RCMP
ROYAL CANADIAN MOUNTED POLICE

GAZETTE

Serving the police community since 1938

Vol. 70, No. 1, 2008
www.rcmp-grc.gc.ca

2010 OLYMPICS
Keeping the Games fraud-free

DISASTER RELIEF SCAMS
Lessons from Hurricane Katrina

WIKI WARM-UP
Public helps shape New Zealand Police Act

Seeing through the scams

The fight against fraud

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Fraud knows no borders

When we read and hear about major scams and fraud, the details are sometimes hard to believe — details about how low criminals will stoop to make money, and how trustful the public can be despite the warnings. The fact is, fraud will never completely disappear. But the goal is to make it more difficult.

In this issue on fraud, we take a look at some of the unscrupulous ways that scam artists make off with what isn't theirs, and the most effective methods of fighting back.

To begin, our cover story highlights major mass-marketing scams based in Nigeria that use fake cheques to fool victims overseas. The cross-border investigations involve the joint work of law enforcement agencies from the United States, Canada, the United Kingdom, the Netherlands and Nigeria. These international partnerships are now the way business must be done to curb fraud, and other crimes too.

We look at the RCMP's National Anti-Counterfeiting Bureau and the role it plays in analyzing and identifying fake currency and documents seized in investigations. The bureau has recently changed its mandate to provide advice to agencies outside the police arena — a role that is welcome and needed.

The RCMP-led Integrated Security Unit (ISU) for the 2010 Winter Olympic and Paralympic Games in Vancouver was established to examine the complex security matter for that international event. With over $3.1 billion projected for construction, the ISU's special financial intelligence unit was formed to protect public and private funds associated with infrastructure at the Games. Learn more about this winning approach to preventing corruption.

Our contributors explore a wide variety of ways in which members of the public are fooled — sometimes without ever knowing it — and how police are pursuing their cases.

Insp Barry Baxter of the RCMP's Commercial Crime Branch looks at identity fraud and how our personal and financial information has become a valuable commodity. RCMP Cst Lloyd Schoepp of Commercial Crime Section in Calgary talks about a joint initiative between local police and retailers aimed at raising awareness of payment card fraud known as skimming.

The Hon. David R. Dugas, U.S. attorney for the Middle District of Louisiana, talks about the Hurricane Katrina Fraud Task Force and the widespread fraud that took place while relief efforts for that disaster were in full swing. Dugas presents three basic principles in investigating disaster relief fraud that should be mandatory reading.

Meanwhile, Prof. Jeffrey Rosenthal from the University of Toronto discusses how the field of mathematics helped solve a high-profile investigation into an Ontario lottery fraud. He crunched the numbers in that case, and the figures were hard to refute.

Cross-border fraud abounds and police are seeing more and more victims taken in by criminals based in other countries. Read about an Australian man who travelled to Mali and was kidnapped for a ransom in that country. This article highlights the very real dangers lurking on the Internet, as well as how international collaboration can save lives.

Olaolu Adegbite of Nigeria's Economic and Financial Crimes Commission talks about the work being done to tackle advance fee fraud schemes based in that country through increased enforcement, and how police can stay ahead of these scams by predicting how they will evolve.

Finally, David Jones of the U.K. Serious Fraud Office (SFO) describes the international co-operation required for many of its cases, including one in which a persistent Canadian victim triggered a major SFO investigation.

Outside our cover section, you can read a Q&A with the RCMP's first criminal investigative psychologist, learn what coping strategies some RCMP child exploitation investigators use to help them in their work, find out how the New Zealand Police used the web to encourage the public to shape that country's new policing act, and much more.

We hope you enjoy our first issue of 2008.

Katherine Aldred

More to explore on fraud from the Canadian Police College Library

www.cpc.gc.ca/library_e.htm

Books

Corporate Fraud: A Manager's Journey / Pickett, K. H. Spencer. Mississauga, ON, Canada: John Wiley & Sons Canada. 2007 HV 6691 P58.

Education and Training in Fraud and Forensic Accounting / U.S. National Institute of Justice. Washington, D.C. USA: United States Department of Justice. 2007 HV 8079 .F7 N21.

The Handbook of Fraud Deterrence / Cendrowski, Harry. Hoboken, NJ, USA: John Wiley & Sons. 2007 HV 6691 C33.

