

**NOT FOR CITATION OR CIRCULATION WITHOUT PERMISSION OF THE
AUTHORS**

**CHEATS AT PLAY: THE SOCIAL ORGANIZATION OF VIDEO LOTTERY
TERMINAL FRAUD**

Working Draft

By

**Dr. John L. McMullan
Professor of Sociology
and Criminology
Saint Mary's University
Halifax, Nova Scotia, Canada
john.mcmullan@stmarys.ca**

**Dr. David C. Perrier
Associate Professor of
Sociology and Criminology
Saint Mary's University
Halifax, Nova Scotia, Canada
david.perrier@stmarys.ca**

@ 2002

**Paper presented at the Gambling, Law Enforcement and Justice System
Conference, Alberta Gaming Institute and University of Alberta, March 2002,
Edmonton, Alberta**

Introduction

Gambling in Canada has been stimulated by the decriminalization and subsequent legalization of new products and services, and by the consolidation of provincial governmental authority over many gambling markets, policies, regulations, operations and profits. The proliferation of “grind gambling” in the form of video lottery machines (VLTs) and casino-based slot devices has not only extended the scope of gambling, it has radically reordered the entertainment industry, consumer spending patterns, and prevalence gambling rates, while adding to both government revenues and associated social costs (Azmier, 2001; Campbell and Smith, 1998; Marshall, 1996a, 1996b, 1998; McMullan, Perrier and MacDonald, 2002; National Council of Welfare, 1996; Smith and Azmier, 1997). Much research, it seems, has been designed to improve the industry’s sensitivity to the market, provide advice to political decision makers and control the industry’s darker sides. Social research, while sparse, has emphasized the demographics and psychographics of player involvement, the social and economic benefits and costs of gambling and the individual and social pathologies that the industry produces (Black, 1996; Campbell and Smith, 1998; Henrikssen, 1996; McMullan, Perrier and MacDonald, 2000, 2002; Seelig and Seelig, 1998; Smith and Azmier, 1997; Smith and Hinch, 1996).

In addition, the gambling marketplace in Canada includes a viable illegal industry with strong criminal norms and a proven ability to survive over time in an era of liberalized legal tolerance. Legalized gambling has not displaced illegal

gambling and, if anything, the relationship between the two sectors may be symbiotic and supportive of mutual growth (Goodman, 1995a, 1995b). Yet the study of illegal gambling and gambling's relationship to crime is under-researched and poorly understood in Canada. Recent academic work, however, has studied organized crime's ability to penetrate casino gambling by laundering money and corrupting elected and appointed officials (Beare and Schneider, 1990; Beare, 1996), compared the competition between legalized sports lotteries and illegal bookmakers (Smith, 1990), investigated the unethical, international resale of lottery tickets by Canadian telemarketing and mail-order companies operating in the United States (Campbell, 1996), and examined the many myths surrounding gambling and crime in Western Canada (Smith and Wynne, 1999).

Indeed Smith and Wynne (1999:49-69) suggest that gambling related crime in Canada can be classified in a threefold manner: (1) illegal gambling as prescribed by the Criminal Code, by which they mean unlawful sports betting and card clubs, unlicensed electronic gambling devices, offshore lottery sales, internet gambling and so on; (2) crimes associated with a gambling milieu, for example race fixing, counterfeit transactions, cheating at play and stealing between players at gambling sites that are directly related to gambling, or illegal substance trafficking, car theft, embezzlement and fraud that are peripheral to gambling proper, but which are linked indirectly to a gambling environment; and (3) crimes committed by disordered gamblers, by which they mean acts such as check forgery, theft, credit card fraud, burglaries and so on that uncontrolled gamblers commit in order to

continue to play or to pay off gambling debts.¹ Crimes associated with categories (1) and (2) can range from small scale "hustles", to insider work crimes committed by operators, dealers, and pit bosses, to the provision of an alternative underground economy service, to well organized international conspiracies involving dozens of participants operating at multiple sites in transnational settings. Crimes associated with category (3), they say, are committed mostly out of a sense of desperation. These include conventional crimes such as prostitution, thieving and burglary but more frequently white collar crimes that entail strategic planning and non-violent, stealth techniques. Disordered gamblers are especially prone to criminal activities with anywhere from one-half to two-thirds of them reporting illegal conduct to finance their gambling habits (Rosenthal and Lesieur, 1996; Walker, 1997; Smith and Wynne, 1999:24-27, 67-69).

The relationship between gambling and crime is thus complex and ambiguous. The recent academic research on casino gambling and higher crime rates, for example, cannot confirm a direct casual connection or correlate the short term or long term community impacts of this gambling format (Sternlieb and Hughes, 1983; Hakim and Buck, 1989; Giacomassi and Stitt, 1993; Zendzian, 1993; Kindt, 1994; Chang, 1996; Stokowski, 1996a, 1996b; Thompson, Gazel and Rickman, 1996b; Grinols, Mustard and Dilley, 1999). Nor is it certain as to what type of gambling is more criminogenic than others. The fragmentary evidence suggests that there are numerous crime costs associated with most gambling venues and that lotteries, casinos, horse tracks, bingos, electronic gambling machines, and the internet have all

generated diverse types of criminal activities such as lottery fraud, money laundering, race fixing, "bingo-gate", electronic crime and internet fraud, to name a few (Rosecrance, 1990; Beare, 1996; Campbell, 1996; Reuter and Rubinstein, 1982; Liddick, 1999).

Video lottery terminal gambling, however, has been identified by law enforcement authorities as a source and a site for much crime. It has been associated with a large "black market" in illegal gambling machines, and linked to several influence peddling schemes and rackets. Indeed the tendency for VLT machines to encourage continuous play is said to have resulted in desperate illegal acts in most locations where these machines have been legalized (Nova Scotia Department of Health, 1998; Smith and Wynne, 1999; MPM Gaming Research, 1999). Yet there has been little academic research on the topic of VLT based crime in general and, virtually no research on crimes that are directly associated with this type of gambling and its immediate environment.

In this paper, we study the criminal organization surrounding a cheating at play project that occurred in the Province of Nova Scotia over a 4 year period ending in June 1998. It involved a well orchestrated and highly sophisticated series of electronic frauds which allowed a criminal group to: (1) predict the random number generator and then gain winning outcomes on VLT machines; (2) alter the VLT on-board random access memory (RAM) and/or the VLT storage device (EPROM) to either predict and trigger the bonus meter feature or modify the pay-out schedule to increase the profits for a winning combination; and (3) manipulate the VLT on-board

RAM and random operating memory (ROM) so as to disconnect the terminal and put it in off-line, stand alone mode without the knowledge of the industry regulator².

This paper is organized as follows. First, we present our perspective on criminal organization. Second, we discuss our research methods. Third, we study in detail the technical skills surrounding electronic fraud in the VLT industry. Our concern is to concentrate on the organization of VLT crime as rationally geared to confronting *technical* problems of social order. Fourth, we analyze the *social* organization of VLT crime and examine how the criminal organization routinized illegal acts, managed social surveillance and handled law enforcement. Finally, we conclude our case study by discussing why the organization of crime is best seen as associated with the conditions of social control.

Criminal Organization

Criminologists, sociologists and legal researchers have for so long treated crime as an individual deviation from group norms or laws that they have not always appreciated that crime is also a rational, collective activity. They often start by puzzling about why some people stray from the straight and narrow path; when they have exhausted the study of individual traits and personality characteristics they typically turn to consider the individual's social position, community, subculture, relations with family and peer groups, official labeling by police, courts and corrections, prison cultures, and so on. In effect, these types of social explanations approach illegal and criminal activities, not as subjects in themselves, but always with the question: how do they determine individual activity?

In the approach adopted here, VLT crimes are treated as activities that are rationally geared to the conduct of the illegal behavior in question. They have their own patterning and continuity and possess a degree of uniformity and autonomy in the sense that the main elements explaining their organization may be found within the illegal activity and the problems confronted there. This explanatory approach emphasizes: that at a given stage of social and technological development, a given illegal act presents certain technical and social problems which must be resolved for its successful completion; that we can identify the most efficient types of organizations for managing those problems and that the existence of these kinds of organizations are explained in terms of their technical efficiency in the situation at hand.

