



ARCHIVED - Archiving Content

Archived Content

Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.

ARCHIVÉE - Contenu archivé

Contenu archivé

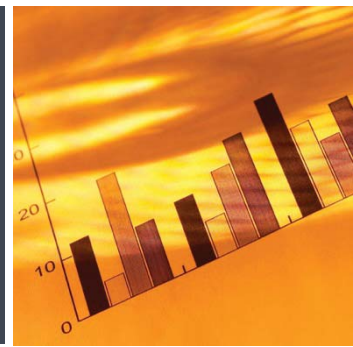
L'information dont il est indiqué qu'elle est archivée est fournie à des fins de référence, de recherche ou de tenue de documents. Elle n'est pas assujettie aux normes Web du gouvernement du Canada et elle n'a pas été modifiée ou mise à jour depuis son archivage. Pour obtenir cette information dans un autre format, veuillez communiquer avec nous.

This document is archival in nature and is intended for those who wish to consult archival documents made available from the collection of Public Safety Canada.

Some of these documents are available in only one official language. Translation, to be provided by Public Safety Canada, is available upon request.

Le présent document a une valeur archivistique et fait partie des documents d'archives rendus disponibles par Sécurité publique Canada à ceux qui souhaitent consulter ces documents issus de sa collection.

Certains de ces documents ne sont disponibles que dans une langue officielle. Sécurité publique Canada fournira une traduction sur demande.



EMERGING THREATS AND TRENDS IN MONEY LAUNDERING

In Canada, between CAD 5 billion and 15 billion is estimated to be laundered annually; worldwide the figure is between USD 500 billion and 1 trillion.

There are two pillars in most anti-money laundering (AML) systems: 1) prevention; and 2) enforcement. Prevention includes customer due diligence, reporting, regulation or supervision and sanctions. AML prevention depends on the financial institutions that act as the gatekeepers in the system, which assess and disclose the risks to the authorities “through the financial investigation unit (FIU), in the appropriate jurisdiction” (42). Enforcement includes forfeitures (criminal and civil), prosecutions, investigations, and predicate criminal cases (substantive offences other than money laundering, like drugs or fraud).

Drug trafficking continues as the major predicate crime for money laundering since it is a cash business. The risk of money laundering varies with the level of drug activity. Street level dealers exchange product for small denominations of cash. Mid-tier dealers try to ‘refine’ the money, seeking bills in larger denominations, to reduce its bulk. “Mexican cartels control 90% of the cocaine that reaches American streets (Simser, 2011) and smuggle the cash proceeds in bulk to countries where placement into the financial system is less scrutinized” (43).

Fraud is a different type of crime where cash is often not the medium of exchange. There are a myriad of illegal acts that fall under fraud, ranging from ‘Ponzi’ schemes to telemarketing and credit card scams. Proceeds from fraud move through traditional channels in financial institutions. It is sustained by ‘the patina of

In This Issue

Emerging Threats and Trends in Money Laundering	1
Organized Cybercrime?	3
Criminal Organizations and Conspiracy Laws Usage.....	5
Attempted Intimidation of Quebec’s Police Force	7

legitimacy’ designed to fool victims (both individuals and financial institutions). Financial institutions were deeply affected by the economic meltdown. In the US, more than 300 insured depository institutions have failed since 2007 (GAO, 2011). Once liquidity in the markets became an issue, there was, literally a ‘run’ on the Ponzi funds. Ponzi schemes present two types of risk to financial institutions. One, the fraudster launders victim money through financial institutions to offshore destinations such as Europe, Canada and Antigua. Two, beyond AML compliance concerns, there is a risk of civil liability.

The author reviews a number of emerging systems used for payment: new payment methods (NPM), prepaid access cards, electronic money, and person-to-person (P2P) loans. New Payment Methods were developed to address two kinds of market needs: 1) facilitate online transactions; and 2) help those who are under-banked. In the US, 4 million social security recipients lack a bank account and rely on prepaid access cards to receive a benefit. The Financial Action

Task Force (FATF) “concluded that NPMs are misused in three ways: as a method of third-party funding (using straw men and nominees); as an exploitation of the non-face-to-face nature of NPM transactions; and finally as an exploitation of NPM providers and their employees” (44).

