any evidence, that it is plain and obvious that there is no cause of action.

The court determined that the relationship between a credit reporting agency and the consumer about whom reports are made is not the type of relationship which fits exactly into one of the recognized categories. However, the court found this situation to be analogous to the relationship that founds a cause of action for negligent misrepresentation and a prima facie duty of care. The analysis in *Hedley Byrne & Co. v. Heller & Partners Ltd.*, [1963] 2 All E.R. 575 (H.L.) can be applied to consumer reporting agencies.

In the first stage of the test, the judge found that it was reasonably foreseeable that if the respondents are negligent in the way they gather and report the information, and if they report inaccurate information, their actions could cause credit grantors to either deny credit or charge more than they otherwise would.

The court found that the policy considerations of the first stage of the test support a duty of care based on the fact that fairness to the consumer is a clear legislative imperative in the *Consumer Reporting Act*. This further supports the policy basis for recognition of a relationship of proximity and a duty or care on consumer reporting agencies to consumers about whom reports are made.

The court found that whether as an analogous category to negligent misrepresentation or as a new category, on the proximity analysis there is the basis to find a duty of care.

In the second stage of the test, the court rejected the motion judge's conclusion that to extend liability in this case "would create a serious risk of imposing liability in an indeterminate amount and an indefinite time to an indeterminate class" for three reasons: 1) the class of persons to whom the duty would be owed is wholly within the knowledge and control of the respondents; and 2) the timing of the potential harm and therefore of liability is not indefinite. If errors are corrected for future reports, then normally the adverse effect of the inaccurate report would be spent. 3) The amount of liability is also limited by the purposes for which the report is sought, which purposes the credit agency knows.

The court also rejected the motion judge's second policy issue that the plaintiff had recourse to alternate legal remedies via certain provisions for the *Consumer Reporting Act*. The court found that although potentially useful, these provisions should not bar recognition of a cause of action in damages. The court gave four reasons: 1) the provisions do not provide a remedy in damages; 2) the act does not provide for punitive damages, a remedy that can be useful in the context of class actions where one purpose of the action is deterrence of illegal conduct; 3) the appellant had pleaded the difficulties, expense and inconvenience of attempting to use the statutory procedures; and 4) at trial the parties will be able to lead evidence on the effectiveness of the statutory procedures.

The court also rejected the respondent's argument that recognizing this cause of action would be an encroachment on the law of defamation. The statutory prohibition in question is in respect of reporting certain information, which may arguably be viewed as true. In the defamation context, truth is a complete defence to an action. The cause of action in negligence could encompass reporting such arguably "true" information.

On the question of the action against the American parent companies, the court concluded that the pleading fell short of suggesting that the relationship of the respective related respondent

corporations constituted conduct to avoid liability. Nor was there an allegation that the parent company controlled the subsidiary for an improper purpose.

Bongeli v. Citibank Canada, [2004] O.J. No. 3272 (Ont. Sup. Ct. (Civ. Div.))

Facts

Mr. Bongeli was an employee of Minacs WorldWide Inc. ("Minacs") which provided consumer representative services to Citibank. On January 24, 2002 the defendant removed the plaintiff from its premises pursuant to its contract with Minacs. The defendant was removed from the premises following an investigation by the bank of alleged misconduct. The bank eventually forwarded the results of its investigation to Minacs and to the police. Minacs eventually terminated Mr. Bongeli's employment and the police proceeded to charge Mr. Bongeli with breach of trust. The charges were ultimately withdrawn.

The investigation conducted by the bank showed that Mr. Bongeli had made changes to the accounts of certain clients without them requesting the changes. It also found that he had failed to close some accounts when requested by consumers. The investigation found 12 accounts where Mr. Bongeli had made unauthorized changes. The computer system used by the bank tracked all changes made to accounts by logging which user made the change and what the nature of the change was, such as "change of address". The investigation also found that Mr. Bongeli made unauthorized changes to addresses and had requested additional cards for certain accounts.

Following an a review of the investigation, Bongeli was laid off by Minacs. He was provided with a severance package. Following his dismissal, Bongeli obtained employment with National Cheese. While he was still in a probation period, National Cheese laid him off because they had just lost a major client.

Bongeli was arrested the day he was laid off from National Cheese. When Mr. Bongeli was arrested he was found in possession of paper towels with the names of individuals and their personal information including credit card numbers, dates of membership, expiry dates, addresses, dates of birth, phone numbers and social insurance numbers. Mr. Bongeli also had the limit and balance of the line of credit of one of the individuals on which he had information.

Legal Issue(s)

1. Did the bank interfere with Bongeli's contractual relations at Minacs and National Cheese?

Holding

The action was dismissed.

Decision

The bank and its employees did not intend to cause any injury to Mr. Bongeli and neither of them interfered in his contractual relationship with Minics or anyone else.

Reasoning

The judge made the following findings of fact: 1) Mr. Bongeli had the knowledge and intelligence to use the bank's system to commit the alleged acts; 2) the suggestion that his terminal was left unattended and was used by others was rejected; 3) the information on the paper towels tended to implicate Mr. Bongeli in the dishonest action taken on certain accounts; 4) Mr.

Bongeli's evidence that part of the copy of his notepad is not a true copy was proven incorrect by the exhibits at trial; 5) the plaintiff's testimony that detective Maciek mentioned his criminal record to Mr. Murray was rejected; 6) Mr. Bongeli's belief that he was removed from the bank's premises because he complained of the unequal treatment of black people by the bank was rejected; and 7) Mr. Bongeli did have a criminal record for crimes of dishonesty and he was on probation when arrested.

The bank had proceeded with a reasonably careful investigation to determine whether or not he should be removed from the bank's premises as someone who placed at risk the integrity of its cardholders' accounts. The bank had a duty to ensure the confidentiality of its customers' accounts.

The bank's employees honestly and reasonably believed that Bongeli had committed unauthorized actions on the affected accounts that should be investigated by police through a complaint.

The court found that no one from the bank was involved when detective Maciek decided to lay charges or when he requested a detention order. The detention order was made by a judge, not the bank. The fact that the charges were withdrawn did not prove they were improperly laid. The decision by National Cheese to terminate Mr. Bongeli's employment was done with no input from the bank.

Furthermore, Mr. Bongeli did not suffer any damages since Minacs provided him with a two week severance package and in that time he obtained employment with National Cheese. Finally, although he was without income while in jail, the loss was not caused by the bank and there was no evidence of mental anguish or distress suffered by M. Bongeli while in jail that would have warranted an award for aggravated damages.

Clark v. Scotiabank, [2004] O.J. No. 2615 (Ont. Sup. Ct. (Civ. Div.))

Facts

On January 19, 1994 Mr. Clark applied for a personal loan which was denied because of an R-9 rating in his credit record. I-9 and R-9 ratings are the worst possible rating in a credit report.

Mr. Clark communicated with Equifax to determine the details of the rating. Equifax assured him the matter would be investigated and that, if there was in fact an error, his credit rating would be cleared up. Mr. Clark did not follow up with Equifax to find out if the rating was removed.

From 1994 to 2000, Mr. Clark sought and eventually obtained credit on different occasions. On many of these occasions, because of an R-9 rating in his credit record, he had difficulty obtaining credit.

On September 8, 2000 Equifax sent a confirmation request to Scotiabank to confirm whether the I-9 rating for the loan account number 100744275350 related to Mr. Clark. Scotiabank confirmed the loan was not attributable to Mr. Clark. Scotiabank requested and obtained a copy of Mr. Clark's credit report to make sure the erroneous rating was removed.

Legal Issue(s)

1. Did the defendants, Equifax and Scotiabank, owe Mr. Clark a duty of care with regard to his credit rating?
2. Did the defendants breach their duty of care?
3. Are the defendants liable for the psychological harm problems claimed by Mr. Clark?

Holding

The action was allowed.

Decision

Equifax and Scotiabank did owe a duty of care to Mr. Clark and had breached that duty. Damages in the amount of $5,000 were awarded against each defendant.

Statement of Rule

There is a relationship of proximity between a credit reporting agency and a person who is the subject of a credit report.

Reasoning

The court followed the decision in *Haskett v. Equifax Canada Inc. et al*, 2003 CanLII 32896 (ON C.A.) in finding that the defendants had a duty of care towards Mr. Clark.

The court found that the defendants had breached their duty of care when they failed to take reasonable care with his credit rating. As a result, Mr. Clark was entitled to compensation for the foreseeable harm suffered as a result of the negligence of both defendants.

The court found it difficult to find the defendants liable for the plaintiff's psychiatric harm for two reasons: 1) the evidence did not support his claim; rather it pointed to other sources for his psychiatric difficulties; and 2) Mr. Clark had failed to establish that his psychological problems were a foreseeable consequence of the defendant's negligence.

The court found that Mr. Clark suffered distress caused by the negligence of the defendants: Scotiabank for having caused the error which endured so long in the first place; and Equifax for having failed to clean up the mistake when it was first, then repeatedly, brought to its attention. The distress was clearly foreseeable by the defendants.

Policy

The court found that as matter of public policy, it is appropriate to find these parties to be in a relationship of proximity giving rise to a duty of care.

Anderson v. Excel Collection Services Ltd., [2005] O.J. No. 4195 (Ont. Sup. Ct. (Civ. Div,))

Procedural Background

Anderson was awarded $5000.00 in damages. This case was Excel Collection Services' appeal.

Facts
Mr. Anderson had given proper notice to terminate his tenancy and did not owe Excel's client, Azuria, the amount claimed.

In February, 2000, Mr. Bryant from Excel was informed that Mr. Anderson disputed the debt. In September 2002, Roger Lansing, an employee of Excel, called Mr. Anderson nine times using threatening and abusive language. Mr. Lansing communicated with Mr. Anderson's employer and communicated information beyond what he was entitled to discuss.

Legal Issue(s)
1. Did the Deputy Judge err in finding that Excel fell below the standard of care and was negligent, because it failed to comply with regulations under the *Collection Agencies Act*, R.S.O. 1990, c. C.14?
2. Did the Deputy Judge err in awarding damages for mental distress in the absence of any medical evidence or evidence of any physical or psychiatric injury?

Holding
The appeal was allowed.

Decision
The Deputy Judge had erred in awarding damages, the Deputy Judge's decision was set aside and the claim was dismissed.

Reasoning
The Deputy Judge had correctly stated that proof of a statutory breach which causes damages may be evidence of negligence. Given his findings about the nature of Mr. Lansing's calls and their frequency, he reasonably concluded that s. 20(d) of the regulation set a standard of reasonable behaviour and that, given the violation, Excel's conduct fell below the standard of care.

The Deputy Judge had made no finding that Excel *knowingly* provided false information to Equifax. In the absence of a finding that the report was made with knowledge that the information about the debt was false or provided without due care in determining whether the debt existed, there had been no breach of the standard of care in reporting the debt. The fact that the debt was subsequently found not to exist was not, on its own, sufficient to show dishonesty nor a breach of the standard of care.

The Deputy Judge had reasonably found that Excel fell below the standard of care in the contacts made with Mr. Anderson's employer.

While there was evidence of mental distress, there was no evidence of psychiatric or medical problems caused by Excel's conduct. In the absence of this evidence, the Deputy Judge had erred in awarding general damages for mental distress, despite his finding of negligence.

Policy
Mr. Anderson had done a public service in bringing this case in an effort to help define the standard of reasonable care applying to collection agencies. This was a case where no costs of the appeal should be awarded, given the conduct of Excel.

Craig v. Independent Order of Foresters, [2005] Q.J. No. 1387 (Qc. C.Q. (Civ. Div.))

Facts
On May 13, Mr. Craig was admitted to the Montreal Neurological Institute and was in a non communicative vegetative state. Subsequent to his admission, his wallet, containing his debit card and personal identification number (PIN), was handed to his son.

The plaintiff's son completed and filed with the defendant an "Application to Surrender Certificate". The son forged his father's signature on the application. The defendant's employee, Ms. Carluan, processed the request and issued a cheque for the amount of $10,422.03 payable to the plaintiff. The plaintiff applied the usual fees for this type of transaction. The cheque was later deposited in the plaintiff's bank account. The defendant's son then perpetuated the identity fraud by using the plaintiff's debit card to make frequent withdrawals.

Legal Issue(s)
1. What is the standard of care applicable to the defendant in regard to the handling of the plaintiff's investments?
2. Is the defendant liable of negligence in regard to the security of the plaintiff's investments?

Holding
The plaintiff's action was maintained in part.

Decision
The court found that the defendant was only liable for a charge of $635.16 deducted as a payment for the applicable surrender charges. The court awarded this amount since Ms. Carluan's fault was the effective cause of that part of the plaintiff's loss.

Statement of Rule
The standard of care in handling the plaintiff's investment is that of a prudent and diligent financial institution although the defendant is not a bank.

Reasoning
The court found Ms. Carluan was negligent in handling the plaintiff's account when considering the application was mailed and not brought in person and considering that the plaintiff had never made a withdrawal. The court found the omission to communicate with the plaintiff to validate the authenticity of his signature constituted a fault that engaged the defendant's liability pursuant to article 1463 C.c.Q.

The defendant pleaded that the plaintiff was responsible for his misfortune by keeping his PIN in his wallet. However, the court did not accept this submission. However, the court accepted that the actions of the plaintiff's son constituted a *novus actus interveniens* that severed the casual link between Ms. Carluan's omission and the plaintiff's loss.

National Bank of Canada v. Nugent, 2005 CanLII 20499 (Qc. C.Q. (Civ. Div.))