Cressey, (1972, Mack (1972), McIntosh (1975), Cohen (1977), Chambliss (1978), Block and Chambliss (1981), Best and Luckenbill (1982), Clinnard and Quinney (1983), Sutherland (1983), Reuter (1985), Haller (1990) and Potter (1994), to name some of the more important scholars, have developed substantial theoretical work on the topic and proposed different schemes of organizational rationality. Clinnard and Quinney (1983) emphasize four characteristics: the criminal career of the offender, the group support for the criminal behavior, the connections between criminal wrongdoing and legitimate institutions, and the social reaction to the crime. Using this typology, they have provided a number of useful descriptive accounts of the criminal organization of shoplifting, forgery, and counterfeiting, for example. Sutherland (1937), likewise, identifies "essential characteristics" of competent crime:

non-violent techniques, status gradations in the crime group, belief systems, differential learning processes, sponsored memberships, and organization by which he means the sense of informal unity and reciprocity which coordinates and structures members' participation. These categorizations have informed much subsequent research on criminal organization and indeed on professional crime. They delineate distinctions between random, amateur and structured crime and create a sense of order among a plethora of ethnographic, life history, and biographical accounts. But the cumulative result, while useful, is somewhat unsystematic and many of these typologies are really reformulations of commonsense categories in more technical and articulate forms.

Two works which deal systematically with variations in organization and which deploy organizational ideas rather than lay categorizations are Donald Cressey's *Criminal Organization* and Mary McIntosh's *The Organization of Crime*. Cressey (1972), for example, catalogues six varieties of criminal organization in terms of a series of "key positions" that are tasked with increasingly complex responsibilities as the organization becomes more rational. Thus at the top end, variety A is distinguished by having positions for "commissioners" who meet to coordinate the illegal activities of a confederation or cartel of multiple subunits, while at the bottom end of the scale variety F has only a role for a "task force guide" in the immediate act of crime. Cressey is able to write of specific kinds of criminal organizations assembled and staffed for a wide variety of different criminal activities including extortion, long term fraud, and for specific criminal interventions such as bank robberies, check-

forgeries and automobile thefts. He appears to assume that any kind of profitable criminal activity can be conducted by his most developed form of rational criminal organization, and that the forms of organization at the lower end of the scale are subsystem parts of a more complex rational form.

McIntosh (1975) questions the evolutionary character of Cressey's theory and suggests that the dynamics of organizational growth and change are diffuse and context bound. While Cressey sees the impediment to rational criminal organization to be ignorance or short sightedness on the part of criminals, or alternatively effective law enforcement by the police, inspectors and other regulators, McIntosh insists that there is no progressive tendency towards rational centralization. It is normal and routine for crime networks to be diverse and specific because "in different social contexts the problems confronted by criminal groups, and therefore the appropriate organizational solutions will vary" (McIntosh, 1975:17). She is able to identify four varieties of criminal organization which she calls picaresque, craft, project and business (McIntosh, 1971, 1973, 1975).

Each of these is a typical form of organization for groups of criminals engaged in a specific range of criminal activities in a specific type of society. Thus the picaresque kind of organization occurs in largely rural societies and is typical of bandits, pirates and brigands. It is a fairly permanent gang structure under one persons leadership, sometimes with a few supporting officers. Profits are shared among the members according to rank. These groups operate in the interstices of weak state power. They are often known in local communities and they cannot

completely cut themselves off from contact with other people: craftsmen, merchants, traders, guardians of estates, servants of households and state officials. To emerge safely from these encounters pirates and bandits make use of superior force, surprise attacks and quick escapes. They seek out safe havens – friendly ports and mountain sanctuaries – from which they plan their activities and escape the reach of law and social control (Hobsbawm, 1969; McIntosh, 1975: 29-35; Chambliss, 1989).

The business organization, typical of racketeers who supply illegal goods and services and who have gained some degree of immunity from legal control, is the largest in scale and the most permanent and advanced in her typology of criminal organization. It is composed of a hierarchy of agents who engage in relatively specialized activities and who are either paid by their superiors or offered a share of the profits in a particular market sector. Business criminal organizations, however, are more difficult to delineate than other criminal types. The division of labour needed to engage in a successful crime of this sort is the most complex, and business organizations need to both neutralize state control through systems of corruption and acquire legitimacy by engaging in legal business ventures such as transportation, currency exchange, real estate, restaurants, bars, nightclubs and the like. The boundaries of the organization are therefore often in flux and methods such as loyalties to criminal norms, violence, control over law enforcement regimes and efficacious and profitable racket management are central in controlling competitors, subordinates, and customer-victims. As McIntosh (1975:58) puts it criminal business organization “depends, in a way that no other organizational system does, on

relationships with non-criminal sections of the society that are built up interactively over time.”

Cressey’s and McIntosh’s approaches share the same logic as ours: treating the rationality of an organizational form as a explanation of its existence. Many criminologists see social control as a reaction to deviance. They are chiefly concerned to explain why people become deviant or else to investigate the effectiveness of social control institutions. In this paper we explore the proposition that radical deviancy theory and social constructionism have formulated; namely that deviance does not exist without social control, nor crime without law. Because we are concerned with collective behavior, that is the pattern of relationships *between* individuals and not individual conduct per se, we deploy organizational concepts that can be combined and recombined for a variety of purposes. These concepts which explain the internal organization of groups in terms of their technology of production and development and which explain the division of labour among groups in terms of market conditions and technology are, in turn, related to concepts concerned with social control, relations with clients and victims, and so on.

This leads us to situate electronic forms of crime within the specific structures of social control: opportunities for crime, crime prevention, law enforcement and systems of penalty. In attempting to “cheat at play” on VLT machines, we ask what types of technical problems had to be overcome and solved for a successful criminal outcome? Furthermore, since many of these technical problems are also social in nature, we ask what criminal division of labour was needed to accomplish the illegal

activity and how did it handle problems of opportunity, access and work safety, property protection, site surveillance and detection, law enforcement and relations with site owners, other customers and victims? The criminal group is thus seen as embedded in a larger social configuration, and criminal technology is the pivot in the relationship between the criminal organization under study and the wider social organization that it is a part of. The larger configuration is always changing and these changes, in turn, also affect the criminal group sometimes in a way to transform it or, as we shall see, sometimes in a way to vary the very conditions for its success and existence.

Methodological Issues

The case of video lottery fraud came to our attention via people in the security branch of the Atlantic Lottery Corporation when we interviewed them in May of 1999 for a research project on the social impacts of gambling. We were especially interested in this case because of the organizational complexity of the crime and because its discovery and resolution had a major impact on the Atlantic Lottery Corporation security system. As one officer explained:

We had to hire a specialist to come in ... to understand how this individual hacked into our machines My interest in the case was very specific, rather callous If I could convince this fellow, with the cooperation of the RCMP that we should have a little chat and find out what is transpiring, well then at least we know what he knows and we can put something in place to prevent it later.

The upshot of this approach was that one of the offenders provided a series of technical demonstrations on how the crimes were committed and agreed to detailed

interviews about how they were organized. These were videotaped and recorded over a three day period and resulted in the accumulation of over one hundred pages of archived materials.

In September of 2001, we entered into a series of discussions with the Atlantic Lottery Corporation and their legal counsel to obtain access to the written texts and the videotaped materials. In December of 2001 we were granted permission to take notes from these materials provided that we did so under their supervision at their headquarters in Moncton, New Brunswick, and provided that we presented and published our results without attribution. We agreed to both of these conditions and in early January we spent two days at their office reviewing the written materials and interviewing staff members. This data was especially detailed and complete. We extracted information from interviews, test documents and investigative reports, and clustered it according to specific questions and themes. Questions and gaps in the data were supplemented by six interviews with members of the sales, security and enforcement, and technical departments of the Atlantic Lottery Corporation.

The qualitative data allowed us to piece together a relatively coherent picture of the social organization of video lottery fraud. In particular, we were able to detail the different illegal techniques of fraud, the size of the criminal unit, the division of labour, the economic value of the crimes and the modus vivendi between the criminal organization and systems of protection, surveillance and legal control. To date we have been unable to conduct direct interview based research with the offenders. This would further clarify and confirm our organizational analysis, and

extend our understanding to include the relationship between ideology, character and social structure as it relates to the criminal activity. We are now in the process of attempting to contact the principal perpetrator of the fraud. So we realize that we are some way from a complete analysis, but this paper is a first step in moving the research boundaries concerning VLT crime beyond simple impressions.