The Law of Fraud and the Forensic Investigator / Debenham, David. Toronto, ON, Canada: Carwell. 2006 KE 8973 D35.

Occupational Fraud and Abuse Within Canada's Department of National Defence / Williams, Alan Lee. Utica, NY, USA: unknown. 2006 HV 6699 .C2 W67.

Personal Information and Scams Protection: A Canadian Practical Guide / Waite, Mélanie. Ottawa, ON, Canada: RCMP. 2007 HV 6685 .C2 W133.

Principles of Fraud Examination / Wells, Joseph T. Hoboken, NJ, USA: John Wiley. 2005 HV 8079 .F7 W46.

Stop Fraud: A Veteran Police Investigator Shows You How / Trainor, Brian. Calgary, AB, Canada: Red Deer Press. 2007 HV 6691 T68.

Articles

Environmental Fraud: More Subtle Than Midnight Dumping / Liberti, Francesco. Fraud Magazine Vol. 20, No. 6 (2006), pp. 32-34, 47, 50.

Fighting Fraud With Research / Carozza, Dick. Fraud Magazine Vol. 20, No. 5 (2006), pp. 32-36.

...Continued on page 25

GAZETTE

Serving the police community since 1938

Vol. 70, No. 1, 2008 — A Royal Canadian Mounted Police Publication

Cover

Fraud

Departments

ON THE COVER

No form of crime seems to bring out a criminal's creativity quite like fraud. But whether a scam artist hits his victims in the perceived safety of their homes, at local businesses or even following a disaster, police agencies and their partners are becoming more savvy to fraudsters' methods — and are teaming up to stop them.

THE GAZETTE ONLINE HAS MOVED!

Please bookmark us at
www.rcmp.ca/gazette/index.html
and pay us a visit.

PUBLISHER – Nancy Sample EDITOR – Katherine Aldred WRITER – Caroline Ross GRAPHIC DESIGN – Jennifer Wale
ADMINISTRATIVE SUPPORT AND CIRCULATION – Angela Muia TRANSLATION – RCMP Translation Services PRINTING – Performance Printing

The *Gazette* (ISSN 1196-6513) is published in English and French by the Public Affairs and Communication Services of the Royal Canadian Mounted Police in Ottawa. Cover design and contents are copyrighted and no part of this publication may be reproduced without written consent. Canada Post Publications Mail Agreement 40064068. The *Gazette* is published four (4) times a year and is issued free of charge on a limited basis to accredited police forces and agencies within the criminal justice system. Personal subscriptions are not available. The *Gazette* welcomes contributions, letters, articles and comments in either official language. We reserve the right to edit for length, content and clarity. HOW TO REACH US : Editor — RCMP Gazette, L.H. Nicholson Building, Rm A200, 1200 Vanier Parkway, Ottawa, Ontario, CANADA K1A 0R2, Phone: (613) 998-6307, E-mail: gazette@rcmp-grc.gc.ca, Fax: (613) 993-3098, Internet: ***www.rcmp.ca/gazette/index.html***, © Ministry of Public Works and Government Services (2000).

NEW RCMP RECEPTION CENTRE WELCOMES INTERNATIONAL VISITORS

International visitors to RCMP Headquarters in Ottawa now have a dedicated space to meet with RCMP staff, conduct business and relax between engagements.

The RCMP International Visitors' Reception Centre, which officially opened on September 28, 2007, is "the focal point" of an international delegation's visit to Ottawa, says S/Sgt Pierre Patenaude, manager (now retired) of the RCMP International Travel and Visits Branch. "All the meetings will be held here."

The Centre boasts a 25-person meeting space, Internet and teleconference facilities and close proximity to the main entrance. An added lounge area provides visitors with a comfortable, secure place to remain between meetings.

"People will stay here, enjoy coffee or tea, chat amongst themselves and with RCMP members," says Patenaude.

The Centre is the icing on the cake of the RCMP's International Visits and Protocol Program, which began in 2003 and provides visiting delegations with airport reception, transportation in RCMP vehicles, tailored itineraries and other services arranged by a dedicated protocol visit officer.

Patenaude notes that the program has been well-received by visitors and is helping strengthen international rapport. RCMP liaison officers abroad have more contacts now than they did before the program began, he says, and that makes the RCMP better able to work with foreign partners on cases that span borders.