Facts

Nugent and Mrs. De Sève lived together. On November 21, 1995 Nugent filed an application for a credit card. The credit card was subsequently issued by the National Bank of Canada (NBC). All the monthly statements except the last four showed an applicable interest rate of 13.90% *per annum*. The last four show a rate of 26.00%. The rate was increased when Nugent became in default.

Nugent denied he ever agreed to a rate of 26.00%. He insisted that the credit card was under his control at all times. Nugent claims that after May 2002 Mrs. De Sève had used his credit card without his knowledge and consent.

When Nugent discovered the alleged unauthorized use, he immediately notified NBC in March 2003 and filed a complaint with the police against Mrs. De Sève for credit card fraud. Mrs. De Sève denied making any purchases without Nugent's knowledge and consent. She claimed it was understood between them that only the purchases made for her personal use had to be reimbursed by her. Over the months covered by the statements, all the payments made against the card were made by her in order to reimburse her personal purchases. Nugent admitted the payments came from her. All such payments amply covered her personal purchases.

Legal Issue(s)

1. Is NBC entitled to the amount claimed under the credit card agreement resulting from the Credit Card application executed by Nugent on November 21, 1995?
2. In the affirmative, is NBC entitled to claim the interest rate of 26.00% *per annum*?
3. Did Mrs. De Sève used the Credit Card unlawfully and, if so, must she indemnify Mr. Nugent and to what extent?

Holding

The NBC action was allowed in part. The action against Mrs. De Sève was dismissed.

Decision

The NBC was entitled to the amount claimed, $3,819.14 plus a $39.46 "Insurance 3" charge, with interest thereon at the rate of 13.90% *per annum* from September 21, 2003. The action in warranty against Mrs. De Sève was dismissed.

Reasoning

In the credit agreement, Mr. Nugent undertook to verify the monthly statements sent by NBC and notify the latter within 30 days of the date of each statement of any error or irregularity concerning the debits or credits appearing on each statement. The conditions stipulate that "After this 30-day period has elapsed (with the exceptions of errors or irregularities previously reported to the Bank), the Cardholder can no longer contest the balance recorded on the monthly account statement. Nugent failed or neglected to honour his obligations towards NBC.

The court noted that after March 10, only cash withdrawals were made against the card. In the absence of any evidence that the credit card had been duplicated, the court concluded the withdrawals could only have been done by Nugent. The court also noted that Nugent did not change his PIN number for the card after alleging the fraudulent use of his card. The court

concluded NBC is entitled to claim the various purchases and cash advances charged to the credit card.

Article 1617 of the Quebec Civil Code that damages are recoverable for the delay in performance of an obligation to pay a sum of money. The damages consist of interest at the agreed rate. The court found that NBC did not establish that 26.00% annual rate was the agreed rate. The court also rejected the argument that the rate could be changed verbally by way of a notice under article 129 of the Consumer Protection Act. The court also found that Nugent could not have given his consent to the raise as he did not make any payments since the rate increase. The court held that the agreed rate is 13.90% *per annum*.

The court held that it could not give any credence to Nugent's testimony which as highly emotional and inconsistent with the facts and realities stemming, *inter alia*, from the Statements. The court noted that many of the purchases were for gas and that Mrs. De Sève did not own a car. The court held that on the preponderance of evidence Mrs. De Sève's version is favoured.

Administrative cases

Kalombo v. Canada (Minister of Citizenship and Immigration), [2003] 4 F.C. 810 (T.D.)

Procedural Background
A removal order was made against Kalombo. He appealed that decision to the Immigration and Refugee Board, Appeal Division (IAD) who sustained the removal order. Kalombo sought judicial review of the Board's decision.

Facts
Between May 14, 1998 and March 14, 2001, Kalombo was convicted of approximately 11 criminal offences which were mostly fraud-related, including personation with intent contrary to s. 403(a) of the *Criminal Code*.

Legal Issue(s)
1. Is the removal order valid in law?
2. Should it be stayed having regard to all the circumstances?

Holding
The court dismissed the judicial review.

Decision
The court concluded that the IAD made no error in law or in jurisdiction or based its decision on an erroneous finding of fact.

Reasoning
The applicant argued that the removal order was instituted for purposes beyond the legislation. The applicant also argued that the removal order was illegal since it placed conditions on him. Third, the applicant argued that there was no intention to give effect to the removal order because Canada does not send refugees back to the Democratic Republic of Congo.

The court found that the deportation arose from the operation of law as the applicant was convicted of fraudulently impersonating a person with intent to gain an advantage for himself, a criminal offence under s. 403(a) of the *Criminal Code*. The act mandates that immigration officers forward a written report to the Deputy Minister setting out that the applicant has been convicted of an offence for which a term of imprisonment of six months has been imposed. The Deputy Minister must then decide if an inquiry is warranted. His decision is analogous to a prosecutor who decides to proceed with charges before the courts.

The only question for the adjudicator was whether the allegations against the applicant were true. The adjudicator had found them to be true and made a valid and lawful deportation order pursuant to the mandatory terms of the Act. The facts do not support the argument that the deportation order was made to place conditions on the applicant. The court concluded that the applicant's actions had given rise to the deportation order and that it was not issued to place conditions on the applicant.

As for the argument that the minister has no intention of giving effect to the order, the court found that the Act did not make the removal order contingent upon its execution or enforceability. The court also found that the validity of a removal order and the issue of where and when an individual will be removed are separate issues.

Arinze v. Canada (Solicitor General), 2005 F.C. 1547 (T.D.).

Procedural Background

Arinze was determined to constitute a danger to the public in Canada pursuant to p. 115(2)(a) of the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 (the Act). Arinze applied for a judicial review under s. 72 of the Act.

Facts

M. Arinze had committed approximately 14 Criminal Code offences since being designated a permanent resident. Arinze was convicted of 28 offences since 1994. These offences include personation, the use of fraudulently obtained credit cards and other means.

As a result of the convictions, a deportation order was issued on June 11, 1998. This order was subsequently stayed for 5 years. In November 2003, the applicant was informed of the intention of local officials to seek an opinion from the Minister that he was a danger to the public, which could result in his removal from Canada. Such an opinion was issued on December 1, 2004.

Legal Issue(s)

1. Did the Minister's delegate err in finding the applicant was a danger to the public in Canada?
2. Did the Minister's delegate fetter his discretion and absent all the facts, unfairly reached a decision?

Holding

The application for judicial review was dismissed.

Decision

1. The evidence was sufficiently reliable to warrant the conclusion that Mr. Arinze was a danger to the public in Canada.
2. Mr. Arinze had failed to illustrate that the Minister's delegate improperly exercised his discretion, or made any reviewable error.

Statement of Rule

To support the issuance of a danger opinion, the individual must be inadmissible on the basis of serious criminality and he or she must, in the opinion of the Minister, constitute a danger to the public in Canada.

Reasoning

A resident is inadmissible for having been convicted of an offence for which a term of imprisonment of more than six months has been imposed. Arinze's convictions included one in which a term of more than six months was imposed; this fulfills the serious criminality requirement.

The Minister's delegate took into consideration the nature and frequency of the crimes committed, and their serious effect on the Canadian Public. The absence of violence was also considered. The decision maker is presumed to have considered all the evidence unless the contrary can be shown.

PIPEDA cases

PIPEDA Case Summary #116, Customer withdraws consent but continues to receive promotional materials, 2003 CanLII 42249 (P.C.C.)

Facts

The complainant had written to her bank, on two occasions, to opt out of receiving promotional materials from the bank. The bank acknowledged both requests in writing. After 7 months, she received another solicitation for a credit card from the same bank.

Investigation

The bank explained that the error occurred because it had two files for the complainant in its computer system. One was under her first and last name and the second file included her middle name.

The bank modified both files to reflect that she withdrew consent to receive solicitations. The bank was also upgrading its systems so that all combinations of names and addresses will be matched to a single person.

Findings

The complainant provided reasonable notice of the withdrawal of her consent, which was acknowledged. The bank did send her a further solicitation.

The bank was in contravention of Principle 4.3.8 which provides that individuals can withdraw consent. The bank was also in contravention of Principle 4.5 for using her information without her consent for purposes other than those for which it was collected.

PIPEDA Case Summary #121, Bank employee uses customer's information to commit fraud, 2003 CanLII 33645 (P.C.C.)

Facts
A bank employee used a customer's name and telephone banking password to enrol the customer in Internet banking. Using the Internet banking, the employee changed the account's mailing address and ordered cheques for the customer's line of credit. The employee then used several of these cheques.

The bank, upon notification by the client, closed the account, cancelled the debt and offered a monetary settlement which was refused.

Investigation
The bank discovered which employee had committed the fraud and dismissed him. The bank acknowledged that despite its best efforts, the possibility remained that a determined individual with criminal intent would be able to circumvent security measures.

Findings
The bank did not dispute that an employee used the personal information without knowledge or consent. However, the bank is responsible for the behaviour of its employees and as such it was in contravention of Principle 4.3, which requires knowledge and consent, and of Principle 4.5 which requires information to be used only for identified purposes to which the individual consented.

Considerations
The Commissioner noted that the bank's monetary offer was appropriate in the circumstances. The Commission agreed with the bank that no security system, no matter how sophisticated and effective, may ever completely eliminate the possibility of such an act.

PIPEDA Case Summary #177. Bank leaves computer logged on in public area; customer obtains sensitive personal account information without password, 2003 CanLII 38271 (P.C.C.)

Facts
While waiting at a kiosk branch, the complainant noticed a computer terminal in an open area. She thought it was a public terminal and keyed in her name and address. The computer displayed a screen containing her account information. Since she was not asked for a password, she was concerned. After that, she saw the bank's employee entering his password. She claimed the password appeared in clear text.

Investigation
The bank explained the incident as an employee error. Such neglect was a breach of the bank's security policy. As for the password being entered, the bank suggested the complainant mistook the username with the password. Both are required; the username appears in clear text while the password appears in symbols (*). The bank installed a new screen saver that locks the computer after 15 minutes of inactivity.

Findings

The bank, by installing computers in open areas, had created a considerable risk of unauthorized access to customer's sensitive personal information. The safeguard, a directive in a security manual to log off, upon which the bank relied, was neither effective nor appropriate for protecting the customer's sensitive personal information.

The Commissioner noted that the measure taken, i.e. the screen saver, was not an adequate safeguard since access would still be possible in the 15 minute timeframe before the computer is locked. It might even incline employees toward non compliance with the rule that requires them to always log off before leaving a computer.

The bank remains in contravention of Principle 4.7 which requires appropriate security safeguards for personal information.

PIPEDA Case Summary #292, Former employer changed account information of Air Canada frequent flyer member, 2005 CanLII 15494 (P.C.C)

Facts

An individual complained that Air Canada, which at the time owned and operated Aeroplan, had disclosed his personal information without his knowledge and consent. The complainant traveled frequently when working for his former employer. The travel agency used by that employer had the complainant's Aeroplan account number on file.

On one day, the complainant received a duplicate copy of his last Aeroplan statement in the mail, which he had not ordered. He contacted Air Canada and an agent informed him that it had been requested and the cost of processing had been applied against a credit card. The agent informed him that a week earlier someone had called requesting information on his travelling and had paid for the duplicate. The caller had also changed the email address in his account to that of the former employer.

The complainant spoke to security and was advised to contact police. The police investigation concluded that it could not charge the former employer since he had not misrepresented himself or pretended to be the complainant.

The former employer readily admitted that he had obtained information about the complainant's travel itinerary from Aeroplan's computerized telephone system. Air Canada confirmed this was feasible as no personal identification number was required.

Investigation

The Privacy Commissioner assistant determined that at the time of the incident, it was possible to obtain, via the computerized telephone system, travel information for the last five travel transactions in the Aeroplan account.

It would not have been possible to change the email address. When speaking to an agent, the agent was supposed to ask the caller to confirm other information on the account file, or if the account was password protected, to ask for the password, in order to authenticate the caller.

The transaction records confirmed that the email address had been changed to that of the former employer and that a $10.70 fee was paid for the duplicate statement.

The agent who made the change could not remember receiving any specific privacy training. She indicated that if given a credit card number different from the one on file "a light would go on" but did not remember this happening.

It was determined that no name for the credit card holder was required to be placed on file at that time; the billing was against the card number. The lead supervisor stated that the changes made to the complainant's account would not be considered normal procedure.

Findings

- The former employer obtained information without misrepresenting himself.
- The Commissioner's assistant did not believe that having account information readily available, without any protection on it, constituted an adequate safeguard.
- The former employer did provide his name when giving his credit card number but the agent was not concerned she was not speaking to the account holder. She did not even seem aware of the importance of maintaining the confidentiality of personal information.
- There was a clear lack of diligence on the part of Air Canada with respect to its handling and protection of customers' personal information. The company did not have adequate safeguards in place for its teleprompt system, and while it might have had some protections when a caller spoke with an agent, the agent did not follow them in this case.
- The complainant's personal information was disclosed without his knowledge or consent. Thus Air Canada is in contravention of Principles 4.7, 4.7.1, and 4.3.
- Air Canada did not direct the complainant to its internal mechanism for dealing with privacy complaints even though the company had a privacy officer and procedures in place.
- The most serious privacy breach occurred when the agent was speaking to the former employer. There is no evidence that anyone in the company addressed this issue with the agent.

PIPEDA Case Summary #300, Company collecting consumer personal information without identifying purposes halts practice and implements privacy policies and practices, 2005 CanLII 27662 (P.C.C.)