The Techniques of VLT Crime

Thefts and frauds can take a number of organizational forms. Some can be structured on a craft basis involving small permanent work teams, subtle techniques of stealth and deception, small takes, and always avoiding risk in favor of future criminal conduct. Many of the tricks, cons, and swindles associated with early gambling related crimes in bowling alleys, boxing matches, pool rooms, race tracks and casinos were organized in this manner and they have shown a remarkable capacity for survival both individually and as a type (Skolnick, 1980; Rosecrance, 1990). However, as the technical problems confronting criminals became more complex, the organizational forms that they developed became more sophisticated and better orchestrated. Thefts and frauds became organized as “projects” that were larger in scale, greater in risk, more complex and technically advanced, and less routinized. As Einstadter noted (1969:76), criminals and their opponents were often engaged in “all out military operations” in which each side improved its techniques to try to outwit the other side.

VLT frauds have been conducted in a number of ways. One form is a deceptive gambling practice known as “ghost programming” or “gaffing,” which

typically lowers the required minimum payout percentage of a machine, so that the player no longer has a fair chance of payback. Ghost programs are usually executed by pushing a numbered combination of buttons on the exterior of the machine. Once initiated it is virtually undetectable because it simulates a legitimate program. This allows the site holder or operator to derive more money from the VLT device because there are fewer payouts to players. A second deceptive gambling practice is known as the “near miss program” which excites players to believe that a winning payout is imminent. The program determines in advance if a play is a loss, searches the machine’s memory for a combination close to a winning play and then displays those features. Players are led to believe that they almost won and that a winning combination is about to appear. This seduces players to play continuously and increase their bets even though their chances of winning are statistically impossible (Aronovitz, 1997: 625-626). A third fraud technique involves obtaining the source code of a VLT machine and using that code to calibrate the payout sequences in order to manipulate a jackpot. The criminal skills are stealing the source code without the manufacturer’s knowledge or working “insider arrangements” to obtain the code to manipulate a gambling machine to pay out on a predictable basis. This requires advance planning, information gathering, surveillance, accomplices and sometimes silent partners.

However in our case study the technical problems to conduct the fraud required more elaborate techniques because obtaining the source code was not the preferred “solution” to committing the crime. Instead techniques similar to “gaffing”

or “ghost programming” were developed to literally “crack” or disassemble the VLT machine’s code. The first type of technique required an extensive knowledge of microprocessors, micro-controllers, hardware, mathematics, and computer programming and programming languages. According to one technical expert who interviewed the offenders, their knowledge was equivalent to that of “a highly experienced electrical/computer systems engineer ... with five years of experience in the relevant area.” The fraud group had “thorough knowledge of gaming terminal implementations” that had been acquired over an “extended 5 year period of trial and error experiments on the manufacturer’s software and hardware.” This included: (1) producing and modifying electronic chips in the “grey market” before and after legalization of VLT gambling and (2) creating “hack programs” that could simulate (a) the forward progress of the random number generator (RNG) in a gambling machine; (b) decode the RNG seed values and mapping algorithm of the machine; (c) fabricate a phantom computer terminal that was an exact replica of a real VLT screen; (d) discover and disarm the security cycling or iteration mechanisms within an electronic device; and (e) solve complex equation problems (TX Programs) in short search time frames, in order to mathematically produce, predict and play the win sequence in a timely manner. As one security officer noted after interviewing one of the major participants:

He is very knowledgeable with communications.... He also has the capability of downloading, reverse engineering and going right to the basic language and reading it. He can read computer language like you can sit down and read a text book, newspaper, whatever and he does it right off the screen.

In order to understand the social organization of this fraud, it is necessary to provide some information on video gambling devices and pseudo random number generators (RNG) and their use in electronic gambling. Video gambling terminals are run by complex computer logic boards and not by inner governing and timing mechanisms. They are constructed on a number of reel strips, each of which consists of the games' symbols combined in a pre-defined order that operates according to pseudo random number generators (Aronovitz, 1997:621-622). These are mathematical algorithms that use numerical inputs (seed X) to produce numerical outputs (seed $X+1$). The results are then fed into the algorithm to produce the next result and so on. The action of feeding a seed into the RNG to produce an output is called an iteration or cycle of the RNG. These algorithms are used to produce a sequence of numbers, which when considered as a set of numbers display random characteristics. Given a particular input seed (X), it is possible to ascertain the next output number in the sequence by using the formula. Conversely, if the output seed ($X+L$) is known and the formula is known it should be possible to determine the input seed (X) (Aronovitz, 1997:629-631).

In the case of the VLT devices that were defrauded, the reel strip for each reel consisted of 24 symbols or stops. The reel stop is derived from the RNG output, but, the RNG output is always far greater in magnitude than the maximum 24 reel stops. For payouts to occur, however, the machine reduces outputs to a value between the lowest and highest reel stop number. This scaling down or mapping process means

that many outputs (seeds) are ordered to map to similar reel stop values without biasing any reel stop to occur more frequently than others. That is one reel stop number is not favored over another and the terminal output should be unpredictable. In addition to algorithm and RNG mapping, cycling the RNG before and during games is designed to scramble game outputs so that the next one cannot be known in advance.

The fraud team was able to exploit the deterministic qualities of pseudo RNGs and the poor design and implementation of the output determination process. Their technique was based on observing screen outcomes in order to predict and produce profitable payouts. Their first tool was a "C" program that simulated the RNG algorithm. Over the years from 1993 to 1997, one group member had developed an extensive database of over 20 gigabytes of information that listed all of the gaming combinations that had the 24th reel stop on the first two reels and the corresponding RNG seeds that generated the respective screen³. Their second tool was computer programs that searched for the machines' payout combination in the random numbered sequence. These programs were devised to uncover the number of RNG iterations and the number of games required to call up the payout combination on the VLT machine. Their tactics were as follows: first, games would be played on VLT machines at a particular operator's site until the 24th reel stop on both the first and second reel was observed; second, with this information one person would search the database and locate the possible RNG seeds that could produce this exact screen image; third, the same person would iterate the RNG simulator using these possible

seeds and compare the screen output from their simulator to that of the next game on the terminal, thereby locating the correct seeds; fourth, they would then search the sequence of the RNG seeds and the corresponding screens to determine the number of iterations required to generate precise combination payouts; finally, in concert with other team members, they would deploy a minimum betting strategy on a targeted machine until a few games before the payout game, where upon they would use the maximum multiplier to take advantage of the “fever mode” feature which awarded them continuous payouts and higher than average returns.

The process of cycling also had to be overcome by the crime group. Changes made to the game chip technology in the mid 1990s incorporated a security form of cycling during idle mode. However, the protection afforded by this improvement was easily breached. The RNG algorithm was not changed in the new chip and with trial and error experiments the criminal group was able to determine that the rate of iteration was actually constant and predictable. Furthermore, they discovered another flaw in the terminal software; once the bet button was held down the software waited for its release, and the RNG cycling was immediately suspended. This meant that the fraud team could determine the place in the random number sequence where the generated numbers actually originated. They no longer needed to take the risk of playing poker games on VLT terminals to synchronize the RNG and predict their payouts. The VLT terminal could now be left to cycle in idle mode. Then at a number of iterations (for example 50) prior to the payout combination, the bet button would be alternately pressed and released to reveal a screen output thus

interrupting and releasing RNG cycling. This screen output was matched on the simulation program allowing precise calculations to carry out the crime more quickly and efficiently with less monetary outlay up front. As one security officer put it:

When the machine was changed and there was still a flaw in it, what he was able to do was save his nickel a plate because he knew that the thing (machine) would iterate so many times in a minute. So all he had to do was let it go wild for 17 minutes and he knew it moved ahead 3000 games. Then he stopped it, then he would up his bet to \$2.50 and so we made it faster for him by improving it (machine) and made it cheaper for him by improving it (machine).

The second type of technique required an advanced knowledge of the logic area of the machine as well an ability to access it. One version exploited bonus prizes that increment when a particular combination is achieved on the VLT screen. When the bonus prize reaches a maximum value, that value is displayed on the game screen and then awarded to the player. Although the Video Lottery Corporation master meters are stored in critical memory and are regularly copied in different physical RAMs, the bonus meter feature was not part of critical memory and so RAM storage was neither multiple nor regularly validated. In order to accomplish this deficit fraud technique, it was necessary for members of the criminal group to access and remove the machines' back up memory boards from the main logic boards, and observe the contents of RAM by using a commercially available reader program device. They then had to locate the bonus meter in RAM, modify a back up RAM board that substituted non-volatile RAM for volatile RAM without loss of data, and manipulate the contents of the bonus meter memory logic to a score just below the bonus meter maximum. The RAMs were reinstalled and the game was played until the bonus

was triggered. The credit meter was then cashed out and returned to an updated position. This fraud was accomplished successfully because: (1) the manufacturer's hardware could be altered without their knowledge and detection; (2) there was no internal check on the validity of the bonus meter value and the corrupt substitution of RAM; (3) the logic access detection mechanisms were easily disassembled and compromised; and (4) the event log registering evidence of tampering in the machine could be erased without trace and the log pointer stored in RAM could be re-set to a previous proper logic access.