Since 2003, RCMP Headquarters has received 1,393 foreign visitors in 404 delegations. The most frequent visits are from China, the United States and South Africa.

Caroline Ross

RCMP Commr William J. S. Elliott cuts the ribbon on the new RCMP International Visitors' Reception Centre, while A/Commr, Raf Souccar, Federal and International Operations, looks on.

—Caroline Ross

TEAMS TO FIGHT INTERNATIONAL CORRUPTION

Combating international corruption requires a global effort. By April 2008, two new RCMP teams will have joined the fight.

The two RCMP international anti-corruption teams — one in Ottawa and the other in Calgary — will focus on detecting, investigating and preventing international corruption such as bribery, embezzlement and money laundering. The teams help fulfil Canada's commitments under the United Nations Convention Against Corruption (UNCAC).

"The way to combat corruption on a global scale is for countries to work together to create a level playing field," says Supt Stephen Foster, director of the RCMP Commercial Crime Branch under which the teams will operate.

The UNCAC includes several measures to improve global collaboration against corruption. One measure requires that each member state establish a preventive anti-corruption body to enforce appropriate anti-corruption policies, gather and disseminate knowledge, and assist foreign partners in the fight against corruption.

The RCMP teams will fulfil this requirement for Canada by specifically targeting public sector corruption, including bribery of national and foreign public officials and related laundering of the proceeds of crime.

"(The teams will) gather intelligence, make contacts and identify tactical targets for investigation," says Foster. He adds that having investigators dedicated to combating corruption is important because it allows law enforcement agencies to thoroughly address corruption cases without stretching resources across other ongoing investigations.

The RCMP teams will work closely with foreign enforcement bodies, as well as Canadian partners such as the Department of Foreign Affairs and International Trade (DFAIT) and Justice Canada, both of which are involved in implementing other Convention requirements on behalf of the Government of Canada.

The UNCAC is the first legally binding international instrument against corruption. The Convention came into force in December 2005 and has been ratified by over 100 member states, including Canada in October 2007.

Besides law enforcement, the UNCAC includes measures to improve public and private sector accountability and expedite the prosecution of offending parties.

—Caroline Ross

POLICE TECHNOLOGY MAY HELP MILITARY

A "geographic profiling" system first implemented by Canadian police to help locate and apprehend serial criminals is now being evaluated by the Canadian military for use in counter-insurgency operations overseas.

The system, developed by former Vancouver police officer Kim Rossmo in the mid 1990s, allows trained users to input the geographic co-ordinates of sites where serial crimes like murders, rapes and burglaries are committed. The system then generates a "probability map" showing areas where the perpetrator is most likely to live based on the locations of the crimes.

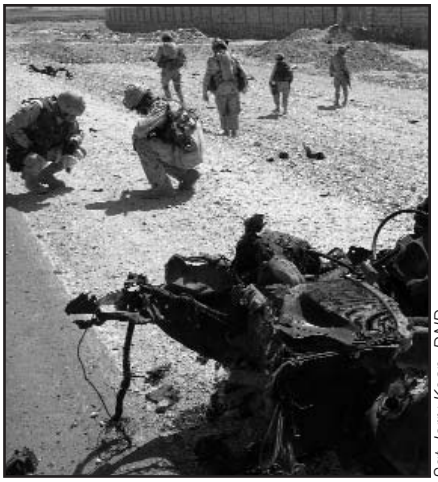
"It's basically just least-effort principle," says Ian Laverty, President and CEO of Environmental Criminology Research Inc. (ECRI), the Canadian company that now develops and distributes the geographic profiling software. "The most probable home site is simply the place from which it takes the least effort to travel to all the crime sites."

Defence Research and Development Canada (DRDC) is now working with ECRI and other partners to determine if the tool can be used to help combat improvised explosive device (IED) attacks and detect threat.

"We're basically trying to take this policing tool and adapt it for military use, so that instead of reacting to IEDs, we'll be able to take a more offensive approach," says Major Dave Waller, project director for the Counter-IED Technology Demonstration Program at DRDC.

The project is in its early stages, but Waller credits knowledge transfer from police as a key enabler for future research and development. In partnership with ECRI, RCMP geographic profiler Carl Sesely runs the software training program at DRDC, sharing his seven years of police profiling experience and teaching foundational theories on the geography of crime.