Facts

An individual complained that a company was collecting personal information of consumers without consent and without identifying the purpose for the collection and use of the information.

After unpacking a product the complainant noticed a label stating "For important product information call before using". When he called, an automated attendant asked him to provide the model number, his name, address, home and work telephone numbers, his employer's name, and where he had purchased the unit.

Investigation

Following the complaint, the company removed the labels on its products. It did so because it could not reasonably be assured that the information would be handled in accordance with Canadian privacy legislation; the information was sent to a U.S.-based company.

As for existing products and labels on store shelves, the company indicated it would not collect the personal information of callers. The company also implemented a privacy policy and designated a privacy representative.

Findings

- The company was trying to collect personal information without identifying its purposes contrary to Principles 4.2 and 4.4.
- The company did not have a privacy policy, in contravention of Principles 4.1 and 4.1.4(d).
- The company did not follow up with the complainant when he contacted it.
- The company made necessary changes to comply with the *Personal Information Protection and Electronic Documents Act*.
- The Assistant Commissioner concluded the complaint was resolved.

APPENDIX B – U.S. CASE BRIEFS

Federal Trade Commission cases

FTC v. Seismic Entertainment, Inc., No. 04-377-JD, 2004 U.S. Dist.

This case was a default judgement, permanent injunction, and equitable relief against Seismic Entertainment, Inc. (Seismic).

Seismic had engaged in unfair acts or practices in violation of s. 5 of the *Federal Trade Commission Act*, 15 U.S.C. § 45(a) in connection with their marketing and distribution of software to consumers. The unfair practices the defendants engaged in consisted of marketing and downloading software to consumers' computers. The software in question included "Spy Wiper" and "Spy Deleter" which the defendant purported to be "anti-spyware" software.

The defendants controlled and operated a network of web sites including, but not limited to, www.default-homepage-network.com, downloads.default-homepage-network.com, www.passthison.com, and www.smartbotpro.net ("the sites"). This network was used to download software to consumers' computers that exploited vulnerabilities in Microsoft's Internet Explorer ("IE") web browser.

The defendants lured unsuspecting consumers to their websites by disseminating banner, pop-up, and other online advertisements that automatically re-directed computers to the sites when viewing these advertisements.

The software installed on consumers' computers "hi-jacked" their home page, i.e. changed the browser's default home page to point to sites controlled by the defendants. When the browser was launched, the defendant controlled websites launched a series of pop-up advertisements, including full-page advertisements, and other web pages, which prevented consumers from visiting their intended websites.

These advertisements included advertisement for the "Spy Wiper" and "Spy Deleter" applications to induce their purchase. The advertisements warned consumers that they must purchase the advertised software immediately to resolve the computer problems the defendants created. The defendants compelled consumers to either spend $30 to purchase their products or otherwise spend substantial time and money to resolve the problems with their computers that the defendants had caused.

The defendant's software also exploited vulnerabilities in IE to change the browser's default search engine. The software also exploited vulnerabilities in IE to download and install spyware, advertising delivery software and other software programs to consumers' computers without their authorization or consent. The software installed also created security holes through which other software programs and malicious code could be downloaded and executed on the consumers' computers.

The consumers whose computers were affected also received a stream of advertisements and had their computers' memory and resources depleted. This caused computers to malfunction, lose important information, operate more slowly and in some cases, cease to work completely.

To regain control of their IE web browser, consumers had to exit IE and change the settings for the home page to their original home page and for their default search engine. Consumers often had to repeat this process. The consumers could not reasonably avoid this substantial injury because the defendants exploited security vulnerabilities to download and install software. The court held that the defendants' practices did not benefit consumers or competition.

The defendants also generated revenue through exploiting security vulnerabilities in the IE web browser to market products on the behalf of others. They earned at least $4,089,550.48 in revenue from their unlawful conduct. The defendants were jointly and severally ordered to pay $4,089,550.48 for disgorgement to the FTC. The FTC was directed to use the funds for equitable relief, including consumer redress and consumer information remedies.

The defendants were enjoined from publishing or otherwise distributing on or through the Internet, the World Wide Web or other electronic means, any software, script or code that exploits a security vulnerability of any computer operating system, web browser or other application to download or install onto any computer any software, script or code.

They were further enjoined from 1) downloading any software program without express consent; 2) redirecting computers to different web sites other than those that the consumer selects to visit; 3) changing or causing to change any web browser's default home page or default search engine.

The Commission was also authorized to monitor compliance with the order.

FTC v. Odysseus Marketing, Inc., No. 05-CV-330-SM

This case was a preliminary injunction against Odysseus Marketing Inc. for having likely engaged in acts and practices which violate Section 5(a) of the *Federal Trade Commission Act*, 15 U.S.C. § 45(a). The court considered the preliminary injunction in the public interest.

The injunction prohibited the defendants from:

- Distributing or publishing on or through the Internet, the World Wide Web or other electronic means of distribution, any software, script, code or other content that exploits a security vulnerability or any computer operating system, web browser, or other application to download or install onto any computer any software code, program, script or content.
- Selling, renting, leasing, transferring or otherwise disclosing personally identifiable information of any person from whom the defendants obtained such information.
- Benefiting from or using any personally identifiable information of any person from whom the defendants obtained such information.
- Further obtaining any personally identifiable information of any person.
- Making representations that their software program makes users of peer-to-peer file-sharing programs anonymous.
- Distributing or causing consumers to download or install software that (a) displays any advertising; (b) modifies any web browser or operating system software; or (c) collects personally identifiable information or passwords unless the defendants clearly and conspicuously disclose the effect that downloading such software would have on consumers' computers.

- Distributing or causing consumers to download or install software without providing a reasonable and effective means to uninstall such software program.
- From deleting, modifying, altering, or replacing files contained in the System32 folder of any Microsoft Windows operating system.

The injunction mandated that the defendants would:

- Provide to counsel for the commission a software utility that is effective in uninstalling all files, registry keys, and components that such programs download and install to the computer.

In the Matter of Advertising.com, INC. (File No. 042-3196)

This case was a settlement between the Federal Trace Commission (FTC) and the respondents. Advertising.com made representations which were considered deceptive trade practices by the FTC under Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

This settlement did not constitute an admission by the respondents that the law has been violated as alleged in the complaint, or that the facts as alleged in the complaint, other than jurisdictional facts, are true.

The respondents were prohibited from making representations regarding SpyBlast or any other executable computer software programs whose principal function is to enhance security or privacy. They were required to maintain and make available for five years all advertisements and promotional materials containing the representation.

John Ferber, for a period of ten years, must notify the FTC of the discontinuance of his current business or employment, or of his affiliation with any new business or employment.

This order terminates in twenty years from the date of its issuance.

Criminal cases

United States v. Sample, No. 99-3475 (8th Cir., May 31, 2000)

This case was an appeal of a sentence following a guilty plea for one count of credit card fraud contrary to 18 U.S.C. § 1029(a)(2).

Sample perpetrated her scheme by procuring personal information about her roommates, casual acquaintances, visitors, and individuals whom she met through other friends. The information included Social Security Numbers, dates of birth, addresses, and physical descriptions. Sample used the information to open various bank accounts, to secure credit cards, and even to establish false driver's licences in the names of the victims. She also wrote cheques and withdrew money from her fraudulent bank accounts. She also visited a health centre to obtain a prescription in Kery Shirk's name which resulted in her medical records being altered.

Sample "guesstimated" to an agent of the Secret Service that she had either caused or intended to cause her victims to lose a combined amount in excess of $70,000. In the plea agreement, the parties agreed the total amount of actual and intended loss fell between $40,000 and $70,000.

At sentencing, the district court held that an upward departure was warranted based on the degree of psychological harm that Sample inflicted upon her victims. The district court also rejected the amount of loss in the plea agreement and adopted an amount consistent with Sample's statement to the Secret Service.

Sample contended that the district court had failed to afford her proper notice that it had been considering a departure from the applicable sentencing range. Rule 32 of the Federal Rules of Criminal Procedure requires a district court to provide a defendant notice if it intends to depart upward from a defendant's prescribed sentencing range. Inclusion in a pre-sentence report (PSR) of specific grounds that may form the basis for an upward departure satisfies Rule 32's notice requirement. In this case, the PSR indicated that departure may be warranted pursuant to U.S.S.G. § 2F1.1.

Sample argued that the district court had departed on the basis of extreme psychological injury as stated in U.S.S.G. § 5K2.3 and not U.S.S.G. § 2F1.1 and that as a result she had received insufficient notice. After reviewing the record, the court rejected the argument and concluded that the district court based itself on Application Notes 11 and 12 of U.S.S.G. § 2F1.1.

Next, Sample argued that the district court had erred when it decided to upwardly depart. According to the court, departure is appropriate only in extraordinary cases where there exists an "aggravating or mitigating circumstance of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission in formulating its guidelines. Section U.S.S.G. § 2F1.1 specifically encourages an upward departure whenever the amount of loss fails to capture the harmfulness and seriousness of the conduct. However the court held that the district court's departure was a factor not taken into account by an applicable Guideline.

After reviewing the record, the Court of Appeals concluded that more than enough evidence existed for the district court to find that Sample had caused her victims to suffer sever emotional distress and trauma.

Sample argues that even if the district court had discretion to impose an upward departure, it erred when it sentenced Sample to 30 months in prison. The Court of Appeals found that the district court's decision to issue an upward departure of nine months was more than reasonable under the circumstances of this case.

Sample argued that the district court had erred when it had rejected the amount of loss stipulation in her plea agreement. The Government bears the burden of proving the amount of loss by a preponderance of evidence. The district court had found that the detailed statements that Sample gave to the Secret Service were more credible. Hence the decision was based on witness credibility which is practically unreviewable on appeal.

The district court's judgement was affirmed.

United States v. Karro, No. 00-1565 (2nd Cir., Jul. 13, 2001)

This was an appeal by Karro of her conviction and sentence, following her guilty plea for twelve counts of mail fraud in violation of 18 U.S.C. § 1341. Karro made fraudulent credit card applications using the names and social security numbers of others.

When Karro pleaded guilty, she had attested that she was satisfied with her counsel's representation, had reviewed and understood the charges, understood the rights she was waiving, understood the applicable range of penalties, had discussed the guidelines with her counsel and knew that her guideline range could not be determined until her sentencing proceeding, and had reviewed and fully understood the consequences and terms of the plea agreement, including its binding nature.

Karro argued that the district court had erred in denying her motion to withdraw her guilty plea, and in upwardly departing. The court noted that "as a general matter, a defendant has no absolute right to withdraw a plea of guilty. When a motion to withdraw a plea of guilty is made before the imposition of a sentence, the court "may" grant the motion if "the defendant shows any fair and just reason." The district court should examine the amount of time elapsed between the plea and subsequent motion to withdraw.

The court held that since the defendant had conceded both at her plea allocution and in her papers seeking withdrawal of the guilty plea that she had intentionally performed the offence conduct charged in the indictment, and since the district court had properly determined that the defendant had not advanced a legally cognizable defence to the mail fraud charges, it had not been an abuse of discretion to hold the defendant to her guilty plea.

On the date of sentencing, July 16, 1999, the Sentencing Commission had not yet implemented the changes required to the sentencing guidelines by the *Identity Theft Assumption and Deterrence Act of 1998* (ITADA), Pub. L. No. 105-318. Karro contended that this failure to act indicated in fact "that the Commission has specifically forbidden departures based upon… features relating to identity theft."

The court held that the district court's upward departure had been based on an "encouraged" factor as explained in the Application Notes. These factors let a court upwardly depart when the fraud "risked reasonably foreseeable, substantial non-monetary harm" (U.S.S.G. § 2F1.1, app. note 11(a).

The Court of Appeals found that the district court had been right in determining that guidelines prior to the passage of ITADA did not take into account the type of non-monetary harms that identity theft like Karro's risks imposing on the individuals whose identities are stolen.

Karro contended that there had been no evidence before the district court of non-monetary harm to any victim, and that this "potential harm", with no other evidence to support it, was insufficient as a matter of law to justify an upward departure. The court held that the offence conduct in pre-sentence report and alluded to by the defendant, clearly gave the district court a sufficient basis to find a risk of substantial harm to those individuals.

Judgement of conviction and sentence were affirmed.

United States v. McNeil, No. 02-30138 (9th Cir. Feb. 26, 2003)

This was an appeal from a conviction of one count of bank fraud (18 U.S.C. § 1344(2)) and one count of wire fraud (18 U.S.C. § 1343).

In October 1999, McNeil opened a post office box in Montana under his own name. His application authorized Ian P. Doe and Jason Kimionakis to receive mail there, but neither could retrieve mail without a key from McNeil. McNeil also obtained a Montana driver's licence in the name of Ian P. Doe bearing his own photograph. In March 2000, McNeil opened an account with $400 in Doe's name using the driver's licence and Doe's social security number.

McNeil then tried to get a wire transfer from the "Doe" account to a bank in Massachusetts, that ultimately failed for lack of complete information. In 2001, while in prison in New Hampshire, McNeil typed and signed a tax return requesting a tax refund of $4,788. McNeil filed the tax return with the IRS in the name of Ian P. Doe.

A search of McNeil's house yielded a bank card in the name of Doe, an envelope addressed to Doe at the Montana post box, handwritten notes with Doe's social security number, date of birth and address, and an envelope from the Montana state DMV addressed to Jason Kimionakis.

The jury heard evidence that the IRS refund necessarily crossed state lines over the phone lines and that McNeil had access to a type writer while in prison.