The second version of this technique manipulated the payout schedule stored in the EPROM⁴ of the machine to increase the payouts for a winning combination, thereby raising the totals won and cashed out. This involved two distinct tactics. First, they removed the EPROM from the terminal, scanned its contents using an EPROM programming device to look for possible table locations by searching for the sequence in the EPROM image, then they copied the contents of the EPROM to a binary image along with the contents of the relevant locations, next they altered the values found in these locations in excess of the original awards, following this they modified the EPROM and experimented in the terminal to reveal the correct placement of the pay tables. Second, they discovered how to bypass the EPROM verification process when the machines were turned on. In many gambling devices internal check sums are computed over the entire contents of EPROM in order to prevent fraud. However, in the case of VLT machines, check sums were reinitialized and overwritten each time the terminals were powered on.⁵ Changes to the ROM

were undetected because the check sum verification implementation did not register them. So the fraud team simply determined the relevant memory locations for the pay tables, altered a copy of the EPROM image, programmed a new image to a blank EPROM and reinstalled it. This meant that counterfeit values when added to the EPROM pay tables were not discovered by either the manufacturer or the regulator. Consequently, these machines were exploited regularly and profitably.

The third type of technique involved placing a terminal in stand alone mode without the knowledge of the monitoring system. In effect, by knowing micro controller code and assembler programming language, the criminal group made illegal terminals out of legal ones. First, they created a custom built board that manipulated the VLC back-up RAM. This board consisted of a micro controller with ROM storage, a serial port that could be interfaced with a personal computer and a connector for the VLC back-up RAM board. Next, they either uploaded or downloaded the contents of the VLC RAM to a personal computer using this back-up board. The micro controller ROM on the back-up board was programmed to clear RAM and modified to copy an image of an on-line, enrolled terminal to the RAM before it was reinstalled in the VLT terminal.⁶ This was not especially complicated as they had already outwitted the RAM protection system. In this instance, however, the modified image was not a manipulation of the bonus meter, rather it was a technique that deceived the enrollment system of the regulator into believing that the VLT machine was operating in playable, on-line mode when in fact it was in stand alone mode⁷. This was possible because upgraded copies of EPROM images were

easily obtained in the “black market” to overcome the latest chip technology innovations. These images were installed in ALC terminals with relative ease because the logic area locks supplied by manufacturers were easy to access, and because the monitoring system was incapable of detecting network disconnections in a timely and constant manner.

These criminal techniques suggest that VLT fraud was organized as a series of crimes that were “projects” in themselves. Each was complicated and technically sophisticated involving separate advanced planning and organization. These were high stake, high-risk ventures. But the illegal techniques were geared to reducing risk (McIntosh, 1975). To start with, the criminal organization identified many of the strengths and weaknesses of the machines’ electronic technology and calculated the risk costs before they even planned their deficit manipulations. The simulation methods used to decode the RNG also reduced the dangers of recognition at the fraud sites. The speed of the crime act was progressively increased as the organization became more experienced and effective in manipulating, copying and reinstalling the software on the machines. Similarly, the threat of being stopped or questioned by other players, patrons and employees was neutralized by the skill of the criminal group in determining and calibrating payouts and bonuses quickly, thus reducing visibility and suspicion at the crime site. Detecting and monitoring systems which were designed to discover faults, corruptions, substitutions, verifications, system enrollment breakdowns and unauthorized access to the machines were combated by techniques which duped the manufacturers’ hardware and software

and tricked the law enforcement system into believing that its technology was functional when in fact it had been sabotaged and subverted. The risks of surveillance, identification, apprehension and prosecution were technically managed so that these project crimes could be committed repeatedly and relatively successfully without much fear of corporate, regulatory, or police discovery.

The Social Organization of VLT Crime

We have emphasized the core technology at the heart of the organization of VLT crime and argued that these techniques were tactically designed to achieve survival in an arena of uncertainty. But as Dwight Smith (1980) observes most criminal organizations are also embedded within an external environment where numerous factors act upon the immediate fraud enterprise. Unless an illegal enterprise provides something desirable, it will not receive the inputs necessary for survival. Its future then is also contingent on how efficiently it deals with the constraints imposed upon it by the external environment, and these exchanges or negotiations will also determine the future success of the criminal organization.

The social organization of VLT fraud consisted of a small work team that structured the financing costs, monitored the flow of information and executed the criminal conduct: a technical expert or “hacker” who planned and innovated the crimes and compromised the game machines; an accomplice who “cased” crime sites, relayed information from the crime scenes to the intelligence site; received recoded information back from the technical expert, executed the fraud on the machines and collected the winnings; and, a “lookout” who spotted for trouble. The major

operatives were in their mid 20s, came from the same community and learned many of their practical skills in the social milieu surrounding the illegal gambling market.

As one security officer observed:

One of the individuals had a grade 12 education, maybe one year of university... and he is generally what we would call a hacker who had a great deal of mobility. His family has been involved in the business for some time, from the grey market to the legitimate market. And this individual had access to the game chips. He was also very familiar with the inside of the machine because one time he set up a similar system to what we operate on the reserves.

None of the members of the fraud enterprise had criminal records before they engaged in these illegal acts. They were not involved in either professional or other organized crime groups. Nor is there any indication that they resorted to violence, blackmail or corruption, or were subjected to competitive pressures from other illegal operations in carrying out their many frauds.

The size of the organization was approximately 4 to 5 members, most of who functioned as allies to a technical expert. As one security officer stated "the computer guru ... knew how to operate the system and find out where to match the game plan and the machine. The other people that he had working with him were primarily 'button pushers' and 'betters', two of whom were women. The boundaries of this criminal organization were not especially rigid; work relationships were routine but relatively informal and fluid. Not all members were used in each and every fraud. But each participant was interested in furthering their own welfare and subordinating their own interests to cooperative and coordinated strategies. Personal

kinship relationships ensured trust, secrecy and group integration that protected the core criminal technology in the task environment from external scrutiny.

The overall operation required little expenditures. Items such as computer hardware and software technologies, video equipment, and communication devices were the major expenses. Betting capital and travel were also regular but minor costs. Labour power and expertise, however, were not needed as they were supplied internally. These crimes were conducted with modest cash flows that, in turn, limited the growth potential of the organization. To the best of our knowledge, the illegal enterprise was unable to tap economies of scale, obtain external financing or advertise their services widely (Reuter and Rubenstein, 1982).

The geographical scope of the crimes was therefore local and confined to scattered, rural communities in an area of approximately 500 kilometers. From October 1997 to June 1998, there were 2 to 3 “attacks” a week that resulted in approximately ninety machines being defrauded. The estimated “take” per machine was between \$1,111 and \$3,333 for a total of between \$100,000 and \$300,000. This suggests that the grand total for 4 years of operation was between \$400,000 and \$1,200,000.⁸ The distribution of illegal profits was on a commission basis; the fraud enterprise was small and unable to establish or monitor enduring employee relationships (Reuter, 1985).⁹

The social organization likely included collusive arrangements. As Haller (1990) observes, illegal actors normally enter into symbiotic relationships with legitimate business people who often simultaneously manage or own legal enterprises.

Liddick's (1999) study of the numbers gambling industry is illustrative. He argued that the provision of illegal gambling products was not only achieved by a criminal organization of numbers' workers and dealers responsible for taking bets and tabulating wagers, but by a variety of "societal players" involved in countless informal relationships around the marketplace and in the community. Police, lawyers, politicians and legitimate business and community organizations were active participants in the organization of numbers gambling. These public and private officials were not passively corrupted, or recruited as peripheral agents for criminal organizations. Rather they assumed the more dynamic roles of managers and partners without making themselves part of a formal organization.