"Having that kind of expertise has been instrumental in generating acceptance of this (tool's) capacity (within the military community)," says Waller, adding that many geographic profiling concepts can apply to both police and military operations.



Sgt Jerry Kean, DND

A geographic profiling system developed for police work may help the Canadian military counter the threat of improvised explosive device attacks, like this one in Afghanistan in 2005.

Eighty-two police agencies in North America and Europe currently use ECRI's geographic profiling software

For more information on ECRI's geographic profiling software, visit ***www.ecricanada.com.***

—Caroline Ross

EMPOWERING THE VICTIMS OF BULLYING

Every seven minutes in Canada, a child or youth is the victim of bullying at school — a statistic identified by Canadian researchers. But bullying is often overlooked because bystanders are afraid to intervene and because victims feel alone and helpless.

"One thing we never really cover is the victim side," says Jordan Boudreau, a Grade 9 student who describes the anti-bullying programs offered by schools in Nova Scotia (N.S.), where he lives. "If we can empower the victims, we won't have to worry about bullying — know what I'm saying?"

Empowering victims is exactly the message of a student-led anti-bullying movement that swept through Nova Scotia schools last fall, generating media attention across North America and garnering support from provincial police.

The movement began when two high school students saw a younger student being bullied for wearing a pink shirt to school. The next day, the two students came to school wearing pink shirts and encouraged others to do the same. The message took off, with schools across the province holding "pink shirt days," and Nova Scotia's premier declaring the second Thursday of every new school year as "Stand Up Against Bullying Day."

RCMP officers in Halifax, Nova Scotia, wear pink arm bands to support a student-generated anti-bullying initiative.

Cst Anna Cochrane, Halifax District

RCMP officers who work in schools in Halifax, N.S., now wear a pink arm band in the school environment to show support for the student initiative.

"This is something student-generated and we're jumping on the bandwagon, showing our support," says Cst Curt Wentzell, the Halifax-area RCMP officer who started the pink arm band program. "Kids are enthusiastic. They appreciate authority figures supporting a youth initiative."

Wentzell says that combating bullying at school can have longer-term benefits, such as reduced bullying in sports, the workplace and beyond. "Bullying is a circle of violence," he says. "It's not totally removed from domestic violence."

Thirteen RCMP officers regularly visit Halifax-area schools to walk the hallways and speak to students about topics such as bullying, drugs and Internet safety.

—Caroline Ross

Crawling inside the criminal mind

Lessons learned from a criminal investigative psychologist

He has penetrated the psyches of countless psychopaths, pedophiles and hostage takers. He has spent time in the jail system assessing predatory sex offenders. He is one of only 17 people in North America who are both police officers and qualified psychologists, and one of even fewer who specialize in the criminal mind. S/Sgt Matt Logan, the RCMP's first criminal investigative psychologist, speaks with the Gazette's *Caroline Ross about his work.*

What was your most intense case?

The one that is most traumatic is when a hostage taker killed a hostage in front of me. I was the negotiator, and that was my first (negotiation). That was 1988. It wasn't a good introduction to hostage negotiation, but it moved me to take my Masters Degree (in psychology) at the University of Victoria. I recognized that this was a psychotic individual, and I had no understanding of what was going on with that individual. I felt kind of handcuffed (by my lack of knowledge).

As a criminal investigative psychologist with the RCMP, one of S/Sgt Matt Logan's roles is to identify emotional hooks, psychopathology and passivity in interview subjects.

Caroline Ross

How did you move into the position of criminal investigative psychologist?

I had finished my Masters degree. I came to Ottawa on a three-year tour of duty. The SEC (RCMP Senior Executive Committee) at the time, after Gustafson Lake, said, "Do we not have anybody in the RCMP that has an advanced degree in psychology that can help us deal with another Gustafson Lake or another major incident?"* They figured at that time that we'd be having major incidents all the time. So they said, "Would you go back and do your PhD?" and I said, "Sure."

What is your main role within the RCMP?

It's dissected into a number of assist or consultative roles, and probably working with major crime cases is the largest part of that right now. One of the roles is to look at cold cases — unsolved — look at the subjects of interest in those cases, and determine which of those suspects is the most likely to have committed the crime based on the mindset of the individual and the various personality factors.

What factors help you make an assessment?