McNeil contended that his conduct did not fall within the scope of § 1344(2) and that he had lacked the requisite specific intent required by that section. McNeil also contended that the evidence for the wire fraud conviction was insufficient.

The Court of Appeals found that section § 1344(2) is broader than § 1344(1) in that it criminalizes schemes to obtain money or property in the custody or control of a bank by deceptive means. Even if McNeil's ultimate goal was to obtain funds from the IRS, bank fraud charges may lie even if the bank is not the immediate or sole victim of the defendant's conduct. The court found that the scheme to deceive the bank was essential to McNeil's overall plan and the bank was not merely an unwitting instrumentality of the scheme but a victim of McNeil's deception. The court also found that Congress had not intended to limit the reach of § 1344(2) to cases in which a bank is put at risk of a loss.

The Court also held that specific intent is established by the existence of a scheme which was reasonably calculated to deceive persons of ordinary prudence and comprehension. The evidence was sufficient to establish that McNeil had acted with the intent required by that section.

McNeil argued that the government had not offered evidence of how he could have obtained or created the false W-2 form that was filed with the "Doe" tax return, and that, based on this lack of evidence, his conviction should be overturned.

Wire fraud has three elements: 1) a scheme to defraud; 2) use of wires in furtherance of the scheme; and 3) the specific intent to defraud. McNeil had filed a false IRS return in Doe's name that requested that an electronic refund be sent to the "Doe" account. This evidence suffices to meet the government's burden regardless of whether the government was able to show how the W-2 form was obtained or created.

The conviction was affirmed.

United States v. Mejìa-Barba, No. 02-3216 (8th Cir., May 5, 2003)

This was the appeal of Mr. Mejìa-Barba's sentence for illegally re-entering the United States after being deported. Mr. Mejìa-Barba appealed on the basis that the District Court had erred by finding that his conviction in Iowa for Identity Theft qualified as an aggravated felony, which had provided the basis for an eight-level enhancement of his sentence.

Mr. Mejìa-Barba was arrested for falsely representing himself as Marcos Rivera to a Department of Transportation investigator. Mr. Mejìa-Barba showed the inspector a birth certificate and a Social Security card in Rivera's name. Mr. Mejìa-Barba had also used Mr. Rivera's identity to obtain employment. The state of Iowa charged, convicted and sentenced Mr. Mejìa-Barba to a suspended term of imprisonment, and the INS deported Mr. Mejìa-Barba to Mexico. Mr. Mejìa-Barba subsequently re-entered the United States and was discovered while trying to renew his employment card.

Mr. Mejìa-Barba pleaded guilty to one count of unlawfully being in the United States after being deported. The pre-sentence report treated the conviction for identity theft as an aggravated felony. In a hearing Mejìa-Barba argued that his conviction for identity theft was not an aggravated felony. The district court denied his motion and held that Iowa's crime of identity theft fits within the parameters of the definition of a "theft offence" defined in the Sentencing Guidelines 8 U.S.C. § 1101 (a)(43)(G).

The Court of Appeals looked *de novo* at the district court's interpretation of the Sentencing Guidelines. The court found that § 1101 (a)(43)(G) includes as a definition of aggravated felony, "a theft offence or burglary offence for which the term of imprisonment is at least one year." The court of appeals held that Iowa's statutory scheme describing identity theft offences in general, and identity theft specifically, reflects that identity theft is an aggravated felony "theft" crime under the federal statute.

First, Iowa statute § 714.1 makes it a crime to take the property of another, and also to use that property without the owner's permission. § 714.1(3) defines theft as obtaining "the beneficial use of property of another, by deception" and finally § 714.1(10) states that theft is "any act that is declared to be theft by any provision of the Code".

Second, the Iowa identity theft statute includes many of the same considerations and considering these two statutes together, it is apparent that the Iowa legislature intended that identity theft, by its name and by its description, be a more specific type of theft crime.

Mejìa-Barba also argued that his actions constituted fraud and not theft. The court held that though, his actions were fraudulent, they were also theft under the Iowa statute. The court dismissed the appeal.

United States v. Stovall, No. 02-1210 (6th Cir., Jun. 13, 2003)

Stovall appealed her 77 months sentence, imposed pursuant to her guilty plea to charges of bank fraud and conspiracy. Stovall argued that the court made prejudicial error by failing to make explicit findings when rejecting her objections to her pre-sentence report (PSR). She also contended that some of her prior criminal activity had been double-counted in her criminal history score.

Stovall and 19 co-defendants were charged with conspiracy, forgery, identity theft, credit fraud and bank fraud. In exchange for an appropriate sentence and the dismissal of other charges, Stovall had agreed to plead guilty to bank fraud and conspiracy. Stovall agreed not to appeal any of the sentencing calculations.

In the plea agreement, the Government agreed that a sentence of no more than 51 months was appropriate. The PSR on the other hand calculated a sentence in the range of 77 to 96 months. Stovall had presented 23 objections to the PSR. The district court offered her to renegotiate or to withdraw her plea agreement. Following a recess, the parties agreed to amend the plea agreement by establishing a sentencing "cap" of 77 months. Without further discussion, the district court overturned Stovall's objections and imposed a sentence of 77 months.

Rule 32(c)(1) of the Fed. R. Crim. P. provides that "for each matter controverted [in objection to a PSR], the court must make either a finding on the allegation or a determination that no finding is necessary because the controverted matter will not be taken into account in, or will not affect, sentencing. Rule 32 requires "literal compliance" which means the district court must make independent factual findings and not merely adopt the findings in the PSR.

Stovall contended that Rule 32 was violated when the district court summarily overruled four objections to the PSR: 1) that because she had worked closely with only one of her co-defendants and had no knowledge of the others' activities, her role had been over-stated; 2) the enhancement of her offence level for the commission of an offence while release on bond; 3) the assessment of criminal history points for sentences imposed in earlier federal cases; and 4) her requests for a downward departure.

As for the first objection, Stovall had stipulated in her plea agreement that a three-level enhancement was appropriate because she was a manager or supervisor. In light of the stipulation, the district court did not have to make a finding on the issue.

The court held that Stovall had never disputed the fact that the period in which the offences were committed overlapped the period in which she was on bond. Given the overlap, the enhancement was *mandated* by U.S.C. § 3147.

As for the criminal history objection, the court held that Stovall had not raised this argument in the district court and that she had expressly agreed not to appeal any of the stipulated sentencing factors, thereby waiving her right to appeal the two-point addition.

Finally, the court held that Stovall's departure requests were not "objections to the PSR" within the meaning of Rule 32(c)(1). The report set forth the requests without comment, as a result, the district court was not obligated to make express findings with respect to the requests.

The sentence imposed by the district court was affirmed.

United States v. Banks, No. 02-16866 (11th Cir., Oct. 20, 2003)

This was an appeal by Mr. Banks of a sentence enhancement for obstruction of justice. On August 8, 2001, Banks was arrested after he posed as Bruce Lester and accepted the delivery of 10 fraudulently purchased computers. At the time of arrest he identified himself as James

Wyckoff III and provided a Michigan identification card bearing that name. Banks also possessed a fake New Jersey driver's licence issued to Bruce Lester but with Banks' photo.

Later that day, Banks was released on a $5,000 bond under the name James Wyckoff III. On October 12, 2001 a bondsman informed the secret service that James Wyckoff III was in fact Banks and that he had been arrested in Georgia while committing identity theft and credit card fraud.

The pre-sentence report recommended the two-level sentence enhancement for obstruction of justice because "during the course of the investigation of the instant offence, the defendant provided a materially false statement to a law enforcement officer… that was intended to significantly obstruct or impede the official investigation."

Banks argued that the false name and identification provided at arrest did not significantly obstruct either the investigation or the prosecution of his offence.

The Court of Appeals found that the district court had made no finding describing how the investigation or prosecution of the offence would have been helped or hindered by the defendant giving truthful identification at the time of arrest and during pre-trial periods. The district court should note specifically what each defendant did, why that conduct warrants the enhancement, and, if applicable, how that conduct actually hindered the investigation or prosecution of the offence.

The Court of Appeals held that it is not enough for the sentencing court to adopt the uncontested parts of the PSR and recite its agreement with the arguments of the prosecutor and the recommendations of the PSR.

Banks' conduct at arrest could not support an obstruction of justice enhancement without a finding that the conduct actually resulted in a significant hindrance to the investigation or the prosecution of the offence. Neither the intent nor the potential of evading investigation or prosecution could constitute a significant hindrance because the application notes explicitly stated that the conduct must have "actually resulted" in a hindrance.

To show hindrance, the prosecutor must show how it fruitlessly spent investigation or prosecution resources because of the untruthfulness. In other words, the prosecutor must show what action it took that it would not have taken had the identity of Banks been known at the time of the arrest.

The case was remanded.

United States v. Vieke, No. 02-30232 (9th Cir., Nov. 3, 2003)

This was an appeal by the United States of a sentencing decision. Ms. Vieke had been sentenced to five years probation and ordered to pay $51,536.37 in restitution for pleading guilty to one count of identity theft (18 U.S.C. § 1028(a)(7). Vieke had been responsible for fraudulent charges in the amount of approximately $50,000.00 in her parents' names.

At sentencing a downward departure for aberrant behaviour had been granted. Aberrant behaviour is defined as "a single criminal occurrence or single criminal transaction that (A) was

committed without significant planning; (B) was of limited duration; and (C) represents a marked deviation by the defendant from an otherwise law-abiding life."

The Government contended that the district court had failed to make, and a reasonable reading of the record failed to support, any findings with respect to the first two elements. The Government argued that the scheme to obtain multiple credit cards to manage her revolving debt required substantial planning. The government also argued that the scheme lasted for years, from 1997 to 2001.

The Court of Appeals declined to exercise its discretion to review the Government's unpreserved legal issues on appeal under the plain error standard. Neither the particular requirements of the Sentencing Guidelines that the Government asserted on appeal, nor the application of the facts to those requirements were raised for consideration by the district court.

The long standing rule in this and other circuits is that claims of error generally will not be considered if they are raised for the first time on appeal.

The sentence was affirmed.

United States v. Peyton, No. 02-50482 (9th Cir. Dec. 32, 2003)

Peyton was tried and convicted of access device fraud (18 U.S.C. § 1029(a)(1) and (2)) and sentenced to 15 months imprisonment. Following a successful appeal, in which six of the eight counts were reversed, Peyton was re-sentenced to 30 months.

Peyton appealed the sentence on three grounds: 1) the district court had acted vindictively by doubling the sentence; 2) the district court had applied an improper evidentiary standard to evidence supporting sentencing factors; and 3) insufficient evidence existed to apply the sentencing enhancement for accountable loss, obstruction of justice, and abuse of a position of trust.

Peyton fraudulently procured American Express credit cards in the name of fellow postal workers which she used to obtain goods. Peyton, like other supervisors, had access to the names and social security numbers of fellow employees. The brother of Peyton's roommate served as an administrative assistant with the United States Navy. He also had access the naval personnel information. From July 1999 to September 1999 the social security numbers of six naval officers were used to apply for American Express cards that were delivered to Peyton's address.

At re-sentencing, the district court applied a two-level enhancement for more than minimal planning and a two-level enhancement for abuse of a position of trust, and denied Peyton's request for a minor role downward departure. The district court applied the preponderance of evidence standard and determined that there was sufficient evidence to attribute the entire loss of $67,355 to Peyton. The district court reversed its prior ruling and applied a two-level enhancement for obstruction of justice. However, the court did not provide an explanation as to why the enhancement was appropriate now and was not earlier.

Whenever a judge imposes a more severe sentence upon a defendant in a new trial, the reasons for his doing so must affirmatively appear. If no explanation is present, a presumption arises that a greater sentence has been imposed for a vindictive purpose. This presumption must be rebutted

by objective information. The presumption only arises in cases where "there is a 'reasonable likelihood' that the increase is the product of actual vindictiveness on the part of the sentencing authority. If the presumption does not apply, actual vindictiveness must be proved by the defendant.

Because the district court's reasons for attributing a greater amount of loss to Peyton affirmatively appear in the record, no presumption of vindictiveness exists. Peyton had failed to prove actual vindictiveness.

The district court had failed to provide reasons for applying the obstruction of justice enhancement which raises the presumption. The Government had failed to rebut the presumption. The Government did not present facts to show why, on remand, the court had found the enhancement to be appropriate when it previously had found the contrary.

The application of the preponderance of evidence standard violated Peyton's due process rights only if it led to enhancements that had an "extremely disproportionate effect on the sentence relative to the offence of conviction". The court held that because the preponderance of evidence standard does not result in an extremely disproportionate sentence, the district court had not erred by applying it.

Peyton contended that the Government had not provided sufficient evidence to prove the $67,355 loss was relevant conduct attributable to her. Relevant Conduct is the sum of two figures: (1) the amount of loss that resulted from the acts "committed, aided, abetted, counselled, commanded, induced, procured, or wilfully cause by the defendant"; and (2) "all reasonably foreseeable acts and omissions of others in furtherance of the jointly undertaken criminal activity." Because a common scheme to defraud had existed, the conduct of the co-conspirators can be considered relevant conduct for the purpose of her sentencing. In this case, the scope of the scheme included the fraudulent acquisition and use of at least 17 credit cards. Peyton had been aware of the cards obtained in the name of navel employees because they were sent to her home address and were conspicuously issued in other peoples' name. Sufficient evidence existed to support a finding that Peyton had participated in and had knowledge of the full scope of the scheme.