We also suspect that there was a symbiotic relationship between the legitimate VLT gambling marketplace and those directly involved in the illicit fraud activities.¹⁰ With the exception of the techniques for predicting random number generator outcomes that often defrauded both operators and governments, all other criminal techniques seemed to involve social arrangements that required overt complicity or covert approval by venue operators or employees. Deficit fraud techniques such as manipulating bonus meters and modifying combination payouts required identifying appropriate machines which had Spielo clearing chips, accessing the logic areas of machines, removing components, re-engineering those parts and reinstalling ghost programs into the existing machines. Placing terminals in stand alone mode and operating them off-line illegally for a period of time was also difficult to accomplish. In some instances, machines were chosen in out of the way places that were difficult

to observe by site owners and employees (i.e., in separate rooms or corridors attached to bars or lounges). In other instances, a joint venture between the criminal organization and a legitimate operator or an employee was required to defraud both players and governments of bona-fide revenues. As one technical investigator put it “the terminal will not be part of the daily pull ... all profits will be directed to the venue personnel.” Arrangements to accomplish this type of fraud included: obtaining access to the door detection system, altering access records, creating interface and connector arrangements between a VLT machine and a PC on site, overcoming property and terminal security measures and exiting the site without detection or causing suspicion. As one security officer observed: “If someone wants to tamper with the machine then it usually has to be collusion between an employee and a site holder.... If there is going to be financial gain then it is the site holder who has to reimburse to make everything look legitimate.”

The social organization of VLT fraud, then, was primarily a working method or system comprised of criminal teams and some wider social coalitions that seemed to involve legitimate enterprises in order to be successful. In one sense these computer frauds required an organization pursuing common goals. But in another sense, they also seem to have entailed some exchange relationships where there were few obvious organizational boundaries. This suggests that part of the process through which these frauds were perpetrated was based on informal exchange networks, where well-connected persons used differing levels of influence to mediate legal and illegal gambling markets. As Cressey (1972) observed, criminal organizations do not

resemble neat hierarchical pyramids, but roadmaps with the lines that connect the various positions going off in different directions.

These collusive arrangements were multiple, historical and easy to form. Some site holders in the legitimate market had once been operators in “the grey market.” When legalization occurred they tried to modify their illegal machines to operate them legally. As one security officer remembered:

These local entrepreneurs were hoping to have them (VLT machines) on an Internet type of set up where there was no central control, auditors would go out and read meters, that type of thing, all manual.

However, the legal marketplace was eventually organized around a centralized, on-line, dialup system which made thousands of grey machines impractical for legal use.¹¹ One game machine, however, was successfully altered for the legitimate market: *Swinging Bells*. The motherboard on this machine was a modification of a wing board that had developed from earlier gaming technology. It was changed to include a refitted dotted board over the original and a new Geneva processor chip that allowed it to be connected to a centralized enrollment system. But as one technical consultant also noted, “this game was ideally suited for attack” because it was older, less secure and known by those working in the black market. Indeed, the fraud team had one person who actually “produced Spielo clearing chips for the illegal VLT market.” This meant that instrumental friendships, working knowledge and patron client ties forged in the grey market were likely the nexus around which VLT frauds in the legal domain were practiced. Some venue operators and their employees, service and repair personnel, and technical advisors allied themselves

with the primary purpose of furthering their own goals. This resembled a dyadic alliance where at least two parties of unequal status, power or resources seemed to ally themselves with someone superior or inferior to them. Taken together these actors constituted the social world of VLT fraud determining its size, complexity, reach, work force, modus operandi and modus vivendi with the structures of social control.

Law Enforcement and the Social Control of VLT Crime

Fraud operations on this scale, of course, cannot always remain unknown to state agencies, so the possibility of this kind of law breaking flourishing depends not only on technical competence and patron-client networks but as well on the ability of the state to control it. Four points should be emphasized. Firstly, law enforcement responsibilities are divided between R.C.M.P. officers, provincial or inter-provincial gaming regulators and inspectors, regional or municipal police forces and specific gambling industry security personnel (i.e., casino staff or VLT operators and staff). The R.C.M. police respond to complaints associated with Criminal Code gambling offences and facilitate the gathering, communication and distribution of criminal intelligence information between law enforcement agencies. Municipal and regional police in urban centres have vice and morality squads to conduct gambling investigations. Provincial and inter-provincial gambling commissions or corporations oversee the terms and conditions of licensed gambling activities, and audit, inspect and investigate suspected gambling violations in order to preserve the fairness and

integrity of the games. Specific staff at gambling sites secures the financial aspects of the games and monitors the security of play (Smith and Wynne, 1999).

Enforcement roles and responsibilities, however, overlap and coordination is sometimes lacking. R.C.M. police and regional policing agencies are not always properly staffed or trained to enforce gambling related laws. They are often underfunded and do not make illegal gambling a top policing priority. Policing strategies such as preventative, directed and managed patrols cannot easily penetrate the sites where gambling frauds occur unless these frauds are reported to them. Gaming commissions and corporations are more focused, better trained and more aggressive in monitoring and controlling the illegal gambling marketplace, but they are not nearly as well resourced as are the public police. In fact, the “frontline force” in detecting and reporting VLT gambling related crime is often the specific staff at an approved premise. As one security officer noted:

The protection of our equipment that would be VLTs, 649 machines, tickets or any of our assets is totally different in scope than for a casino that is under one roof and very easy to control... Big difference, some people equate us with a mini casino in a couple of thousand places throughout Atlantic Canada. So trying to protect assets under those circumstances is rather difficult... The best way to protect our assets is to make them (site holders) feel responsibility for them... When we put in a VL terminal the site has the responsibility for the overall security for that asset.

Site operators watch for underage gamblers, theft from machines and cheating at play as well as for the safety of customers and the operational integrity and efficiency of the gaming machines. In some sites, they monitor electronic surveillance systems to detect wrongdoing or property damage. In other sites they have only their eyes

and ears to check for suspicious conduct. But unlike casino security staff that are trained and supervised, those monitoring VLT sites are not. As one security officer put it:

Here is a big difference between a casino and a VLT operation, if you take a VLT operation at a bar or a corner store, those machines are there for 24 hours a day and it is rare compared to a casino that somebody in authority is around looking at the machine or monitoring the machine... Therefore, wherever the machine is located those people have the opportunity to gain access to it... and can try to tamper with the machine.

The enforcement structure therefore lacked a precise integrated command system with clear lines of authority and responsibility. Policing was often lax, reactive and from a distance.¹² Keeping the law away was not especially difficult since the law was rarely present at the locations where organized frauds occurred. As Smith and Wynne (1999:75) astutely observed, police forces generally responded “to complaints and tips” about gambling related crime, but did not “initiate investigations on their own.” Risks of detection, apprehension and prosecution were low as long as no obvious recognizable crime pattern was discerned. As a result the fraud organization was able to function on a continuous basis, without much fear of legal interference. It was able to stabilize its activities and establish a *modus vivendi* with the forces of social control such that overt detection and conflict were at a minimum. Indeed one official noted that the spread of gambling had facilitated new opportunities for crime that were exceedingly difficult to control. As she put it, “there are rumors that there are 70 or 80 illegal machines operating in this one province ...

Neither municipal police departments, the ALC, ALC security or ALC sales distributors have found any trace of them.”

The deployment of resources is a second problem in the social control of VLT crime. The R.C.M. police have only modest resources to police illegal gambling, provide investigative expertise and coordinate and disseminate information to other crime control agencies. At present, Nova Scotia has a small contingent of officers dedicated to illegal gambling activities. Municipal and regional police resources are also sparse and allocated to cover all forms of vice. Like R.C.M.P., regional and municipal police officers undertake gambling enforcement as part of a larger complex of official duties for which they have only limited time and little training. Specialized gambling investigators are few and criminal intelligence about gambling related crimes is lacking.

The size of provincial and inter-provincial gaming regulators and investigators, however, has grown rapidly with the spread of legalized gambling and this has caused concerns about policing jurisdictions and mandates. Provincial gaming commissions are encroaching on previous police powers by taking a lead enforcement role in the field of illegal gambling. This has created an anomalous situation where policing mandates and authorities are increasingly blurred and ambiguous. Conflict of interest allegations create further complications because governments are both major promoters and beneficiaries of gambling products and regulators of their own conduct. The temptations to overlook, evade or cover up certain questionable gambling practices to avoid scandals have been palpable (Smith

and Wynne, 1999:75). Despite these developments the number of gambling investigators remain small: in Western Canada the average number per province is approximately 11, whereas in Atlantic Canada it is approximately 6. In Nova Scotia there are 3,234 VLT machines operating in 600 locations. The ratio of investigators to VLT machines is 1 per 539 and the ratio of investigators to VLT locations is 1 per 100.¹³

The resources the enforcement agencies command disadvantage them in policing organized frauds of the sort under study. Their limited numbers do not allow them to easily discover infractions on their own. They must depend on on-site reporting, consumer complaints or intelligence from insiders. When enforcement bodies detect violations, they are often hampered in their ability to prosecute. Reduced budgets, understaffing, limited training programs, inadequate intelligence gathering and communication, and the lack of qualified expert officers to operate as credible court witnesses combine to make the social control of VLT crime difficult (Smith and Wynne, 1999:74-75). In the interstices of diffuse and de-centered state authority and the emergence of the “grind gambling marketplace”, black market entrepreneurs, professional crime groups, and sophisticated fraud organizations can function persistently and “beat the odds” of capture.