Prepaid access cards are devices where the value is paid in advance and extracted later. They are used as prepaid credit cards. The card itself does not hold value, but allows access to a shared pool of funds. For example, a consumer swipes the card at the point of sale, the terminal verifies whether there is sufficient value to support the transaction; if the card’s issuer (or a third party processor) indicates ‘okay’ then the transaction proceeds. A notional hold is placed on the balance identified with the card regarding the purchase. The transaction is settled between the merchant and the issuer.

Commodity-backed electronic money, such as e-money or digital currency, potentially poses an AML risk. “A typical digital currency is backed by an asset” (46). An issuer holds bullion and contracts through exchange agents who sell the digital currency to end-users with cash or a wire transfer. The end-user can use the electronic currency online. Unlike credit cards, transactions are usually non-recourse nature (there is no charge back process to a merchant, and the currency provider will not refund a dissatisfied customer). The exchange agent can exchange e-money for a fiat currency, such as dollars, euros, and yen.

Internet-based platforms allow individuals to lend to other persons, either as an act of charity or to make money. A rapidly growing market segment is P2P lending. The for-profit platforms, such as Prosper Marketplace and LendingClub in the US, have facilitated 63,000 in unsecured loans worth USD 469 million by March 2011. A lender can advance all or part of a loan (in increments as small as USD 25) by purchasing payment dependent notes from a P2P company. The lender bears a risk of non-repayment. The P2P posts loan requests, interest rates and assigned letter grades (indicating credit risk). The P2P then works with a chartered bank such as WebBank of Utah who disburses the loan and assigns it to the P2P.

Money is collected by electronic funds transfer and the lender is repaid, less a service fee of 1 percent. The author notes that there is less than a 1 percent default rate on the top three grades of loan.

Three of the largest online gaming poker sites doing business in the US (Poker Stars, Full Tilt Poker and Absolute Poker) were indicted in New York in April 2011. The US Department of Justice alleges that the defendants have engaged in money laundering. “In 2006, the US Government, concerned about online gaming, passed a law making it a crime to accept payment for internet gambling” (47).

Gambling poses a significant AML risk. A launderer can go to a casino, place a few bets and then cash out; as a result casinos file currency and suspicious transaction reports to Financial Intelligence Unit worldwide. The same is true of online gaming. To access a poker site, a prospective gambler downloads their software, creates a profile and then funds an e-wallet. Pursuant to US legislation in 2006, companies like Poker Stars would issue the winnings in cheque form. The author states that the system, from an AML perspective, is only as strong as the electronic wallet provider uses ‘dirty’ money as a source of funds, then, a ‘clean’ cheque from an offshore gaming company will launder the money.

The FATF reviewed money laundering typologies in sports, concentrating on football. From their review, “the FATF have identified a number of AML risks associated with football clubs including:

- Football is a cash business (at the gate, in merchandise and in the concession booth). Football is also a business that needs large influxes of capital, which can be sourced from a variety of stakeholders, supporters and sponsors. Observers of the player transfer market know that money is not always spent rationally.
- The culture of football is important: owners acquire a social status; young players may come from socially vulnerable environments; the allure of the sport can give owners access to and influence over politically exposed persons (FATF, 2009:36)”

Using trade-based money laundering (TBML) schemes, Colombian cartels have laundered millions of dollars. For example, over-invoicing of emeralds, inferior stones injected with oil would be shipped. To a customs inspector the ‘shiny’ emeralds appear to have the attributed value. Clean money can be paid against the value of the emeralds and dirty money can be paid against the balance.

The author observes that “financial institutions are expected to play a role in combating trade-based laundering yet are not always in the best position to do so” (49). He adds that most international trade involves open account transactions where “the financial institution sends money at the behest of their client without review of the underlying trade documentation” (49).