The Court considered the following factors to determine if Peyton held a position of trust: (1) "inability of the trustor to objectively and expediently determine the trustee's honesty"; and (2) "the ease with which the trustee's activities can be observed."

Peyton as a supervisor was subjected to significantly less supervision and she possessed managerial discretion to access a secured roster listing the names and social security numbers of postal employees. Peyton's argument is that she did not hold a position of trust with American Express – the only victim. The Court of appeals rejected that argument and noted that victims of fraud are not limited to the entities that bear the ultimate financial burden, but also include those who bear "emotional, financial and other burdens." Peyton's actions injured these people named on the credit cards because their credit histories were adversely affected.

The Court of Appeals affirmed the district court's calculation of the accountable loss. It reversed the obstruction of justice enhancement and vacated only that part of the sentence. The case was remanded for re-sentencing in accordance with the Court of appeal's opinion.

United States v. Williams, No. 02-20151 (6th Cir., Dec. 23, 2003)

This was an appeal by Williams and Kelly of their sentence pursuant to their guilty plea to identity theft in violation of 18 U.S.C. § 1028(a)(7). Ward appealed her sentence pursuant to her guilty plea to identity theft in violation of 18 U.S.C. § 1028(a)(7) and to making a false statement in violation of 18 U.S.C. § 1001(a)(2). Williams, Kelly and Ward had been involved in a scheme in which they used false identifying information to obtain home loans.

Williams appealed the application of enhancement § 2B1.1(b)(9)(C)(i). Kelly appealed the use of the 1998 sentencing guidelines, contending that the 2002 guidelines should be applied without the § 2B1.1(b)(9)(C)(i) enhancement. Ward appealed the refusal to depart downward because of her family circumstances, aberrant behaviour and her relative culpability compared to others.

From September 1998 to June 2000 three individuals provided false identifying information, including social security number (SSN), employment information and salary information, to persons who wanted to buy a house under a loan program of the Federal Housing Administration. Purchasers such as Kelly and Williams signed loan documents containing the false information and submitted them to Community Mortgage Corporation for federally guaranteed loans for down payment assistance.

Subsection § 2B1.1(b)(9)(C) was implemented pursuant to Section 4 of the *Identity Theft Assumption and Deterrence Act of 1998* (ITADA), Pub. L. No. 105-318. It focuses on an aggravated form of identity theft known as "affirmative identity theft" or "breeding", in which a defendant uses another individual's name, social security number, or some other form of identification to "breed" (i.e. produce or obtain) new or additional forms of identification.

Williams argued that the bank loan number was not the equivalent of a false identification, and that she had purchased the entire loan package, not a social security number. Thus the SSN in those documents had not been used to obtain additional false identification. Kelly argued that the enhancement does not apply because he had obtained the bank loan in his own name.

The court held that since a bank loan is an account number that can be used to obtain money, it is a "means of identification" as the term defined in 18 U.S.C. § 1028. A SSN is clearly defined as a "means of identification" and, thus, its use to obtain a loan falls within the scope of the statute and guidelines.

The court also dismissed Williams' argument, that he had bought the SSN as part of a package that was used to procure a loan instead of having bought the SSN and used it to fill out a loan application, as irrelevant.

The district court applied the 1998 Sentencing Guidelines to Kelly's conduct because using the 2002 guidelines would have resulted in a higher offence level. Accordingly, the district court did not err in using the 1998 guidelines because of *ex post facto* concerns.

Finally, the court held that "there is no duty on the trial judge to state affirmatively that he knows he possessed the power to make a downward departure, but declines to do so. As the sentencing court was aware of its authority to depart, Ward lacks a basis to challenge the sentencing court's denial of her motion for a downward departure.

The sentences were affirmed.

United States v. Peterson, No. 03-30025 (9th Cir., Dec. 30, 2003)

This was an appeal of a denial of a motion to suppress evidence obtained in an unconstitutional search.

In late 2001, the police learned from three sources that Peterson was involved in an identity theft operation. Peterson and an accomplice Watson had been stealing mail in Portland and Vancouver. Peterson possessed a ring of duplicate U.S. Postal Service mailbox keys, and the floor of Peterson's room was littered in stolen mail. The source also said that Watson had an assault riffle and binary plastic explosives. This information led to the issuance of a search warrant.

The first source also told police that when Watson was arrested, he had requested that the explosives be moved in to another apartment. Based on this information, a second search warrant was obtained. The police seized about two pounds of explosives.

The second source informed the police that Peterson was a "master" forger and identity thief who used a computer to produce fraudulent cheques and identification. A third source confirmed this information and told police Peterson had about 200 pieces of stolen mail in this room. This source also saw explosives and said Peterson had claimed he could use them at any time." With this information, the police received a state warrant to search Peterson's residence. Because of the presence of explosives, the police considered the execution of the search warrant to be high-risk. As a consequence they requested assistance from the SWAT team.

When the SWAT team members were taking their final position to knock and announce, Guy Edwards opened the door. When he recognized the police, he immediately tried to close the door. The police entered the premises, where they seized binary explosives, blasting caps, 5.8 grams of methamphetamine, a quantity of tar heroin, over 1000 pieces of stolen mail, more than 20 fake IDs, illegal duplicates of mailbox keys, a laminator, a credit card imprinting machine, counterfeit and forged cheques, and $10,500.00 in cash.

Peterson argued that the entry in to his residence was unreasonable under the Fourth Amendment. The Supreme Court held that a "no-knock" entry is constitutional in three situations, when officers "have a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be 1) dangerous, 2) futile or 3) that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence."

In this case, the Court of Appeals held that the SWAT team faced all three. The court found announcement would have been futile, because just as one cannot close a door that is already closed, one cannot "announce" a presence that is already known.

The Government pointed to the danger and potential for destruction of evidence as justification for the manner in which the warrant was served. The court found that the record revealed that the officers' concerns had been well-founded. The SWAT team reasonably believed that Peterson's residence contained explosives. They also knew that Peterson had been known to carry a concealed weapon illegally. The SWAT team also knew that Peterson's residence probably contained methamphetamine and that it could easily be disposed of.

Peterson next argued the fact that the SWAT team's preliminary pre-raid plan for serving the warrant seems to have contemplated not giving an announcement. The predetermined strategy for effecting the raid had fallen by the wayside when the door was opened and immediate entry had been justified. The lawfulness of the team's original plan was not relevant to the court's consideration; its role is to evaluate the events that actually occurred.

Peterson next contended that the SWAT violated the "knock and announce" statute 18 U.S.C. § 3109. When the door was closed by Edwards, he obviously knew he was denying entry to the police. Under the plain language of the statute the entry was lawful. The three circumstances of the Fourth Amendment apply with equal force in the § 3109 context.

The district court's judgement was affirmed.

United States v. Melendrez, No. 03-30221 (9th Cir. Nov. 9, 2004)

This was an appeal of a sentence where a six-level enhancement was imposed for "identity theft" U.S.S.G. § 2B1.1(b)(9)(C) (2002). Melendrez pled guilty to a charge of producing more than five identification documents in violation of 18 U.S.C. § 1028(a)(1), (b)(1)(A)(i) and (ii), (b)(1)(B). The pre-sentence (PSR) report recommended the "identity theft" enhancement which increased Melendrez's offence level to twelve. The district court adopted the PSR's recommendation and sentenced Melendrez to thirty months imprisonment.

Melendrez argued that the enhancement should not have applied because each of the documents created by him was in his own name or the name of a fictitious individual and had not used the actual names of the persons to whom the Social Security numbers were assigned.

For purposes of the statute, a means of identification is the identifying name or number of an actual person, not the document on which such name or number appears. In this case, the means of identification were the Social Security Numbers Melendrez admitted were of actual persons, not the Social Security cards or DD forms 214.

The enhancement is intended to target "an aggravated form of identity theft known as 'affirmative identity theft' or 'breeding', in which the defendant uses another individual's name, social security number or some other form of identification to 'breed' (i.e. produce or obtain) new or additional forms of identification." Such means of identification must be of an actual (i.e. non fictitious) individual, other than the defendant or a person for whose conduct the defendant is accountable under § 1B1.3 (Relevant Conduct).

The enhancement identifies two means of identification, the source ID numbers and the produced ID numbers, both of which must "be of an actual (i.e. non fictitious) individual, other than the defendant." The court found that the fact that real Social Security numbers shared space on bogus identification documents with fictitious names did not make the enhancement inapplicable. U.S.C. § 1028 does not require that a name *and* Social Security number be used together to qualify as a means of identification. The court held that there is no requirement that the source ID and the produced ID be different numbers. The fact that Melendrez had paired the Social Security numbers with fictitious names on the identification documents did not sever the ties linking the victims and the Social Security numbers.

Melendrez also argued that the enhancement should apply only when a defendant poses as the victim to whom the pilfered means of identification belongs. The enhancement clearly is not so

limited. He asked that the rule of lenity be applied to construe ambiguities in criminal statutes in favour of the defendant.

The court found that although the enhancement could have been stated with less complexity, its meaning was not sufficiently ambiguous to invoke the rule of lenity.

The district court's sentence was affirmed.

United States v. Rand, 403 F3d 489, No. 04-1572 (7th Cir., Apr. 5, 2005)

This was an appeal of a restitution order. Mr. Rand pleaded guilty to a charge of conspiring to steal identification information from employees of the Gary, Indiana public school system and to use that information to fraudulently obtain credit cards, in violation of 18 U.S.C. § 371.

The conspiracy had involved: 1) obtaining names and social security numbers of employees of the Gary Community School Corporation in order to establish credit in the employees' names without their knowledge for the defendant's own personal benefit; 2) obtaining credit cards in the employees' names in order to purchase merchandise for the defendant's personal benefit… 4) redirecting the fraudulent credit cards, credit card statements, billing statements and other mail in order to conceal the deceptive use of the employees' identification.

The indictment listed 28 separate overt acts of identity theft, specifying the individual victims. In Rand's guilty plea, he specifically admitted to several acts of fraud involving the identity information of five individual victims.

The pre-sentence report asserted that the conspiracy actually implicated fraudulently obtained credit cards sent to nine different street addresses (not four as indicated in Count 1) and that Rand could be held responsible for 25 additional incidents of identity theft not mentioned specifically in the indictment. Based on these figures, the report concluded that Rand was responsible for $90,744.30 in actual losses and $8,915.49 in intended losses under a theory of relevant conduct.

Rand challenged this alleging that he should be held responsible only for the specific fraudulent acts that he had affirmatively admitted in his guilty plea, which had given rise to losses totalling just $12,594.90.

The district court had found that the evidence conclusively linked Rand only to four addresses. Based on this finding, the court had settled on the sum of $57,431.76 and ordered Rand to repay that amount in restitution and sentenced him to 21 months in prison.

The Government bears the burden of demonstrating the correct amount of the restitution award by a preponderance of evidence. The Court of Appeals can review the calculation for an abuse of discretion. A reversal is warranted if the district court relied on "inappropriate factors".

Rand alleged that the order was invalid because it held him responsible for acts of identity theft relating to victims that were not specifically in the original indictment and thus not covered by his guilty plea.

A restitution award is authorized only with respect to the loss caused by "the specific conduct that is the basis of the offence of conviction". In such a case, examination of the conduct constituting

the commission of a crime only involves consideration of the conduct to which the defendant pled guilty and nothing else.

Federal law defines a victim as a person directly and proximately harmed as the result of the commission of an offence for which restitution may be ordered including, in the case of an offence that involves as an element a scheme, conspiracy, or pattern of criminal activity, any person directly harmed by the defendant's criminal conduct in the course of the scheme, conspiracy, or pattern.

The Court of Appeals concluded that while the conduct underlying a restitution order must be specifically articulated in the charge or a plea agreement, specific victims need not be, especially in a case involving "as an element a scheme, conspiracy, or pattern of criminal activity".

The court found that Rand's guilty plea clearly qualified as such a case. Accordingly any individual "directly harmed" by Rand's criminal conduct in the course of the fraud scheme is presumptively included in the restitution calculus. Moreover, Rand may be held responsible for the losses caused by the foreseeable acts of his co-conspirators.

The court found that the district court had properly looked at the evidence and that Rand, having pleaded guilty, may not pick and choose the victims for which he will be held responsible.

The restitution order was affirmed.

United States v. Bush, No. 03-4552 (4th Cir., Apr. 13, 2005)

Mr. Bush challenged his conviction and sentence for various identity theft crimes.

Ms. Brenda Moon contacted the police saying she thought someone was trying to obtain a loan in her name. The police spoke with bank employees who told them that they had received a call and also that they had heard a man's voice in the background. When "Ms. Moon" called to verify the status of her loan she was instructed to come to the bank.

Yvette Canty was the woman trying to obtain a loan in Ms. Moon's name. She was with Mr. Bush when they were apprehended after leaving the bank and before entering a vehicle. After the arrests, the vehicle was searched. The search revealed a computer printout of a credit report for Brenda Moon as well as a sheet of paper containing handwritten information about her. A phone bill listing an address for Mr. Bush was also found. Ms. Canty also made oral statements in which she revealed Bush's address and that he had a computer with all the loan information in it.

The police executed a search warrant at Bush's home and seized two computers which produced evidence against Bush. Based on the evidence, Bush was convicted of bank fraud. His conviction was reversed on appeal and he was retried on state law charges in 2001.