Inter-provincial and provincial gaming commissions and corporations, of course, monitor VLT machines through an on line, dialup system, but this actually constitutes a third problem in the social control of VLT crime. In Nova Scotia the ALC asserts direct control over VLT assets: it approves the site holders, the

manufacturers that sell the machines and the machines' operating standards and specifications. According to one official:

The coin operators ... are permitted to go to these approved manufacturers and purchase those machines and install those machines and the theory is that only that type of machine will hook up to our central system and function under the specifications that it is meant to function under. So to get the machines in an area where ALC has total control, like Nova Scotia, theoretically it should be a lot more difficult to scam the system.

This centralized dial up system is designed to enroll all VLT machines in the province, audit their proper functions and payouts, detect unlawful machine access and tampering and record normal and abnormal practices. But this system does not monitor in real time and so violations are not reported immediately. Here is the way one enforcement official put it:

We are only aware of what transpires on VLTs or with VLTs 24 hours after it (a violation) has occurred because we poll them once every 24 hours. Everything that has transpired on the machine is stored in memory and that memory downloads to our central system... Therefore if something occurs ... we can go back and look at those records. So it (the system) is always in an audit mode more than a totally preventive mode. In other words, if someone opens the logic area of the machine we don't know they did it instantly at that time, we have to find out afterwards... If there is nothing obvious when our technicians look at it (the record) then we (ALC) may not know until something strange occurs, like payouts are greater than what they should be, that type of thing.

So the computerized registration system was reactive and reliant on site holders. In practice, the security system was really local, dispersed and managed by countless individuals on a daily basis. It functioned according to "the reliability, dependability, and trustworthiness of operators and their employees" who were allowed to "open

the door of the machine, take out the cash, fix paper jams, jiggle a coin and fix a coin jam....” Site holders are expected to operate as “whistleblowers” about unusual occurrences, thefts, property damages and frauds. Once notified, the ALC begins a review of its logs, initiates audits, launches inspections, conducts site investigations and refers cases to specific law enforcement authorities. It is primarily an “audit trap” that catches anomalies after they have occurred.

It really goes back to the fundamentals of security from the day of the Chinese lock, everything is there for the honest person. If you are not dealing with the honest person, you are dealing with the determined person, if you are dealing with the determined person, they are going to do what they set out to do and the next step is to make sure you have an audit trap. Once you know what is transpiring, then you go looking at your statistics, you can pretty well spot a pattern that developed.

These security measures are remote control, accounting procedure. They are not designed to operate on an opportunity reduction basis. The “delay poll feature” permits criminal acts or patterns of crime to occur without immediate suspicion, detection or knowledge of the facts. Ironically, this ensures unobtrusiveness, continuity and relative safety for those involved in conducting VLT frauds of the type under study.

So the trust, honesty and loyalty of venue operators and their employees are fundamental to “real time security.” But this is the “achilles heel” of this type of protection system. In instances of theft from VLT machines or VLT earnings, losses are usually discovered retrospectively: site holders are victimized, governments

retain their profit shares and perpetrators easily escape with “the take.” As one security officer related:

Yeah, it is a fairly common experience ... and there have been situations where money is missing into the thousands of dollars. This is normally where you have an employee theft problem ... but we do not become overly involved in catching that thief. It is not our responsibility and it is very easy to get tied up in lawful business... what you find is they usually have someone in charge and that individual gets the sweep sheets from ALC, they make sure ALC money is there, they deliberately do not keep the audit tapes, they deliberately destroy the sweep sheets, and of course they are taking the money out....

In cases of money laundering crime groups collude with site holders to cycle money through VLT machines. Operators receive illegal profits while criminal groups clean their capital and acquire legitimacy for it. Another law enforcement official put it as follows:

You can probably do 75 cents on the dollar, which is damn good money in money laundering, otherwise you can do 20 cents on the dollar which is not bad The problem with the VLTs is that it takes too long to pump it through, play some and cash it out.... They don't play that much, they just cycle. That is where your stats start to skew and that is where you spot it if it is big dollars.... So in other words they put 10 dollars in, push the cash button and take 10 dollars out. Put 10 dollars in, play one game, cash out whatever is left. And if they are accosted by the police ... they say “well I won this money at this (VLT) location ... go ask them and then the police go ask them and, yes, they were in here last night and they won that money.”

In the fraud cases we studied numerous gaps in the monitoring and site security systems were exploited. When collusive relationships between criminal groups and legitimate site holders existed, access to the machines was open and easy

rather than complicated and clandestine. This enabled them to effectively by-pass audit traps by deceiving its enrollment memory and corrupting its internal checks. Legitimate operators can exploit their social control role by acting as double agents: protecting their assets and conducting their security measures on behalf of the government while simultaneously operating an illegal enterprise by “going on the take.”

Finally, the translation of law into a practical activity has had little deterrent effect on VLT crime. Police investigations into gambling related crimes do carry the threat of incarceration, but few cases actually reach the court system and punishments are typically trifling: suspended sentences and small fines. Smith and Wynne (1999:76) report on a recent defendant who was convicted on 8 counts of cheating at play but received only a \$100 fine. They also observed that penalties for operating illegal VLT machines were lenient when compared to drug trafficking. Both operations were able to net large illegal profits, but illegal gambling charges typically resulted in minimum jail time, or fines and/or confiscation of the gambling machines, whereas drug charges typically incurred 6 to 10 years incarceration. We found a similar pattern in our case study. Two members of the fraud team were eventually apprehended, charged and convicted under section 342.1(1)(b) of the Criminal Code for unauthorized use of a computer, computer programs, computer data and mechanical devices to defraud a video lottery terminal. Both offenders cooperated with the R.C.M. police and the ALC authorities, both of who were

primarily interested in correcting breaches in the VLT security system. The two offenders each received a conditional discharge and 1 year probation.

Gaming commission investigators do have the power to suspend liquor and gaming licenses and to ban persons from provincial gambling sites such as casinos. But the power to put operators out of business is rarely used. To the best of our knowledge no site holders were deprived of their gaming licenses or charged and prosecuted. Gaming commissions and corporations seemed reluctant to prosecute these cheating at play conspiracies because it undermined consumer confidence in the standards and operational integrity of the gambling machines. As one official noted, "our interest was to protect the corporation and to gather technical intelligence." So with the cooperation of the R.C.M. police, "we got what we wanted, the know-how out there, and ... the offenders went through the courts ... it was a fairly innocuous charge and needless to say we did not want a lot of publicity here."

So the social organization of VLT fraud functioned in part because the state was somewhat lax at translating law into effective enforcement action. Unable to enforce many of its own laws and regulations and operating with remote, reactive and hesitant security measures which delayed the discovery of crime and the response of criminal justice administration, the state could not easily or systematically control frauds of this type. The social organization of fraud effectively evaded, avoided and neutralized the law by clever manipulations and deceptions for a period of approximately 4 years. To paraphrase McIntosh (1975:42-50), the hallmark of project crime is its ability to assemble teams of competent criminals for attacks on

valuable and well protected property by overcoming technical problems and the exigencies of social control to such an extent that they can establish stable, though short-lived, criminal organizations.

Eventually the social organization behind the VLT frauds was exposed. The RNG fraud technique, which victimized operators and governments alike, was observed and reported by on-site retailers. Ironically the technical sophistication of the group may have been its downfall. They increasingly used video cameras and wireless communication devices to target, plan, communicate and execute this fraud technique. They were exploiting machines for maximum payouts and this also aroused suspicion. "I am not sure we would have caught them ... if they had been doing it at a level of \$500," states one security officer, "but they were doing \$1000 and \$1900 at a time ... so they (retailers) became suspicious of cashing out so much ... and the suspicions came back to me." In fact, some site holders erroneously reported, "cellular telephones were being used to manipulate the VLTs to pay out." These reports triggered an investigation by the ALC that involved extensive surveillance of the fraud group by private detectives. Eventually enough criminal intelligence was collected to identify all members of the crime group.¹⁴ Then the R.C.M. police was contacted and their gaming section set up an intercept operation that led to the arrest of the core pair involved in mustering and planning most of the frauds. The machines were confiscated and the two offenders were debriefed. "They were very cooperative and they demonstrated at our location the night they were caught what

transpired.” The corporation then launched a major technical review of its gaming machines’ standards and specifications.