For instance, if we know that the person is pyschopathic (psychopathy is determined by a diagnostic procedure that psychologists are specially trained to administer), we can say a lot about the personality features, the level of violence, the gratuitous nature of the violence. Then we can look at a crime and how it was committed, when it was committed, what was the context of the crime and make a determination of whether this might be a pyschopathic offender that committed that crime.

You do a lot of work with interview teams. What is your role there?

I sit in a room with a live feed and watch and give consult to the interviewers. I'm advising them on what I'm seeing of the mindset, what I'm seeing of the psychological makeup, what I'm seeing for emotional hooks that we can use (to build a firmer relationship), what I'm seeing about the relationship-building that is going on or not going on. I'm also watching for passivity, to make sure we're not taking a false confession.

You spent two years providing therapy to predatory sex offenders in the British Columbia prison system. What lessons did you bring back?

I learned so much about offenders, about offender mentality and what the needs of the offender are. Knowing your offender mentality is helpful in so many cases. It's especially important with the undercover team that we know the needs of the target. Is his primary need power? Ego? Greed? Those are the big three. If you can tell me that his biggest need is greed and his second is power and his third is ego, then I'll be able to tell you how we're best able to capture his needs and further the undercover project. ■

** In 1995, failed negotiations to end a land occupation at Gustafson Lake, B.C., resulted in one of the largest police interventions in Canadian history.*

Fighting cross-border cheque scams

Global partners pool intelligence

Photo: Project COLT

By Caroline Ross

You receive an e-mail: a businessman in the United Kingdom (U.K.) is relocating and wants to rent the apartment you advertised online. He mails you a company cheque for 12 months rent. After you deposit the cheque, he e-mails again: his job transfer has fallen through — could you wire him back his deposit, minus a fee for your trouble?

You do it, never suspecting that the "U.K. businessman" is a Nigerian youth in an Internet café; that the "company cheque" is a counterfeit mailed from Canada; that the wired funds were collected by criminal associates in Singapore.

What you do know — when your bank calls a month later to advise you of the counterfeit cheque — is that you must repay the losses. You're just another victim of cross-border mass-marketing fraud involving counterfeit cheques.

Rental schemes, lottery schemes, overpayment schemes, inheritance schemes — the list of scams is endless. And it's lucrative business. Between January and October 2007, law enforcement agencies in the United States (U.S.), Canada, the U.K., Nigeria and the Netherlands collectively seized over $2.1 billion, face value, in counterfeit financial instruments.

"It's a global problem," says Insp Mario Beaulne, officer in charge of major fraud with the RCMP. "A gentleman in Finland gets a letter from Singapore and needs to send money to Canada. Where are the bad guys? They're all over the place."

The bad guys are using international borders and the Internet to evade detection, but international law enforcement is starting to blow that cover, tracing the cross-border network of e-mails, letter mail and money transfers, connecting the dots and apprehending the perpetrators.

Tracing Internet communications

"Most victims, regardless of what country they're in, are identified through the Internet," says Greg Campbell, inspector in charge of global security and investigations with the U.S. Postal Inspection Service (USPIS), the agency responsible for protecting the U.S. mail system from criminal misuse.

Most victims are also U.S. citizens, thanks in part to American banking laws that require banks to make deposited funds available within five days — even though it may take weeks or months for a cheque to clear.

Courtesy of Greg Campbell, USPIS

American and Nigerian law enforcement officers discovered several counterfeit cheques concealed in this shoe, a flip-flop-style sandal, which Nigerian fraudsters were attempting to mail to criminal associates overseas.

To address the problem, USPIS investigators interviewed fraud victims and identified e-mail addresses implicated in the crimes. Working closely with Internet companies in the private sector, investigators were able to trace the line of communication back to the original Internet Protocol (IP) addresses.

Most IP addresses were from Nigeria, says Campbell, so the USPIS joined forces with Nigeria's Economic and Financial Crimes Commission, combining the IP address information with local intelligence in Nigeria. The partnership was so effective that the agencies were able to target specific Internet cafés and arrest several perpetrators on the spot.

"We used the tools of the suspects in order to identify where they were and to arrest them," says Campbell. "It was a private sector and international law enforcement effort. It had never been done before in the United States from a fraud standpoint."

Monitoring the mail

Mass-marketing fraudsters also rely on the mail system to cover their tracks. Counterfeit cheques are often produced in one country, mailed in bulk to associates in other countries, then re-mailed individually to foreign victims.