Inspector Jones was to testify at the trial. In the process of reacquainting himself with the case he discovered that Bush had a 2000 BMW sport-utility vehicle in his name. Jones decided to investigate further. The vehicle was originally titled in the name of Robert Bogle, a recently deceased man. Jones made several inquiries and discovered that Bush had a fake New Jersey's driver's licence made with his picture and Bogle's personal information.

Jones, in collaboration with the FBI, discovered that Bush had used fake driver's licences to obtain online loans for luxury cars. The licences had Bush's photograph and personal information of recently deceased individuals. After discovering this information, Jones executed a second search warrant at Bush's home. The search revealed, *inter alia*, software formats used to create fake driver's licences, personal information of the individuals whose identities Bush stole, and fake lien-release papers.

In January 2002, Bush was indicted for fifty-six counts. Count one was the use of a false identity to defraud in violation of 18 U.S.C.A. §§ 1342, 1344. Count two was the use of a fake Social Security Number to obtain a car loan (42 U.S.C.A. § 408(a)(7)(B). Counts three to six were identity theft to procure loans (18 U.S.C.A. §§ 1342, 1344). Counts seven to fifty-six were for using his step-mother's identity to obtain her Social Security payments in violation of 18 U.S.C.A. § 2 and 18 U.S.C.A. § 510(a)(2).

Bush filed several motions with the district court to appoint new counsel, to dismiss the indictment for a violation of the *Speedy Trial Act*, 18 U.S.C.A. § 3161 and to suppress evidence. Bush then filed another motion for new counsel and for the right to proceed *pro se* which was denied.

The district court eventually found that Bush was not capable of representing himself. The district court also found that Bush was misrepresenting the nature of his relation with counsel. The district court concluded that he wanted to make a mockery of the proceedings.

In this appeal, Bush raised several challenges to his conviction. Fist, Bush argued the court erred in denying his motion for self-representation. Bush also argues his *Speedy Trial Act* rights were violated and that the district court erred in denying his motion to suppress evidence.

The Supreme Court found that the right to self-representation is mutually exclusive of the right to counsel guaranteed by the Sixth Amendment. The Supreme Court found that a defendant need not himself have the skill and experience of a lawyer, but it also cautioned that the right of self-representation is not a licence to abuse the dignity of the courtroom. The Court of Appeals, after reviewing the complete record, found that the district court did not clearly err in finding Bush manipulative.

The *Speedy Trial Act* provides that the trial of a defendant charged in an information or indictment with the commission of an offence shall commence within seventy days from the filing date. The Act also provides that some periods of delay are excluded when calculating the seventy day time period. These delays include the time between the filing of a motion and the conclusion of the hearing. When Bush presented a motion to sever, he specifically requested a hearing. The court concluded that the delay between the filing of the motion and the hearing is excluded thus there is no violation of the seventy day timeframe.

Bush contended that the search of the vehicle was an unconstitutional warrantless search. The Court of Appeals concluded in *New York v. Belton*, 453 U.S. 454 (1981) that the search of vehicles incident to arrests made outside the vehicle is permitted as long as the arrested individual was a recent occupant of the vehicle. Because officers had seen Canty exit the jeep before entering the bank and because she was in the process of re-entering the jeep, Jones was permitted to search the jeep incidentally to Canty's arrest.

The Court of Appeals affirmed Bush's conviction and sentence.

United States v. Yagar, No. 03-20228 (6th Cir. Apr. 18, 2005)

This was an appeal of Yagar's sentence for pleading guilty to mail-theft 18 U.S.C. § 1708. Yagar was sentenced to twenty-one months with two years supervised release and $20,987.15 in restitution.

Yagar claimed that her Sixth Amendment rights were violated by the district court when it enhanced her sentence under sections 2B1.1(b)(1) and 2B1.1(b)(2)(A) based on facts that were neither presented to a jury nor admitted by her.

The Supreme Court in *United States v. Brooker*, 125 S. Ct. at 756 held that "any fact (other than a prior conviction) which is necessary to support a sentence exceeding the maximum authorized by the facts established by the plea of guilty or a jury verdict must be admitted by the defendant or proved to a jury beyond a reasonable doubt. The district court's reliance on judge-found facts to increase Yagar's sentence was a violation of the Supreme Court's Sixth Amendment holding in Brooker. The Court of Appeals vacated the sentence and remanded the case for re-sentencing.

However, the Court of Appeals also considered the remaining claim as to whether the district court was correct to apply a two-level sentence enhancement based on its finding that the offence involved more than ten, but less than fifty, victims. The Government claimed that the crime involved more than fifty victims, namely that more than sixty account holders temporarily lost funds resulting from Yagar's conduct. Yagar claimed that the evidence was insufficient to support the district court's finding that six account holders were not reimbursed for their costs of purchasing new cheques. Yagar also argued that they were not victims as the costs they incurred were similar to minimal damages which the Applications Notes exclude from the enhancement's coverage.

The Court of Appeals found that these six individuals are not "victims" under the Guidelines because they were fully reimbursed for their temporary financial losses. The account holders here had suffered no adverse effect as a practical matter from Yagar's conduct. The Court of Appeals also found that the record suggested that the district court had erred in finding sufficient evidence that the six account holders suffered pecuniary harm.

The sentence was vacated and the case remanded for re-sentencing according to Brooker and with no enhancement for the number of victims.

United States v. Collier, No. 04-2013 (8th Cir., Jun. 27, 2005)

This was an appeal of a sentence obtained by Mr. Collier after pleading guilty to bank fraud, fraudulent use of identification, and fraudulent use of a social security number.

Collier used the identities of victims to obtain loans and credit card accounts. He also attempted to obtain student loans with the identities. The government alleged that in addition to nine multiple corporations; multiple individuals were victimized through the thefts, resulting in losses totalling over $100,000.00.

The district court sentenced Collier to concurrent sentences of 100 months, concurrent supervised release terms, and a special assessment of $500.00 and restitution of $150,896.57.

The court departed upward four levels based on the fact that Collier's criminal history did not adequately reflect the seriousness of his past criminal conduct and based on the fact that his conduct caused his victims substantial damage.

Collier argued that there was insufficient evidence to support the district court's upward departures. The Court of Appeals noted that the district court clearly set forth its reasoning in departing upward, noting Collier's nineteen convictions over a short period of time, two prior crimes of violence, escape charges, and his failure to properly conform his conduct to community supervision while out on supervised release. The court had also properly considered the substantial harm to his victims, noting that Collier stole the identity of one victim twice. Based on the evidence, the Court of Appeals concluded the district court did not clearly err.

Collier also argued that under *Blakely*, his sentence was unconstitutional because enhancements were based on judge-tried facts concerning relevant conduct that were not determined by a jury beyond a reasonable doubt. At sentencing, Collier gave a "lengthy and detailed" testimony regarding all relevant conduct. There was no Sixth Amendment violation; Collier chose to testify and admitted the facts upon which the court based its sentence.

The court did not clearly err in denying a reduction for acceptance of responsibility. The record supports the district court's conclusion that Collier's testimony was not an acceptance of responsibility but rather an attempt to minimize his involvement.

Finally, the district court erred in considering the Sentencing Guidelines as mandatory instead of advisory. However, Collier does not get a new sentencing hearing as he cannot establish a "reasonable probability" that he would have received a more favourable sentence had the court considered the guidelines as advisory.

The sentence and restitution order were affirmed.

United States v. Klopf, No. 04-10663 (11th Cir., Sep. 7, 2005)

This case was an appeal of a conviction and sentence for identity theft contrary to 18 U.S.C. § 1028(a)(3)(2000), and use of unauthorized credit cards contrary to § 1029(a)(2).

Klopf was indicted for possessing with intent to use unlawfully five or more fraudulent identification documents (§ 1028(a)(3)) and using unauthorized access devices with the intent to defraud (§ 1029(a)(2)). The fraudulent documents consisted of approximately sixteen Florida driver's licences bearing Klopf's picture alongside identifying information for several other individuals, while the access devices were credit cards in the names of other individuals.

A search of Klopf's vehicle uncovered credit cards, printouts from public records database with identifying information including address, Social Security Number, birth date and driver's licence number. A search of Klopf's apartment revealed a number of plastic storage containers which held identifying information and various documents pertaining to several individuals.

Leo Johnson testified that he had made several fraudulent Florida driver's licences at Klopf's request. They were not perfect replicas but were passable to an untrained person. Johnson also provided supporting documents, including Social Security cards, voter registration cards, utility bills and American Express credit cards.

Klopf argued that the government had failed to prove (1) that he had intended to use the sixteen driver's licences for an unlawful purpose; 2) that his possession of the licences had any affect on interstate or foreign commerce. Klopf contends that a conviction under 1028(a)(3) required proof that: 1) his intended use of the fraudulent identification documents had violated particular federal, state, or local law; and 2) his "actual use" of the fraudulent identification documents had affected interstate or foreign commerce.

Klopf contended that because the government failed to prove that he had ever used the fraudulent identification documents in any manner, it could not possibly have been proven that his actual use of the fraudulent driver's licences had affected interstate commerce.

To obtain a conviction under 1028(a)(3), the government must prove: 1) the defendant knowingly possessed five or more false identification documents, 2) the defendant had the wilful intent to transfer the false identification documents unlawfully, and 3) the defendant's possession of the false identification documents was in or affecting interstate commerce.

Klopf conceded that the government had proved the first element but challenged the other two. The evidence demonstrated that 1) Klopf had possessed valid credit cards in the names of others, who had not given him permission to use their information, and had charged $30,000.00 to those accounts; 2) he had possessed sixteen fraudulent driver's licence with supporting documentation; 3) identifying information for the persons on the cards had been found at Klopf's apartment; and 4) he had requested and obtained supporting documentation for the individuals named on the driver's licences.

The court held that a reasonable fact finder could infer that Klopf had intended to obtain valid credit cards bearing the same names as those on the driver's licences, and that, if he had been questioned while attempting to use the credit cards, he would have used the driver's licences to verify that he was the individual named on the card. Such use would be unlawful as it would violate 18 U.S.C. § 1029(a)(2).

As for the third element, Klopf 1) rented a storage facility under the name of Bender; 2) possessed two fraudulent driver's licences bearing Bender's identifying information; 3) the number on the driver's licence matched the number entered on the application for the storage facility; and 4) he used the storage facility to receive mail, including unauthorized credit cards and account statements.

The court held that a reasonable fact finder could infer that Klopf had used the fraudulent identification documents to verify his identity when renting the storage and had used the storage to receive mail in connection with a credit card scheme that had a significant effect on interstate commerce. The legislative history of section § 1028(a)(3) showed that Congress had intended only that a 'minimal nexus with interstate or foreign commerce be shown." Consequently the court held that fraudulently inducing a bank to issue a credit card through fraudulent identification documentation would be sufficient evidence of a § 1028(a)(3) violation. The court also held that the government does not need to prove that the defendant knew of the interstate commerce nexus when the offence was committed.

Klopf argued that his conviction under § 1029(a)(2) was improper because the government had failed to prove that he had acted with the requisite intent to defraud. Klopf contended that because he had made regular payments on the credit card accounts, and all accounts were active at the time of his arrest, that he had not possessed the requisite intent to defraud.

The court held that it was irrelevant that he made payments on the cards because, in each application for a credit card, he had intended to defraud the banks by representing to them that they were dealing with persons other than himself. The requirement that access-device fraud affect interstate or foreign commerce was fulfilled because credit cards are generally issued to applicants by out-of-state financial institutions, and credit card account numbers travel state lines, both electronically and by mail. By making purchases with the cards, Klopf engaged in interstate financial transactions.

Klopf further contended that the district judge had abused his discretion by denying his requested jury instructions. To decide if the defendant's requested instructions were substantially covered by the actual charge delivered to the jury, the court "need only ascertain whether the charge, when viewed as a whole, fairly and correctly states the issues and the law."

The court held that Klopf's requested jury instruction was incomplete. The instructions delivered by the district court were sufficient.

The court found that the pre-sentence report (PSR) had erroneously stated the maximum authorized imprisonment for a violation of § 1028(a)(3) was fifteen years, instead of the actual maximum of three years. The case was remanded to the district court which was to reconsider Klopf's "entire sentencing package" so as to impose a sentence that is appropriate for the convictions under the *Booker* advisory sentencing scheme.

Klopf's conviction was affirmed and the case was remanded for re-sentencing.

United States v. Havens, 424 F3d 535, No. 04-2956 (7th Cir., Sep. 12, 2005)

This is was appeal of an order of restitution. Ms. Havens pleaded guilty to various offences of identity theft, was sentenced to twelve months in prison and was ordered to pay $30,000.00 in restitution.

In 1998, Havens applied using her maiden name, Brown, for a mortgage loan in the amount of $144,000 which she planned to use to refinance her home. Havens was afraid that her application would be rejected because of her poor credit rating. She filled in the application using the date of birth, social security number, and various credit card accounts of Patricia Brown who was more creditworthy. Havens also produced two false payroll cheques payable to Patricia Brown. Havens had access to this information in her capacity as real estate broker.

The fraud was discovered in 1999 when Havens fell behind on the payments. Brown initially thought it was an error on the part of the bank, but was soon contacted by other creditors. Havens had also gotten a second mortgage and credit card in the name of Brown. Brown's credit was also damaged by the inclusion of Havens earlier credit history which included a bankruptcy, various civil judgements and other delinquent accounts.

According to Brown, a poor credit rating is particularly harmful to a certified public accountant. Brown proceeded to sue Havens in Indiana state court for damages suffered as a consequence of theft or fraud (Ind. Code § 34-24-3-1).