The author reviews how money laundering infiltrates existing AML systems. He identifies certain risks that have emerged in certain systems that are shared and used to transfer value, be they online or in the form of a prepaid access cards. The author also looks at emerging unlawful activities that could give rise to new problems such as trade-based money laundering. He concludes that “to remain robust, systems need to constantly take note of emergent trends and threats” (51).

Simsler, Jeffrey. (2013). “Money laundering: emerging threats and trends,” *Journal of Money Laundering Control*, 16(1), 2013:41-54.

Associated Papers:

FATF (2009), *Money Laundering Through the Football Sector*, Financial Action Task Force, Paris July, p.42.

GAO, (2011), *Bank Regulation: Modified Prompt Corrective Action Would Improve Effectiveness*, GAO-11-612, June, Government Accountability Office, Washington, DC.

ORGANIZED CYBERCRIME?

Most coordinated cyber-offending does not meet the criteria to be considered organized crime, though some trading forums can be considered criminal organizations.

This study is based on an existing study consisting of interviews with Internet security firm officers, current and former law enforcement agents, former hackers, and analysis of legal documents. The research contained ideas that compared cybercrime to organized

crime. This study supplements that work with ongoing research to address these issues. The paper reviews academic definitions of organized crime, mafias and cybercrime. The author assesses whether online cybercriminal trading forums could be seen as mafias by some.

Organized crime can be viewed as a form of governance within the criminal world, which lies at the heart of Varese’s definitions of organized crime as “attempts to regulate and control the production and distribution of a given commodity or service unlawfully” (53). To Varese’s definition the author adds “a mafia as a type of organized crime that ‘attempts to control the supply of protection’” (54).

The author defines “cybercrime as the ‘use of computers or other electronic devices via information systems such as organizational networks or the Internet to facilitate illegal behaviours’” (54). He notes that he is focused on cybercriminal groups involved in profit-making activities instead of cybercrime focus on political (terrorism or cyber-activism) or malicious (online pedophilia or stalking) objectives.

Online trading forums have drawn comparison to mafias as these forums serve as online marketplaces for illicit goods and services. Some examples include the now defunct Silk Road and DarkMarket forums.

These forums have a generally defined hierarchy and agenda. An administrator manages a website; moderators are tasked with overseeing the forum and making sure that the rules are enforced by its members of various ranks whose status and privileges differ. As in other criminal groups, “one moves up the ranks by demonstrating their trustworthiness, ability or by offering favours to high-ranking forum members” (54). Their focus is business and profit instead of traditional ideological concerns of hackers.³

To classify such trading forums as mafia, one must answer the question of whether these forums “attempt to control the supply of protection” (55). Since there are “low barriers of entry in establishing such a forum, requiring relatively basic programming skills, and the vastness of the Internet” suggests that an Internet

monopoly in this area would be “a difficult proposition” (55).

The paper presents the example of Iceman, a hacker “who was the administrator of a major cybercriminal forum called CardersMarket. He launched a campaign to unify the major cybercriminal forums under his control. Using his high-level hacking skills, Iceman snuck into each site, stealing its membership information and other data. He then merged the cybercriminal membership into his own forum and took down the pre-existing sites. With the exception of DarkMarket, which would be at war with CardersMarket, all other sites were either destroyed or had their credibility irreparably damaged” (56).

The author observes that a key challenge to online trading forums being classified as mafias is that “it is difficult to classify these markets as criminal organizations at all” (56). He stresses that these should be seen as marketplaces, whereas, “the mafia is not a marketplace” (56). Although the mafia may seek to govern various marketplaces, its existence is distinct from the various enterprises it is involved with.

“The problem facing the conception of online forums as mafias is that their structure and organization appear to be tied to the site itself rather than to an autonomous group” (56). The author observes that “there is little evidence suggesting that the key forum officers belong to a defined and organized group outside of the forum setting” (56). He observes that major markets such as ShadowCrew and DarkMarket operate for a few years and tend to disintegrate when law enforcement scrutiny of their sites increases and its leaders are arrested. This contrasts with mafia groups that can be damaged by such scrutiny or arrests, but are able to limp on or rebuild, showing an institution that is ‘sustainable’ from its individual enterprises and ‘key leadership.’