Montreal has become one of many re-mailing hubs, particularly for lottery scams targeting U.S. citizens, says RCMP Sgt Yves Leblanc.

Leblanc works in Montreal and runs Project COLT, one of six Canada–U.S. joint task forces investigating Canadian-based mass-marketing fraud. COLT partners — the RCMP, the Sûreté du Québec (Quebec provincial police), Montreal city police, the FBI, Canada Post Security and Investigation Services, the USPIS, Canada Border Services Agency, U.S. Immigration and Customs Enforcement, the U.S. Federal Trade Commission and the Competition Bureau of Canada — operate a mail interception program designed to identify and interdict counterfeit financial instruments as they enter or leave Canada via postal or courier mail.

Partners know what to look for, says Leblanc. Nigerian addresses, negotiable instruments over $10,000 and bundles of letters dropped in street letter boxes and affixed with specific postage are just some of the signs that could prompt further investigation in an attempt to nab the criminals behind mail fraud.

"When you investigate the people who are doing this," says Leblanc, "it's just small cells everywhere — two or three people working together, often with links to Nigeria."

While many of the counterfeits COLT has intercepted originate in Nigeria, others are produced in Canada by criminal offshoots. The patterns have only become evident over the last few years of mail interdictions, says Leblanc.

"It's difficult investigation, but we have a lot of success. In a lot of cases, we charge the people in Canada, and in a lot of others, we extradite people to the States."

Following the money

A third piece of the puzzle fell into place in March 2007, when the Canadian Anti-Fraud Call Centre's Criminal Intelligence Analytical Unit (CIAU) began a one-month pilot project to "follow the money" implicated in cross-border counterfeit cheque fraud.

The Canadian Anti-Fraud Call Centre is a repository for mass-marketing fraud complaints in Canada. The CIAU analyzes the complaints to identify trends and develop intelligence packages.

"We looked at our database for a period of one month, and we discovered that the vast majority of requests by the criminals were to send money to foreign financial institutions," says Cpl Louis Robertson, RCMP officer in charge of the CIAU.

The pattern was so clear that the CIAU extended the pilot indefinitely. But, says Robertson, Canadian investigators weren't able to link the money trail to other global fraud activity until six months later, when they met with their American, British, Nigerian and Dutch counterparts on a broader project to jointly assess the global threat presented by mass-marketing fraud.

At that meeting, the full picture of the cross-border counterfeit cheque fraud became clear.

"Each country may have a part of the information," says the RCMP's Beaulne. "A scam may be initiated in Nigeria, but then have criminal cells or links in other countries like the U.S. and Canada or elsewhere. In Canada, we might see where some of the envelopes are addressed and where some of the victims are asked to send the money, but we didn't necessarily understand where or who was behind the sending of the letters. At the same time, over in Nigeria and the U.S., (where investigators were pinpointing perpetrators), they may not have known exactly where the money was going.

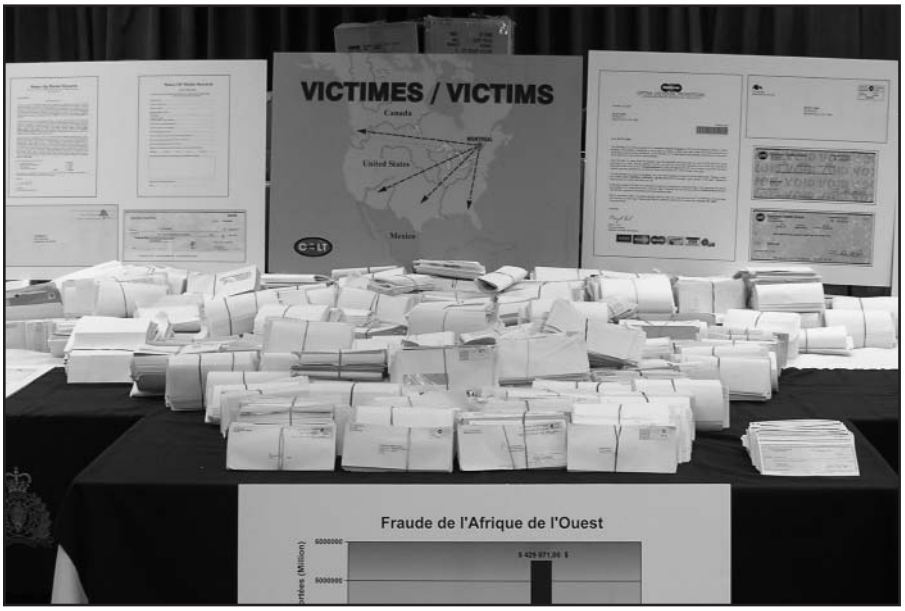
"The break-through, really, was that we were able to have all the key partners in the various countries able to share information and then close the loop on the whole process."