Brown also requested and was granted a court order directing the credit agencies to correct her credit reports and restore her credit rating.

Havens was then indicted on two counts of wire fraud (18 U.S.C. § 1343), three counts of using a false social security number (18 U.S.C. § 408(a)(7)(B), and one count of fraud in connection with access devices (18 U.S.C. § 1029(a)(2)) and (c)(1)). Havens pleaded guilty to all six counts.

The pre-sentence report recommended restitution in the amount of $42,099.70. The district court sentenced Havens to 12 months and ordered her to pay the principal sum of $30,000 to Brown.

The *Mandatory Victim Restitution Act*, 18 U.S.C. § 3663A requires a court to order a defendant to make restitution to the victim of an offence involving fraud or deceit. A victim is defined as "a person directly and proximately harmed as a result of the commission of an offence." Havens conceded that Brown is a victim under the Act.

Havens argued that the court should not have relied on the $30,000.00 state civil judgement award because it was based on a theory of stolen credit and did not reflect the monetary losses suffered by Brown. She also argued no amount of restitution should be awarded because Brown was not required to pay the debts she acquired in her name and thus suffered no loss.

The Court of Appeals found that a civil judgement by itself is insufficient to support an order of restitution because some damages and costs recoverable in a civil action do not qualify as losses under the MVRA. The court found that the district court did not know the origin of the $30,000 award and the lack of information prevented the court of appeals from conducting a meaningful review of the order of restitution. The Court of Appeals remanded the case for further proceedings.

The Court of Appeals, on remand, directed the district court to determine the diminution in value of Brown's property caused by Haven's conduct. Brown contended that she was entitled to be reimbursed for all the time she spent fixing her credit. The Court of Appeals found that this went too far and that she was only entitled to the time where she had to miss work or forego hourly compensation or because she had to turn down clients. Fees paid to counsel or other experts in dealing with the banks to restore her credit rating were also properly included. The costs associated with her lawsuit were not recoverable.

The order for restitution was vacated and the case remanded for proceedings consistent with the decision on appeal.

United States v. Oates, No. 04-4018 (8th Cir., Nov. 3, 2005)

This was an appeal by Oates of his sentence after he pled guilty to one count of identity theft (18 U.S.C. § 1028(a)) and one count of credit card fraud (18 U.S.C. § 1029(a)). Oates used another's social security number (SSN) to obtain a business credit card on which he charged $41,330.09.

First, Oates contended that the district court had misapplied the "means of identification" enhancement U.S.S.G. § 2B1.1(b)(9)(C)(i) by using the wrong definition of "means of identification". The guidelines refer to the definition in 18 U.S.C. § 1028(d)(4), however, because of a reorganization, the definition was at 18 U.S.C. § 1028(d)(7). The district court judge used the definition at 18 U.S.C. § 1028(d)(7). The Court of Appeals held that the guidelines preserved the original definition notwithstanding the failure to correctly cross-reference the statute after its reorganization.

Next, Oates argued that a credit card number is not a "means of identification". The court held that although the credit card account number was issued in the name of a fictitious business, it was still a means of identifying an actual individual. When an individual's SSN is combined with a fictitious name on a subsequently obtained means of identification, it does not necessarily "sever the ties linking the victims and SSNs." In Oates's case, the account still affected the victim's individual credit, and thus was a means of identification. The district court had correctly included the enhancement.

Oates further contended that because the district court heard his case between *Blakely* and *Booker*, it erred by a) failing to advise him of the "statutory maximum" (the guideline range as calculated without enhancements on judge-found facts) and b) sentencing him in excess of that range.

The court held that neither *Blakely* nor *Booker* require a district court to advise a defendant of anything other than the actual statutory maximum at a plea hearing. The sentencing error committed by the district court was to treat the guidelines as mandatory rather than advisory. The Court held that nothing in the record gave it grave doubt that Oates may have received a shorter sentence under and advisory guideline regime.

The sentence was affirmed.

United States v. Green, No. 04-3919 (8th Cir., Nov. 16, 2005)

This was an appeal by Green of his conviction for three counts of social security fraud (42 U.S.C. § 408(a)(7)(B), one count of accessing a computer to steal information used fraudulently to gain credit (18 U.S.C. § 1030(a)(4)) and three counts of devising a scheme to defraud a financial institution (18 U.S.C. §§ 1344 and 2).

Green paid two SBC Communication, Inc. employees to steal names, addresses, and social security numbers of California customers. Green then used this information to buy flat screen televisions from Dell Computers using instant credit provided by Dell.

Green was sentenced to seventy-two months of imprisonment to account for the "serious nature" of the crimes committed and the "objectives of just punishment, general deterrence, and incapacitation."

Green contended that the district court had abused its discretion in allowing testimony of nine victims who were not specifically referenced in the Superseding Indictment because the prejudicial nature of the evidence outweighed its probative value. The court held that the evidence may have been emotional, but Green cannot show that it "lured the fact finder into declaring guilt on a ground different from proof specific to the offence charged."

Green then argued that the district court had erred by admitting charts without the proper limiting instructions. The admissibility of summary charts, graphs and exhibits "rests within the sound discretion of the trial judge, whose action in allowing their use may not be disturbed by an appellate court except for an abuse of discretion." The court held that the four charts, in this case, summarized evidence already introduced. The charts had assisted the jury in understanding how the scheme was perpetrated, and the witness who prepared the charts was available for cross examination. Thus the charts were properly admitted.

Next Green contended that the district court had erred by not dismissing a juror he claimed was asleep. The trial court retains broad discretion in determining whether to dismiss a juror accused of sleeping. The Court of appeals will not find an abuse of discretion if the record shows a legitimate reason for the court's decision to retain the juror. When the district court had been informed of the juror sleeping, it had granted a short recess but had not made a specific finding about the juror being asleep or not. Based on this evidence, the court of appeals concluded that the district court had not abused its discretion.

Finally, Green contended that his sentence should be vacated in light of *Blakely* and *Booker*. The government, as the beneficiary of the error, has to prove that no "grave doubts" exist as to whether the "error substantially influenced the outcome of the proceedings." The court held that there was no grave doubt since the district court had left unused some of its discretion when it had sentenced Green to two months above the minimum Guideline range.

The conviction and sentence were affirmed.

United States v. Grant, 04-12268 (11th Cir., Nov. 29, 2005)

This case was an appeal of a sentence for producing and possessing counterfeit corporate cheques, in violation of 18 U.S.C. §§ 2 and 514. Grant had pled guilty to the charge.

Grant argued that the district court had erred in calculating an intended loss of $230,009.54 and in imposing a twelve level enhancement pursuant to U.S.S.G. § 2B1.1(b)(1)(G). Specifically, Grant contended that the intended loss calculation should not have included the $182,899.54 total face value of photocopies of stolen corporate cheques found in his possession.

Grant and a number of un-indicted co-conspirators participated in identity theft, bank fraud, theft from the United States mails, and manufacturing and negotiating counterfeit cheques.

"Loss" is defined as the greater amount of "actual loss" or "intended loss", where the actual loss includes "the reasonably foreseeable pecuniary harm that resulted from the offence" and intended loss means "1) pecuniary harm that was intended to result from the offence and 2) includes pecuniary harm that would have been impossible or unlikely to occur." In calculating the amount of loss, the district court "need only make a reasonable estimate of the loss."

The Court of Appeals held that when an individual possesses a stolen cheque, or a photocopy of a stolen cheque, for the purpose of counterfeiting, the district court does not clearly err when it uses the full face value of that stolen cheque in making a reasonable calculation of intended loss. Where the Government presents evidence indicating the defendant intended to utilize the full face value of the cheques, and the defendant fails to present countervailing evidence, a district court is especially justified in including the cheque's full face value in its intended loss calculation.

The intended loss calculation and sentence of the district court were affirmed.

United States v. Newsome, No. 04-3292 (3rd Cir. Mar. 9, 2006)

This is an appeal of a sentencing decision in which a two-level enhancement for "the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification" (U.S.S.G. § 2B1.1(b)(9)(C)(i)(2003)) was applied.

Mr. Newsome conspired to make fraudulent withdrawals from customer accounts at Fleet Bank, a Federal Deposit Insurance Corporation (FDIC) insured bank. A co-conspirator, Mr. Hamilton, obtained personal contact and account information of Fleet customers from an unidentified Fleet employee. Using this information, Newsome and Hamilton produced fake driver's licences, employee identification cards, and completed pre-printed withdrawal slips which were used by two other accomplices to make withdrawals.

Newsome and Hamilton contributed to the effort by taking digital photographs of the other accomplices. These photographs were placed on the forged cards.

Before the fraud was discovered the co-conspirators withdrew $135,340.00 that law enforcement was unable to recover. Newsome pled guilty to one count of conspiracy to defraud the United States (in its role as insurer of Fleet) (18 U.S.C. § 371). Newsome's plea bargain included a provision that the Sentencing Guidelines would apply.

Newsome objected to the two-level enhancement above as a matter of law. Newsome contended that taking a misappropriated means of identification – a name or number – and putting it on a new physical document does not trigger the enhancement because the new physical document containing the same means of identification does not constitute a new means of identification.

The court found that the phrase "any other means of identification" does not mean "different" as Newsome suggested. Commentary of the Sentencing Guidelines defines "produce" as including "manufacture, design, alter, authenticate, duplicate or assemble".

The court also found that the forged driver's licence and employer ID had the identity theft victim's correct information. This information by itself constituted a means of identification. When combined with a photograph it became a different means of identification.

When a means of identification is illegally used to produce an altered duplicate means of identification the sentencing enhancement applies. The appeal was dismissed and the sentencing judgement affirmed.

United States v. Montejo, No. 05-4143 (4th Cir., Mar. 29, 2006)

This was an appeal of a conviction for aggravated identity theft (18 U.S.C. § 1028A(a)(1). Prior to his conviction, Montejo pleaded guilty to immigration fraud and Social Security Fraud, on the basis of stipulations that he had knowingly and unlawfully possessed and used false Alien Registration and Social Security cards.

On appeal Montejo claimed that he had no knowledge that numbers on those documents had actually been assigned to other people. He argued that section 1028A requires such knowledge.

In order to obtain employment Montejo provided a Resident Alien card and Social Security card bearing Montejo's name, and on the Resident card, his photo, but fabricated numbers. However, both numbers had been assigned to other persons. When arrested, Montejo admitted to having purchased both cards for $60.00, that he knew they were false and that he had used them to obtain employment.

Montejo argued that the fact that he did not know that the numbers he possessed actually had been assigned to other people, meant that he had not knowingly used or possessed "a means of identification of another person."

The Court of Appeals looked at the interpretation of the statute and held that good usage requires that the limiting modifier, the adverb "knowingly," be as close as possible to the words which it modifies, here, "transfers, possesses or uses". The Court of Appeals agreed with the Government's construction that the defendant need not be aware of the actual assignment of the numbers to an individual to have violated the statute. The legislative history of the provision also supported this construction.

The district court's judgement was affirmed.

Civil Cases

Sherman v. United States Department of the Army, No. 00-20401 (5th Cir., Mar. 7, 2001)

This was an appeal of a summary judgement of a *Freedom of Information Act* (FOIA), 5 USC § 552. Sherman requested copies of computer-tapes containing the Awards and Decorations Computer Assisted Retrieval System (ADCARS) database containing roughly 611,000 general award orders issued between 1965 and 1973. These orders typically contain a soldier's name, rank and unit, as well as specific information relating to the details of the conduct giving rise to the award. Between 1968 and through 1990s, the Army identified personnel by social security number (SSN). Thus award orders issued after 1968 contain SSNs of army personnel as opposed to an Army Serial Number (ASN).

The Army found that it was necessary to redact all the SSNs, pursuant to exemption 6 of the FOIA to avoid a clearly unwarranted invasion of the privacy interests of Army personnel.

Sherman complained that the redaction was unnecessary, improper and prohibitively expensive. Sherman also sought a waiver of the fees associated with reproduction of the un-redacted tapes pursuant to the FOIA fee waiver provisions.

Pursuant to exemption 6, an agency may delete personal details in documents; provided the details to be deleted are reasonably severable and the overall privacy interests of the individual clearly outweigh the presumption of public disclosure. This determination depends on a balancing of the 'individual's right of privacy' against the basic policy of opening agency action to the light of public scrutiny. In considering the public's interest in the disclosure of the requested information, the professed intentions of the requestor are irrelevant. The privacy interest of the

individual must be considered in light of the fact "that other parties, such as commercial advertisers and solicitors, must have the same access under FOIA" as the party requesting the information.

To justify the application of exemption 6, the Army must demonstrate that the release of the SSNs would constitute a clearly unwarranted invasion of the privacy interest of Army personnel.

Sherman argued that the Army's consistent practice of disregarding an individual's privacy right in his SSN effectively waived the Army's authority to rely on exemption 6. Sherman noted that the use of SSNs in the Army has been pervasive and often public; and that SSNs were included with any reference to an individual. Sherman argued that if the court were to allow the Army to exempt material that it had previously released publicly, the court would effectively allow the Army to selectively control disclosure of any documents containing SSNs.

The court concluded that the concern for selective disclosure is not implicated when a government agency relies on exemption 6. The Supreme Court has explained that the privacy interest at stake in a FOIA exemption analysis belongs to the individual, not the agency holding the information. The court consequently held that only the individual whose informational privacy interests are protected by exemption 6 can effect a waiver of those privacy interests when they are threatened by a FOIA request.