Aside from trading forums, most documented forms of cybercrime do not fall under the definition of organized crime. First, many cybercriminal groups are small, loosely structured and without a clear plan. Second, other groups that are more tightly structured are categorized more as predatory cells than groups of criminal governance.

The paper identifies “some groups [that] have been emerging that might suggest an online appropriation of the role played by traditional organized crime groups in regulating or controlling the production or distribution of a product or service” (57). In one example, the “operations of a Turkish cybercriminal known as Cha0, who marketed and sold skimmers and PIN pads online, which could be attached to ATMs to record the card data and matching pins” (57) could be considered organized crime. Cha0 used his position as an administrator on DarkMarket to manufacture grievances against another skimmer salesman called Dron and had him excluded from the forum. This allowed Cha0 to become the primary provider of skimmers. Cha0 then changed his business model from selling skimmers to renting them out. The renters could only download encrypted data from the machines, for which Cha0 had the key. They would be forced to send this information back to Cha0, who would arrange for the card details to be ‘cashed out’, and then provide a cut back to the renters. “The genius of Cha0’s operation was that he effectively deputized all those who hired his skimmers into *de facto* members of his organization” (57).

Another area that shows similarities to organized crime is ‘bulletproof hosting’ where “the provider will not shut down clients whose activities are unethical or illegal” (57-8). Bulletproof hosting is attractive to cybercriminals and is known for providing services to pornography sites and spammers. The Russian Business Network (RBN), is one example of cybercriminals running a protection racket in 2008. “The claim was that RBN’s tactics were to monitor online discussion of web protective services by those running possibly nefarious websites” (58). The RBN would launch an attack on the sites via a third party and would then make an approach offering “protection of RBN services against such attacks for USD 2,000 a month” (58). Although other providers of web protection services exist, many of which are legitimate businesses, the shadowy operations of these sites make these venues less appealing.

There are a number of challenges to classifying the examples outlined in the study as fully fledged organized crime (58). The author states that there is no

analogous tool in the context of the Internet to control various markets. Exclusion from online groups and attacks of a platform are used for coercion and control, without long term lasting harm. Control over territory is more complex in cybercrime. Bulletproof hosting seems to provide some type of cyber analogy, however, bulletproof hosts are never completely bulletproof. The author adds that “when enough pressure is mounted, bulletproof hosts have been and continue to be cut off by ‘upstream’ providers, thereby also cutting off their clients” (58). “Conventional theoretical approaches and comparisons with traditional organized crime groups remain useful tools in understanding some of the issues facing cybercriminal groups and potentially explaining the approaches they take to address them” (59).

Lusthaus, Jonathan. (2013). “How organised is organised cybercrime?” *Global Crime*, 14(1),2013: 52-60.

Associated Papers:

Varese, Federico. (2010). “What is Organized Crime?” *Organized Crime: Critical Concepts in Criminology*, edited by Federico Varese, New York, 2010:1-33.

CRIMINAL ORGANIZATIONS AND CONSPIRACY LAWS USAGE

Increased police and prosecution powers in Canadian criminal organization legislation have been criticized as a threat to civil liberties.

The author reviews the use of criminal organization (a.k.a. “organized crime”) legislation in Canada and other Western countries, and highlights advantages and disadvantages of these laws. The paper also looks at the experience of the Royal Canadian Mounted Police (RCMP) using “criminal organization legislation and conspiracy laws to investigate and prosecute criminal groups” (1). Data for this study are based on case materials and interviews with 24 RCMP investigators, two prosecutors, and the author’s earlier study involving interviews with 70 higher level convicted drug traffickers (Desroches, 2005).

In 1997, Bill C-95 was enacted to target criminal organizations, which was followed by Bill C-24. “Bill C-24 defines a criminal organization as a group that (1) is composed of three or more persons in or outside Canada; and (2) has as one of its main purposes or

main activities the facilitation or commission of one or more serious offences that, if committed, would likely result in the direct or indirect receipt of a material benefit, including a financial benefit, by the group or by any persons who constitute the group” (2).