“This one guy was so good from our point of view, we could not bring in people from an investigator’s point view that had already had a vested interest in approving the product that had been put out there. So we hired an organization ... out of Australia ... and we had them do a re-evaluation of the entire program and the chips.”

This resulted in security changes to the RNG, the EPROMS and the motherboards, the background cycling system, the critical memory features, the logic area locks, the enrollment monitoring system and the regulatory on-site inspection system. To paraphrase one security officer, we developed a stricter control over our inventory by using a new system of keys, tags and seals on all our VLT machines. That way we can detect frauds sooner rather than later. Thus the fraud techniques were made obsolete and the *raison d’etre* for the criminal organization was no longer compelling.

But these developments in new hardware and software specifications and protections do not mean the end of VLT fraud. Rather treating criminal organizations as rationally geared to handling the technical problems of crime – which are the problems of negotiating social control in its widest sense - means that changes in the social control of VLTs will likely lead to new criminal innovations in order to overcome the escalating technology of property protection and gambling security. As one official reminded us, “ I have been in law enforcement for twenty years....

Counterfeits, scams, thefts and frauds get more sophisticated as the evolution of technical security features get more advanced.”

Notes

1. These categories are not theoretically derived or mutually exclusive and appear to be arbitrary. Consequently, there are a number of overlaps that create a degree of confusion. Cheating at play, for example, seems to fit any category depending on the circumstances and motivations. It can apply to illegal gambling as prescribed by the Criminal Code, to crimes associated with the gambling scene and it can be the desperate activity of a problem gambler. Nevertheless, this schema does provide a means of ordering diverse criminal behaviors related to gambling and a starting point for generating interesting research questions.
2. This listing of fraud techniques is not exhaustive. Altogether the criminal group deployed at least 7 distinct types.
3. The search to locate the generating seeds was time consuming. Through a process of trial and error, the perpetrators (using a 32 bit program) managed to reduce the search time from 1.5 weeks to 8 hours to 20 seconds.
4. EPROMs are computer chips that store information in memory that regulates a video gambling device's play, such as creating payouts to players, ensuring an absolute game of chance for each new play and monitoring the machine's electronic account record so that it corresponds to the government's record.
5. In the case of IGT terminals the technical organization of the fraud required more effort and thought because IGT had developed additional security against RAM and EPROM corruption. Check sums were stored in the

- EPROMs and also the RAMs and so the verification implementation was recalculated and rechecked. This meant that the criminal group had to disassemble code through a process of trial and error before they could program a new image and reinstall it.
6. This technique is akin to “gaffing” or “phantom programming” where operators install hidden programs into a gambling machine to change the regulated payout specifications of fair play at the expense of players.
 7. Again in the case of IGT terminals, the fraud techniques were more complicated and involved reverse engineering the disassembled game image and forcing a RAM corruption to disconnect the terminal from the system without ever being detected. In the opinion of investigators, this criminal organization was a step ahead of the manufacturer’s protection system and the government’s monitoring apparatus, and they rated this type of fraud as moderate to high risk.
 8. These estimates are based on information supplied by the RCMP to the Atlantic Lottery Corporation. Our estimate of a grand total is based on the assumption that the level of illegal activity was consistent over a four year period. We anticipate confirming these figures once we have conducted interviews with members of the fraud organization.
 9. At this point in the research we are unable to discuss the exact shares of the take among the crime team. Nor are we able to discuss the distribution of

- profits between other collusive partners such as owner/operators or employees of particular sites where VLT machines were licensed.
10. The information available to map out the collusive relationships between the licit and illicit actors is admittedly sketchy. We can confirm the general pattern of collusion but we anticipate more detailed support for our analysis once we have interviewed members of the criminal organization.
 11. There are a number of controlling, accounting and collection systems: the hard meter, the dial up and the on-line. The dial up system revolves around one central computer that calls up each device at a specified time and records all relevant information. The devices in the gambling establishments are connected by modem to a main computer and the main computer “polls” every VLT machine once every 24 hours. It is estimated by the ALC that approximately 12,000 grey machines could not be connected to the dial up system and these machines were moved west to other Canadian provinces and to the northeastern United States.
 12. A number of provinces, Alberta, British Columbia and Ontario have created specialized task forces or coordinated units to oversee problems associated with illegal gambling and gambling related crime. These initiatives have been implemented to overcome the funding, staff and resource, and criminal intelligence gathering problems surrounding gambling and crime (see Smith and Wynne, 1999:70-71).

13. It should be pointed out, however, that more investigators can be deployed on a case by case basis including people from the technical side and inspectors from other Atlantic provinces.
14. Site holders determined the identity of fraud members by paying out winnings by checks. This resulted in the discovery of their addresses and the development of extensive surveillance of their activities.

References

- Aronovitz, C. (1997). "To Start, Press the Flashing Button: The Legalization of Video Gambling Devices," in W. R. Eadington and J. A. Cornelius (eds.) Gambling Public Policies and the Social Sciences. Reno: University of Nevada.
- Azmier, J. (2001). "Gambling in Canada 2001: An Overview," Calgary: Canada West Foundation.
- Beare, M. (1996). Criminal Conspiracies: Organized Crime in Canada. Scarborough: Nelson Canada.
- Beare, M. and S. Schneider (1990). Tracing of Illicit Funds: Money Laundering in Canada. Working paper, Ministry of the Solicitor General of Canada.
- Best, J. and Luckenbill (1982). Organizing Deviance. Englewood Cliffs, N. J.: Prentice-Hall.
- Black, E. (1996). "Gambling Mania: Lessons from the Manitoba Experience," Canadian Public Administration, 39(1):49-61.
- Block, A. A. and W. Chambliss (1981). Organizing Crime. Amsterdam: Elsevier.
- Campbell, C. (1996). "Lottery Ticket Resales: A Canadian Law Enforcement Nightmare." Unpublished paper presented at the National Conference on Problem Gambling, Crime and Gaming Enforcement, Illinois State University, Normal, Illinois.
- Campbell, C. and G. Smith (1998). "Canadian Gambling: Trends and Public Policy Issues." Annals American Academy of Political and Social Sciences, 556, March.
- Chambliss, W. (1978). On the Take: From Petty Crooks to Presidents. Bloomington: Indiana University Press.
- Chambliss, W. (1989). "State Organized Crime," Criminology, 27:183-98.
- Chang, S. (1996). "Impact of Casinos on Crime: The Case of Biloxi, Mississippi." Journal of Criminal Justice 25(5): 431-436.
- Clinnard, M. B. and R. Quinney (1983). Criminal Behavior Systems: A Typology. New York: Holt, Rinehart and Winston.
- Cohen, A. K. (1977). "The Concept of Criminal Organization," British Journal of Criminology, 17:97-111.
- Cressey, D. (1972). Criminal Organization: Its Elementary Forms. London: Heinemann.

Eadington, W. R. (1994). Understanding Gambling. Ninth International Conference on Gambling and Risk Taking. Las Vegas, Nevada.

Eadington, W. R. (1996). "Ethical and Policy Considerations in the Spread of Commercial Gambling." Ed. J. McMillan Gambling Cultures. New York, Routledge: 243-262.

Einstadter, W. J. (1969). "The Social Organization of Armed Robbery," Social Problems, 17(1):64-83.

Giacopassi, D. and B. G. Stitt (1993). "Assessing the Impact of Casino Gambling on Crime in Mississippi," American Journal of Criminal Justice 18(1): 117-131.

Goodman, R. (1995a). "Legalized Gambling: Public Policy and Economic Development Issues." Economic Development Review 13 (4, Fall): 55-57.

Goodman, R. (1995b). The Luck Business: The Devastating Consequences and Broken Promises of America's Gambling Explosion. New York: Free Press.

Grant, S. (1998). "Atlantic Lottery Corporation 1998 Market Overview" (Calendar Quarters 1 and 2), Moncton: Market Research and Development, ALC.

Grinols, E., D. Mustard and C. Dilley (1999). Casinos and Crime. Study prepared for U. S. National Gambling Study Commission, Washington, D. C. U.S.A.

Hakim, S. and A. J. Buck (1989). "Do Casinos Enhance Crime?," Journal of Criminal Justice 17:409-416.

Haller, M. H. (1990). "Illegal Enterprise: A Theoretical and Historical Interpretation," Criminology 28:207-235.