It's only one loop in a massive fraud network that involves many other countries and many other components — and the crimes will continue as the perpetrators relocate or employ new tactics to delay detection.

"We can't stop them all," says Campbell of the USPIS. "When we take off one suspect, there are plenty standing in line to fill that void. But we're not stopping. We will continue to investigate these crimes."

As the investigations and intelligence sharing continue, global law enforcement shines more light on the criminal trail, leaving future suspects with fewer shadows to hide behind. ■

The Project COLT joint task force in Montreal intercepted 14,648 lottery scam letters — and an accompanying $46 million worth of counterfeit cheques — destined for Canadian and American victims in November and December 2007.



Project COLT

Taking victims out of the loop

Identifying and prosecuting fraudsters is one aspect of the fight against global counterfeit cheque fraud. Teaching the public how to recognize, report and avoid scams is another.

"Education is the key — in all of the countries," says Greg Campbell of the United States Postal Inspection Service (USPIS). "If we educate the public not to become victims, then we take away the crime."

In October 2007, the USPIS and the Alliance for Consumer Fraud Awareness (U.S.) launched www.fakechecks.org, a public education web site specifically focused on counterfeit cheque fraud perpetrated via the Internet. The site includes videos, FAQs and victim interviews that help people recognize popular scams and overcome the stigma associated with reporting victimization.

Visit www.fakechecks.org.

Canada's National Anti-Counterfeiting Bureau

The front line on Canadian document integrity

By Caroline Ross

What's new with the RCMP's National Anti-Counterfeiting Bureau (NACB)? The word "National," for one.

In August 2007, the Bureau changed its name and its mandate to establish itself as a "centre of expertise" on counterfeiting activity and document security in Canada — a role that helps promote a more consistent, unified national anti-counterfeiting effort.

The RCMP began examining suspect documents in 1937, creating a separate counterfeit currency analysis unit in 1961. In 2003, both functions were amalgamated under the Bureau for Counterfeit and Document Examinations, but the program's directive to support police casework didn't reflect the group's emerging role as an advisor to government agencies outside the police arena.

"By the nature of our work, we get exposed to all kinds of methods by which security features on documents — like bank notes, passports and drivers' licences — are altered or counterfeited," says Shawki Elias, NACB program manager. "We see what security features are under threat and what kind of threat."

From 2003 to 2006, the NACB analyzed over 1.8 million counterfeit bank notes and 30,000 suspect documents. The Bureau examines every counterfeit bank note seized in Canada, identifying vulnerabilities and tracking trends in a database. NACB staff also visit seized counterfeiting operations to observe the tools and techniques criminals use.

That experience accumulates over time, says Elias, and the Bureau now receives regular requests to help federal and provincial agencies safeguard their documents against counterfeiting.

"In terms of defeating counterfeits, the people who have the pulse on (our document's) functionality and how it performs are the (NACB)," says Andy Ward at the Bank of Canada. "They bring real-world data to complement technical and scientific analyses performed by our in-house experts."

Ward is project manager for the next generation of Canadian bank notes, targeted for release in late 2011. He invited the NACB's Paul Laurin to sit on a currency development working group, because, Ward says, the NACB provides "first-hand, detailed and comprehensive knowledge of counterfeiting activity," as well as a "retrospective" history of how bank notes perform against counterfeiting over time.

That unique perspective has proved useful in the past, says Ward. In one instance, during a debate about whether to change a security feature on a particular bank note, Laurin drew on NACB analyses to verify that the feature was durable and not well-replicated by counterfeiters.

"That type of input helps the Bank make soundly based decisions," says Ward.

The NACB offers similar intelligence and advice to agencies responsible for travel and identity documents such as the Canadian passport, the Certificate of Indian Status and provincial birth certificates.