The law “broadens the scope of offences that define a criminal organization; creates a reverse onus provision in bail hearings and seizure of property and assets, provides a penalty of up to life in prison for anyone instructing another person to commit an offence for the benefit of a criminal organization, extends wiretap authorizations for up to a year instead of the normal 60 days, offers protection for victims and witnesses against intimidation, and provides a degree of immunity for undercover officers who commit crimes in order to infiltrate and investigate criminal organizations” (2).

The criminal organization statute provides the state with increased powers. Critics, of whom the author is one, state that these laws “lack specificity in defining exactly what is meant by organized crime” (3). He notes that many of the laws are based on stereotypes, such as “traditional mafia-style images of organized crime” with a centrally controlled hierarchical organization, exclusive and identifiable membership, and clearly defined roles (3). Yet research on criminal organizations involved in human trafficking and terrorism show that such groups are small, informal, and loosely structured. Findings from similar studies “suggest that higher level drug trafficking syndicates are made up of small criminal groups that are autonomous, decentralized, coalitional, situational, have no clear hierarchical structure, and collaborate with one another for their mutual benefit” (3).

The author states that existing criminal organization laws “make it difficult to prove ongoing group affiliation, association, and membership” (3). In one case involving the Hells Angels motorcycle club, “When the judge acquitted the only accused known to be a member of the biker gang, criminal organization charges were dismissed against the other defendants” (4).

The author adds that while some offenders have a central role, others are on the periphery, participating

in networks that overlap. Individual interaction with them can be sporadic and take place over long distances or international boundaries. These social networks are dynamic and change in form and membership over time.

In the “case (*R. v. Venneri*, 2012), the Supreme Court of Canada set the evidentiary requirements higher for criminal organization offences than conspiracy charges by requiring proof that ‘some form of structure and degree of continuity are required to engage in the organized crime provisions’ established under the *Criminal Code*” (4).

Criminal organization cases often result in large, cumbersome, resource- and time-intensive ‘mega trials.’ The delays this can create “can result in a case being dismissed on constitutional grounds” (5). For example, a Quebec judge tossed all charges against 31 members of Hells Angels due to unreasonable delays in bringing them to trial. The cost of prosecution was estimated at CAD 11 million, not including 4 million in courthouse renovations “to accommodate the massive trial” (6).

In 2010, a RCMP investigation of a human trafficking ring in the province of Ontario, the police arrested and charged 14 people with conspiracy to commit human trafficking” (6). Evidence showed that the accused lured 23 men to Canada with the promise of work. Instead, the men were forced to work for little or no pay. “Language barriers and threats from their captors prevented the victims from seeking help from the authorities” (6).

“The homogeneous and structured nature of the human trafficking group made it relatively easy for the Crown Attorney to make a case that the accused were part of a criminal organization” (6). All defendants were members of an extended family from Pápa in Hungary. “Most had criminal records in Hungary and all had lied to the Canada Border Service Agency in claiming refugee status” (6). The evidence also showed that all members were engaged in activities of recruiting, supervising, housing, and transporting victims to further the human trafficking activity.

The RCMP seldom uses criminal organization laws instead, it lays conspiracy charges. An “essential element of a conspiracy is an agreement by two or more persons to commit a criminal offence” (7). Section 465 of the *Criminal Code* allows for individuals to be tried in Canada even if the conspiracy occurred elsewhere. “The court is also allowed to draw inferences from person’s actions that an agreement existed to engage in criminal activity” (7).

RCMP Drug Squad investigators realize that higher level drug traffickers use third parties to avoid being caught, however; these dealers must communicate and collaborate with others to purchase and sell their product. Consequently, investigators gather evidence of associations, meetings, taped conversations and supporting documents and drug seizures to show involvement in drug trafficking. For example, in a study of 70 higher level drug traffickers, the majority of the dealers were convicted on conspiracy charges. Most stated that their downfall was due to lack of understanding of conspiracy laws. “Conspiracy law works best in countries in which the content of wiretaps is used evidentially” (7).