The court noted that an individual's informational privacy interest in his or her SSN is substantial. The concern is that the simultaneous disclosure of an individual's name and SSN exposes the individual to a heightened risk of identity theft and other forms of fraud. The court noted that to properly weigh the privacy interests, the dire consequences of identity theft must be discounted by the probability of its occurrence. Thus, the relatively low risk of identity theft may sufficiently diminish the privacy interest of SSNs to warrant their disclosure where a strong public interest in disclosure exists.

The court held that against this substantial privacy interest, Sherman had failed to articulate a clearly competing public interest in disclosure of the SSNs. Sherman argued that the disclosure would help him and other historians identify individuals who fraudulently claimed to have received awards. However, the Supreme Court limited the consideration of "public interest" to the types of information that shed light on the nature of agency action, not those that shed light on fraudulently-claimed military honours.

The court found that Sherman had articulated a public interest that supported the disclosure of the content of the award orders and that redaction of the SSNs does not meaningfully detract from the public utility of the award orders.

The court concluded that the invasion of the information privacy interest of individual soldiers in the disclosure of their SSNs, would clearly be unwarranted in the absence of any public interest in those SSNs; the Army appropriately decided to redact them from the award orders requested.

The summary judgement was affirmed.

TRW Inc. v. Andrews, No. 00-1045 (Sup. Ct., Nov. 13, 2001)

This was an appeal by TRW of a decision of the Ninth Circuit Court of Appeals who had held that under a "general federal discovery rule" the statute of limitations of the *Fair Credit Reporting Act* (FCRA), 15 U.S.C. § 1681 starts running when a party knows or has reason to know she was injured, unless Congress expressly legislates otherwise.

Adelaide Andrews visited a doctor's office and filled out a form containing her personal information. An office receptionist named Andrea Andrews (the thief) copied the information and moved to Las Vegas where she attempted to open credit accounts using Andrews's Social Security number and her own name and address.

On July 25, September 27 and October 28, 1994 and on January 3, 1995 TRW furnished copies of Andrews's credit report to companies from which the thief sought credit. Andrews discovered these disclosures while reviewing her credit file during the process of refinancing her mortgage. She sued TRW, alleging that TRW had violated the FCRA by failing to verify, pre-disclosure of her report to others, that Adelaide Andrews of Santa Monica had initiated the credit applications or was otherwise involved in the underlying transaction.

TRW moved for partial summary judgement arguing the statute of limitations had expired on the claims stemming from the first two disclosures. The District Court held the two claims time barred and the Ninth Circuit reversed this.

The Supreme Court held that the Ninth Circuit had erred by holding that a generally applied discovery rule controlled the case. The court concluded that the text and structure of § 1681p evince Congress' intent to preclude judicial implication of a discovery rule. Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent. The court held that the most natural reading of § 1681p is that Congress implicitly excluded a general discovery rule by explicitly including a more limited one.

Andrews also argued that liability under the FCRA does not necessarily "arise" when a violation of the Act occurs. Andrews argued that the FCRA's substantive provisions tie "liability" with the presence of "actual damages", §§ 1681n, 1681o, and that "arise" means at least to "come into existence". Andrews concluded that liability arises only when actual damages materialize. Andrew argued that until damages materialize the essential elements of a claim are not present.

Andrews argued that her claims were timely because the actual damages did not "arise" until May 1995, when she suffered the emotional distress, missed opportunities, and inconvenience and that prior to that time she had no FCRA claim to bring. The court did not consider this issue because it was not raised or briefed below. However the court noted that even if the argument was valid, it would probably not help Andrews in this case. Her case alleged wilful violations of § 1681e(a) and that they are thus governed by § 1681n. § 1681n states that "Any consumer reporting agency… which wilfully fails to comply with any requirement imposed under the Act is liable to that consumer for actual damages and punitive damages as the court may allow. According to the court, the punitive damages could be awarded at the time of TRW's alleged violation, even if "actual damages" did not accrue at that time. Since some of the liability arose when the violations occurred, the limitation period therefore began to run at that point.

The Ninth Circuit's judgement was reversed and the case remanded.

Hallock, Ferncliff Assoc., Inc. v. Bonner, No. 03-6221 (2nd Cir., Oct. 22, 2004)

This was an appeal of an order providing that a lawsuit could proceed based on the authority of *Bivens v. Six Unknown Names Agents of the Federal Bureau of Narcotics*, 403 U.S. 388 (1971).

A search warrant was executed against the Hallocks to obtain evidence of violations of 18 U.S.C. §§ 2252 and 2252A, which proscribe activities relating to material involving the sexual exploitation of minors. Richard Hallock was apparently the victim of identity theft, and no evidence of any violation of the cited statutes was found in the materials seized. When the seized material was returned, some of it was damaged which gave rise to the actions.

The plaintiff's had invoked the *Federal Tort Claims Act* in a previous action which was concluded by a judgement of dismissal for lack of subject matter jurisdiction. A subsequent action for damages arising from the seizure of the plaintiff's computer equipment in violation of the Fifth Amendment of the United States Constitution was filed. The defendants filed a motion asserting that the first judgement was a bar to the second action. This motion resulted in an order which has given rise to this appeal.

The Court of Appeals found that the first action was not properly brought under the *Federal Tort Claims Act* and was a nullity. The court held that for the judgment bar to apply, the action must first be a proper one for consideration under the *Federal Tort Claims Act*. The district court's order was affirmed although for different reasons.

Westra v. Credit Control of Pinellas, No. 04-3139 (7th Cir., May 27, 2005)

This was a complaint under the *Fair Credit Reporting Act* (FCRA), 15 U.S.C. § 1681. Mr. Westa alleged that Credit Control failed to conduct a reasonable investigation as required by 15 U.S.C. § 1681s-2(b) and that ,as a result, he was denied credit and denied a chance to refinance his mortgage at a lower rate. Credit Control requested a summary judgement, which was granted.

Mr. Westra was a victim of identity theft in 1999 when a former friend fraudulently opened several accounts in his name. Westra successfully disputed many of these accounts and they were deleted from his credit file. In August 2002, Westra received notice of an account that Credit Control was collecting on behalf of Pasco Emergency Medical Services. Westra mailed a dispute letter to Trans Union to inform them that the account did not belong to him. The letter included a fraud statement and information about the identity thief.

Trans Union then sent a Consumer Dispute Verification form to Credit Control in October but it did not make any reference to fraud or identity theft nor did it include the documentation provided by Westra.

In November Westra received a credit report from Trans Union that still contained the Credit Control account. He sent a second dispute letter to Trans Union and sent a letter directly to Credit Control in December. After a few more exchanges, Credit Control finally removed the account.

Whether a defendant's procedure is reasonable is a factual question. A summary judgement is proper if the reasonableness of the defendant's procedures is beyond question. The Court of

Appeals found that Credit Control's investigation was reasonable given the little information they received from Trans Union.

Westra also argued that Credit Control should have contacted him directly. The Court of Appeals rejected this argument because requiring furnishers to automatically contact every consumer who disputes a debt would be terribly inefficient and such action is not mandated by the FCRA.

Administrative cases

Ferm v. United States Trustee, No. 97-16653 (9th Cir., Oct. 7, 1999)

This was an appeal of a fine of $800 given to Ferm for failing to include his Social Security number (SSN) on the documents relating to bankruptcy petitions he helped to prepare.

Ferm filed a motion with the Bankruptcy Court seeking leave to substitute an identification number other than his SSN on the bankruptcy petitions he prepares. The motion was motivated by Ferm's fear or credit card fraud. The Bankruptcy Court denied the motion.

On September 5, Ferm assisted two individuals in completing their bankruptcy petitions. Although he completed the required documents in connection with the petitions, he omitted his SSN.

Ferm did not object to the bankruptcy court's collection of his SSN pursuant to s. 11(c). However, he did object to the subsequent disclosure of his SSN to the general public pursuant to another statutory provision.

The Supreme Court delineates at least two distinct kinds or constitutionally protected privacy interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.

Ferm argued that the disclosure of his SSN violated his constitutional or statutory rights. Specifically, he argued that it implicated the first of the two types of privacy interest. The court agreed with Ferm "that harm can be inflicted from the disclosure of a SSN to an unscrupulous individual, is alarming and potentially financially ruinous." The court also noted that judicial and legislative actions in other contexts also support the conclusion that the disclosure of SSNs can raise serious privacy concerns.

The right to information privacy, however, "is not absolute; rather it is a conditional right which may be infringed upon a showing of proper governmental interest." The government has the burden of showing that "its use of the information would advance a legitimate state interest and that its actions are narrowly tailored to meet that legitimate interest." That interest must be balanced with the individual's privacy interests.

Ferm also noted that the Bankruptcy Court had not established any safeguards to prevent disclosure of his SSN to unscrupulous third parties.

The court found that to weigh properly the privacy interests involved, the dire consequences of identity theft must be discounted by the probability of its occurrence. The disclosure enhances the risk, however, the realization of the injury still requires two additional non governmental

elements: 1) an identity thief; and 2) a vulnerable account. A SSN unlike, for example an HIV status, is not inherently sensitive or intimate information, and its disclosure does not lead directly to injury, embarrassment or stigma.

The Government pointed to the important legislative purpose of s. 110 which was enacted to remedy what was perceived as widespread fraud and unauthorized practice of law in the BPP industry. The Government's interest in preventing fraud relates more to SSN collection than disclosure. The disclosure, along with the rest of the contents of documents filed with the bankruptcy court, serves the important purpose behind the Bankruptcy Code's "public access" provision.

The court concluded, after weighing the relevant considerations, that the speculative possibility of identity theft was not enough to trump the importance of the governmental interests behind s. 110 and s. 107.

Ferm then contended that s. 110(c) impermissibly discriminated between attorneys and non-attorneys. The disclosure is rationally related to the legitimate governmental interest in facilitating public access to the courts. The court concluded that this was enough to defeat Ferm's argument.

Ferm next argued that s. 110(c) violated his substantive due process rights by conditioning his continued work as a BPP on disclosure of his SSN in the public record. Ferm must show that s. 110(c) is "clearly arbitrary and unreasonable, having no substantial relation to the public health, safety, morals or general welfare. For the same reasons, Ferm had failed to satisfy this exacting standard.

Finally, Ferm argued that he came within the "reasonable cause" exception provided by s. 110(c)(3). This provision lets the court fine a BPP for failing to disclose his SSN unless "the failure is due to reasonable cause." After having been specifically notified by the court of the requirements of s. 110(c), Ferm deliberately chose to omit his SSN. The court found that in light of these facts, the district court did not err in concluding that Ferm had failed to show "reasonable cause" excusing his violation of s. 110(c).

Murtuza v. Gonzales (Attorney General), 04-2718 (7th Cir., Oct. 28, 2005)

This was a petition for review of a decision by the Board of Immigration Appeals denying the request to rescind a removal order against Murtaza. Murtaza argued that he did not get notice of the hearing.

Murtaza argued that he was the victim of identity theft. He claimed that whoever signed the adjustment application did so using his full name, but that the record showed that he consistently signs his name, using only the first initial as G. Murtaza. The name was also misspelled and finally the photo provided did not look like him.

The court concluded that it was hard to believe anyone else would want to use Murtaza's identity on such an application; even if it were successful the only one who would benefit would be Murtaza. The inherent implausibility, combined with the Immigration Judge's (IJ) observation about the similarity of signatures and addresses, lead the Court of Appeals to conclude that the IJ

did not abuse his discretion in finding that Murtaza did not meet his burden showing lack of receipt.

The petition for review was denied.

Sokolov v. Gonzales (Attorney General), No. 04-3218 (7th Cir., Mar. 24, 2006)

This was a petition for review of a decision of Board of Immigration Appeals (BIA). Sokolov was denied an application for asylum. While his appeal to the BIA was pending, Sokolov married a U.S. citizen. The case was remanded to the Immigration Judge to consider if Sokolov could adjust his status based on the marriage. The IJ denied Sokolov's application primarily because of his implausible explanation of a recent conviction for financial identity theft.

Sokolov was convicted in Illinois of financial identity theft for having obtained a state identification card in the name of his wife's ex-husband. Sokolov explained that he had found the expired identification card in the taxicab he was driving and, at the urging of his co-workers as a "bad-joke", obtained a new card with his own picture. Sokolov claimed that until he showed it to his wife, he was not aware that it belonged to her ex-husband.

The IJ noted that the circumstances and underlying facts of Sokolov suggest that he and his wife were aware that he had been ordered to leave the U.S. and 'concocted' an idea for the Sokolov to assume a new identity.

Sokolov argued that the decision to deny his asylum request is not based on substantial evidence and that the BIA abused its discretion by denying his adjustment of status based on the marriage.

In this review, the Government argued that the court lacks jurisdiction over both claims. The statute is clear that jurisdiction to make a determination as to whether a late application is timely or not rests only with the Attorney General and that no court shall have jurisdiction to review these determinations (8 U.S.C. § 1158(a)(3)). The BIA affirmed the IJ's asylum decision solely on timeliness grounds. The Court of Appeals therefore lacks jurisdiction over Solokov's challenge of the denial of this asylum application.

The Attorney General also has unreviewable discretion to adjust an alien's status (8 U.S.C. § 1255(a)). Such a door-closing statute precludes judicial review of "any judgement regarding the granting of relief under section 1255". The door-closing statute remains inapplicable to orders that violate the Constitution" and only egregious administrative irregularities may amount to constitutional violations. The court found no such problem in this case.

The petition for review was dismissed for want of jurisdiction.