Henrikssen, L. (1996). Hardly a Quick Fix: Casino Gambling in Canada. Canadian Public Policy, XXII (2), 116-128.

Hobsbawm, E. (1969). Bandits, London: Widenfeld and Neelson.

Kindt, J. W. (1994). "Increased Crime and Legalizing Gambling Operations: The Impact on the Socio-economics of Business and Government," Criminal Law Bulletin 30:538-555.

LaFramboise, D. (1998). "Long-Armed Bandits". Globe and Mail, Eastern Edition, Halifax, Nova Scotia: D1-D2.

Liddick, D. (1999). An Empirical, Theoretical and Historical Overview of Organized Crime. N.Y. Edwin Mellen Press.

Little, D. and R. Beland (1998). "Can I Help You?: The Rise in Household Spending on Services." , Services Indicators 2nd Quarter. Ottawa: Statistics Canada.

MPM Gaming Research (1999). Convenience Gaming and Social Impacts in Nova Scotia: Volume 2 - Appendix K. Unpublished report, Halifax, Nova Scotia.

MPM Gaming Research (2000). "Convenience Gaming and Social Impacts in Nova Scotia." In Annual Gaming Report Appendices Vol. II, Appendix C. Dartmouth, Nova Scotia: Alcohol and Gaming Authority, Annual Report 1998-99.

Mack, J. (1972). "The Able Criminal", British Journal of Sociology, 12: 44-55.

Marfels, C. (1997). "Casino Gaming and VLT Gaming: Substitution Effect or Supplementation Effect?" Gaming Law Review 1(3):333-339.

Marshall, K. (1996a). "A Sure Bet Industry." Perspectives, Ottawa: Statistics Canada Catalogue No. 75-001-XPE (Autumn): 37-41.

Marshall, K. (1996b). "Games of Chance." Family Expenditure in Canada, Ottawa: Statistics Canada Catalogue No. 62-555-XPB (July):32-39.

Marshall, K. (1998). "The Gambling Industry: Raising the Stakes." Perspectives, Ottawa: Statistics Canada Catalogue No. 75-001-XPE (Winter): 7-11.

McIntosh, M. (1971). "Changes in the Organization of Thieving," in S. Cohen (ed.) Images of Deviance. Middlesex: Penguin Books.

McIntosh, M. (1973). "The Growth of Racketeering," Economy and Society, Vol. 2:35-69).

McIntosh, M. (1975). The Organization of Crime. London: MacMillan Press.

McMillan, J. (1996). From Glamour to Grind: The Globalization of Casinos in J. McMillan (ed.) Gambling Cultures: Studies in History and Interpretation (263-287). London: Routledge.

McMullan, J. L. D. C. Perrier and M. MacDonald (2002). "Gambling Expenditures, the Intensity of Gambling and the Affects on Financial Well-Being and Discretionary Spending in Canada," in Journal Review.

National Council of Welfare (1996). Gambling in Canada. Ottawa, Minister of Supply and Services, Canada.

Nova Scotia Alcohol and Gaming Authority (1996-97). Annual Gaming Report. Dartmouth, Nova Scotia.

Nova Scotia Alcohol and Gaming Authority (1999). Nova Scotia and Alcohol Annual Gaming Report 1997-98 and Annual Gaming Report Appendices Vol. II, Dartmouth, Nova Scotia: Alcohol and Gaming Authority.

Nova Scotia Department of Health, Drug Dependency Services (1998). Nova Scotia Video Lottery Players Survey 1997-1998, Halifax, Nova Scotia.

Nova Scotia Gaming Control Commission (1995-96). A Year in Review: Gaming in Nova Scotia. Dartmouth, Nova Scotia.

Omnifacts Research Ltd. (1996). "A Study of Gambling in Nova Scotia: General Population Survey." Pub. in A Year in Review Gaming in Nova Scotia, Halifax: Nova Scotia Gaming Control Commission.

Porter Dillon (1999) Socioeconomic Impact of Video Lottery Terminals: Final Report. Prepared for the Legislative Assembly of Nova Scotia, Halifax, Nova Scotia.

Potter, G. W. (1994). Criminal Organizations. Prospect Heights, Ill.: Waveland Press.

Reuter, P. (1985). The Organization of Illegal Markets: An Economic Analysis. Washington D. C.: U. S. Government Printing Office.

Reuter, P. and J. Rubinstein (1982). Illegal Gambling in New York: A Case Study of the Operation, Structure and Operation of an Illegal Market. Washington, D. C.: U. S. Government Printing Office.

Rosecrance, J. (1990). "The Stoooper: A Professional Thief in the Sutherland Manner." In D. H. Kelly (ed.) Criminal Behavior: Texts and Readings in Criminology: N.Y.: St. Martin's Press.

Rosenthal, R. and H. Lesieur (1996). "Pathological Gambling and Criminal Behavior." in L. Schlesinger, (ed.) Explorations in Criminal Psychopathology, Springfield, Illinois: Charles C. Thomas.

Skolnick, J. H. (1980). House of Cards: Legalization and Control of Casino Gambling. Boston: Little, Brown and Company.

Seelig, M. Y. and J. H. Seelig (1998). "Place Your Bets! On Gambling, Government and Society." Canadian Public Policy XXIV (1): 91-106.

Shaffer, H. J., M. N. Hall and J. V. Bilt (1997). Estimating the Prevalence of Disordered Gambling Behavior in the United States and Canada: A Meta-Analysis. Boston, Mass.: Harvard Medical School, Division on Addictions.

Smith, D. C. (1980). "Paragons, Pariahs and Pirates: A Spectrum Based Theory of Enterprise." Crime and Delinquency 26:358-386.

Smith, G. J. (1990). "Pools, Parlays, and Point Spreads: A Sociological Consideration of the Legalization of Sports Gambling," Sociology of Sport Journal 7(3): 271-286.

Smith, G. J. and J. Azmier (1997). Gambling and the Public Interest? Calgary, Alberta, Canada West Foundation.

Smith, G. J. and T. D. Hinch (1996). "Canadian Casinos as Tourist Attractions: Chasing the Pot of Gold." Journal of Travel Research 34 (3, Winter): 37-45.

Smith, G. J. and H. Wynne (1999). Gambling in Canada, Triumph, Tragedy or Tradeoff? Calgary: Canada West Foundation.

Sternlieb, G. and J. W. Hughes (1983). The Atlantic City Gamble. Cambridge: Harvard University Press.

Stokowski, P. (1996a). Riches and Regrets: Betting on Gambling on Two Colorado Mountain Towns. Niwot, Colorado: University Press of Colorado.

Stokowski, P. (1996a). "Crime Patterns and Gaming Development in Rural Colorado," Journal of Travel Research 34(3):63-69.

Sutherland, E. (1983). White Collar Crime: The Uncut Version. New Haven: Yale University Press.

Thompson, W. N., R. Gazel and D. Rickman (1996a). The Social Costs of Gambling in Wisconsin. Wisconsin: The Wisconsin Policy Research Institute.

Thompson, W. N., R. Gazel and D. Rickman (1996b). Casinos and Crime in Wisconsin: What's the Connection, The Wisconsin Policy Research Institute.

Thompson, W. N. (1997) "Not Exactly! The Grocery Store: Casino and Slot Joints as Tourist Destination Resorts: Some Observations on Dysfunctional Gaming Establishments in Nevada and South Carolina." Conference on the Social and Economic Impacts of Electronic Gambling, Edmonton, Alberta.

Thompson, W. N. and R. Gazel (1998). The Social Costs of Gambling: A Comparative Study of Nutmeg and Cheese State Gamblers. Unpublished paper presented at the 12 National Conference on Problem Gambling, Los Vegas, Nevada.

Vaillancourt, F. (1999) "Government Gambling Revenues, 1985-1995/1996: Evidence From Canada, Great Britain and Australia", revised paper, presented at the 1998 Conference of the National Tax Association, Austin Texas.

Walker, M. B. (1996). "The Prevalence of Problem and Pathological Gambling: A Critical Analysis." Journal of Gambling Studies 12:2 (Summer):233-249.

Walker, M. B. (1997). "The Impact of Casinos in Urban Centres on Problem Gambling," in W. R. Eadington and J. A. Cornelius (eds.) Gambling: Public Policies and the Social Sciences. Reno: Institute for the Study of Gambling and Commercial Gaming, University of Nevada.

Zendzian, C. A. (1993). Who Pays? Casino Gambling, Hidden Interest and Crime. New York: Harrow and Heston.