Drug networks form a chain in which the money moves upwards to the supplier, while the narcotics move downwards from the supplier to distributor to the end user. Conspiracy laws allow the police to charge and convict offenders who play key leadership or organizational roles within a network, despite the fact they avoid committing overt criminal acts. “This means the police can be proactive and arrest suspects before they commit a violent offence” (8). “Another advantage of conspiracy laws is that the state does not have to prove that the defendants were members or were engaged in crime for the benefit of the criminal organization” (8).

Canadian law permits the judge to draw attention to the fact that the defence failed to explain the conduct of the accused. In absence of a plausible account by the defence that counters the state’s conspiracy theory, juries are likely to convict.

The author concludes that Canada followed the lead of other Western countries in passing legislation to give law enforcement authorities greater powers and harsher

penalties to assist in the investigation and prosecution of the crime. Canada's laws have been criticized for infringing on civil liberties, using vague and inaccurate definitions for organized crime, and for giving rise to expensive 'mega trials.' Prosecutors have faced setbacks due to higher evidentiary standards and mega-trials forcing cases to be dismissed.

Instead, the RCMP rarely uses organized crime laws in pursuit of certain criminal groups, such as higher level drug traffickers. In most cases, they rely on conspiracy charges which are easier to prove because they focus on criminal conduct as opposed to the structure and functioning of the group. The author anticipates that this practice will continue unless definitional and evidentiary issues are resolved.

Desroches, Frederick J. (2013). "The Use of Organized Crime and Conspiracy Laws in the Investigation and Prosecution of Criminal Organizations," *Policing*, (February 4, 2013):1-10.

ATTEMPTED INTIMIDATION OF QUEBEC'S POLICE SERVICES

Outlaw motorcycle gangs have been increasingly intimidating police officers in Quebec. Patrol officer behaviour is impacted more than that of investigative officers.

The author shows how criminal organizations, such as the outlaw motorcycle gangs (OMGs) in Quebec, (mainly the East Coast chapter of the Hells Angels) use intimidation to influence behaviour of persons in the judicial system, particularly police officers. Two main tools were used in this research. The first main source was the database of Quebec's Provincial Police (la Sûreté du Québec) Intimidation Project. The other source was based on interviews with 20 Quebec police victims of attempted intimidation by OMGs.

In the 2001 annual report on organized crime of the Criminal Intelligence Service Canada (CISC), OMGs "in Canada continue to use violence, ranging from intimidation and assault, to attempted murder and murder to promote and protect the gangs' interests" (67).

"The database was used for compiling all intimidation events associated with local or distant organized

crime" (69). This allows for assessment of intimidation trends and measurement of the extent of the phenomenon in the province of Quebec. Sampling criteria used in the study are: (i) the period 1999 to September 2001 inclusive was chosen; (ii) the sample included all members of the police victims of attempted intimidation, persons having a relationship with a police officer and third-party civilians involving a police officer; (iii) all incidents aimed at police organizations, such as police services, premises or vehicles were included; and (iv) suspects closely or distantly belonging to OMG.

The author describes the Hells Angels' hierarchical structure based on the CISC 2001 report. Each biker has a specific role and title within the organization. A 'chapter' represents the gang on a given territory, and "is run by official 'regular members', who wear the 'colors' (signs and logos) of the Hells Angels on their jackets" (69). Below this are the 'prospects', who are would be members of the chapter for one year. Lower in the hierarchy, the 'hangers-on,' who hope to become 'prospects.' Around them are people with different interests. The 'puppet clubs' are in a subcategory and work in a smaller territory, sharing the same organizational structure, including 'regular members' followed by would be members known as 'strikers' and the 'hangers-on.' All wear the 'colors' of the 'puppet club.' The 'friends' and 'relations' are often persons in business with the official 'chapter' or the 'puppet club' and do not wear the 'colors.'

Attempted intimidation of police officers rarely takes the form of physical aggression. Instead, it is based on vague and diffuse menaces, such as references to the police officer's personal life. Acts of evoking personal traits of the officer's spouse or his children aim to destabilize the officer. Some OMG "follow the police officer or his wife to their private residence or telephone him at home" (71). Other intimidation efforts aim at destroying the police officer's career via "criminal and civilian lawsuits, as well as complaints to the committee of deontology," which reviews the nature of policing obligation and ethics, to weaken the police officer's will while undermining their credibility (71).

Attempted intimidation occurs when OMGs “depart from the rules tacitly established and attempt to impose their own way” (72). Some police officers become targets due to their overly authoritarian and repressive behaviour. “The level and nature of intimidation exerted by OMGs on investigating police officers differs from that exerted on police patrol officers” (73). “Patrol officers lack the necessary training to deal with organized crime” (74). Knowledge of criminal circles is held closely by investigating officers, who “perceive the tacit game rules established between OMGs and police officials” (74).

Confronted with attempted intimidation, patrol officers react in three different ways. The first group avoids encounters with OMGs as much as possible to prevent potential problems in their private life or career. The second group “includes a restricted core of very active and brave officers who have chosen to specialize in organized crime” (75). The last group consists of provocative patrol officers who ignore police norms when seeking to catch OMGs.

In relation to the research data, the author states that a funnel with three levels was drawn to show the effects of attempted intimidation. Each level reduces the number of police officers willing to specialize in fighting organized crime. In the first level, “the effect of attempted intimidation is widespread and affects only patrol officers and their discretionary power” (76). “Concern about their personal and professional lives discourages patrol officers from intervening against OMGs” (76). The fear that is felt is a potential menace rather than a real one.

“The second level of the funnel includes patrol officers who have voluntarily chosen to fight organized crime.”(77) Their fears are based on the real menaces to their family, where OMGs have tried to get rid of them. The last level of the funnel consists of investigating officers specialized in OMGs. “They are less intimidated due to their authority and respect they inspire in criminals.”(77)

The author states that the research findings show that there is a gap between the training given to patrol officers and the solutions foreseen by interviewed police officers. He views that training on this type of

criminal and their networks could “invigorate the interest of reluctant patrol officers” (77). He adds that it “appears necessary to develop effective intervention methods to avoid police excesses while acting against acts committed by OMGs” (77).

The author suggests that “it may be pertinent to adopt measures aimed at better protection of police officers who are unnecessarily sued by OMGs as well as at ensuring that their personal data are not disclosed”(78). He adds that “the findings of this study indicate a substantial gap in circulation of information within police services” (78). The author notes that “article 423 was introduced in the *Criminal Code*” to fight intimidation committed against law enforcement officers (78).

The author concludes that “the picture of intimidation appears to be more complex” (78). Due to the impact of attempted intimidation on their personal life and work, a large number of patrol officers adopt a conservative attitude. He adds that “with the many arrests of Hells Angels members in the last few years, one should question whether this attempted intimidation phenomenon will not shift to places where Hells Angels are more present: judicial courts and penitentiaries” (79).

Gomez del Prado, Grégory. (2011). “Outlaw motorcycle gangs’ attempted intimidation of Quebec’s police forces,” *Police Practice and Research*, 12(1), 2011:66-80.

Associated Papers:

CISC *Annual Report on Organized Crime in Canada 2001*, 2001: 55p, [accessed 2014-04-11] from: http://www.cisc.gc.ca/annual_reports/documents/2001_annual_report.pdf

For more information on research at the Community Safety and Countering Crime Branch, Public Safety Canada, to get a copy of the full research report, or to be placed on our distribution list, please contact:

For further information:

Research Division
Public Safety Canada
340 Laurier Avenue West
Ottawa, Ontario K1A 0P8
PS.CSCCBResearch-RechercheSSCRC.SP@canada.ca

Research Highlights are produced for the Community Safety and Countering Crime Branch, Public Safety Canada. The summary herein reflects interpretations of the report authors’ findings and do

not necessarily reflect those of the Department of Public Safety Canada.

ISSN: 1927-808x

© Her Majesty the Queen in Right of Canada, 2015

This material may be freely reproduced for non-commercial purposes provided that the source is acknowledged.