The Bureau also participates in larger government initiatives, such as the Document Integrity Interdepartmental Working Group headed by the Canada Border Services Agency. Under that group's auspices, the NACB chairs a technical subgroup of forensic experts who recommend minimum security features and analyze prototypes for federal and provincial travel and identity documents.

In Ontario, the subgroup helped the Ministry of Transportation ensure that its new provincial driver's licence incorporated leading-edge security features — like laser-engraved photographs — that strengthen the card against tampering.

"There's nothing like knowing first-hand exactly what's happening on the street with the cards," says Steve Burnett, manager of the Ontario driver's licence project. "With all the identity theft and counterfeiting that's going on, we need to make sure we have a secure card to help protect the identity of Ontarians."

These collective efforts help standardize Canadian document integrity and ensure that cross-jurisdictional initiatives support one another. A driver's licence, for example, can be used as a secondary document to confirm the identity of passport applicants. With fewer counterfeit drivers' licences in circulation, the Canadian passport becomes more secure.

In the past, says Elias, Canada lacked a well-coordinated document integrity effort. Today, that effort is there, and the NACB is a key part of it. ■

Caroline Ross

Sonia Michaud, a forensic specialist with the NACB, uses specialized equipment to view the ultraviolet light security features on a Canadian twenty dollar bill.

Building an Olympic legacy

Unit targets construction fraud for Vancouver 2010

By Caroline Ross

Nine competition venues, two athletes' villages, significant highway upgrades, and new urban rail lines. Total projected cost of construction: over $3.1 billion, most of it public funds.

Infrastructure development for the 2010 Winter Olympic Games and Paralympic Games in Vancouver, British Columbia, is lucrative business — but it's not always construction companies and communities that benefit. Fraudsters and organized crime groups may also be rubbing their hands together with glee.

Whispers of corruption certainly overshadowed the Montreal 1976 Games. There, false billing and crooked contractors allegedly contributed to a massive $3 billion Games deficit, which tax payers spent 30 years paying down. The original Games budget was $300 million.

To prevent similar corruption from marring Vancouver's Olympic legacy, Vancouver 2010's RCMP-led Integrated Security Unit (ISU) formed a special financial intelligence unit charged with forestalling fraudulent activity and safeguarding the public (and private) funds implicated in Games construction.

"It comes to about $4.5 billion worth of infrastructure development that we're actually providing some level of economic integrity intelligence support to," says Insp Alex Graham, the RCMP officer in charge of the ISU joint intelligence group (JIG), under which the financial intelligence unit operates.

Established in May 2005, the JIG is the first group of its kind to target financial intelligence issues within the context of a major sporting event. The group combines traditional intelligence-gathering techniques with financial expertise to uncover illegal economic activities like price-fixing, overcharging, bribery, contract fraud and theft of materials. Labour shortages in British Columbia's construction industry have also prompted the group to investigate potential links to illegal immigration.

The group has passed some investigations over to municipal police forces or federal partners for further action, but criminal prosecution is not necessarily the ultimate goal.

"In a lot of instances, what we're seeking to do is mitigate the matter before it ends up in a prosecution," says Graham.

Mitigation strategies include advising construction companies and project managers of potential pitfalls and areas for improvement — such as opportunities to enhance quality monitoring or shore up on-site security — and working with partners to include specific access-to-information clauses in key construction contracts.

"That (contract language) allows us to have access to information that normally would require a search warrant," says Graham, who notes that reviewing a company's financial records, management structure and other tombstone data can help investigators determine links to organized crime.

The measures are designed to stop fraudulent activity before it starts, says Graham, and most contractors approve of the arrangement. "The vast majority of business people and corporate entities involved in these projects are honest and not associated with organized crime. . . . They don't want to hire a sub-sub-contractor that is going to cause them some concerns."

The JIG's activities complement other measures implemented by partner agencies in charge of Olympic construction. The Vancouver Olympic Organizing Committee (VANOC), the British Columbia Ministry of Transportation and Canada Line Rapid Transit Inc., for example, utilize ISO9000-certified quality management systems. VANOC requires contractors to regularly test construction materials and submit the results for comparison against the committee's own independent test data.

VANOC

The Whistler Nordic Centre ski jump area is just one of the new venues under construction for the Vancouver 2010 Winter Olympic Games.

"That way, we ensure we get a quality product," says Dan Doyle, executive vice-president of construction with VANOC.

Doyle says that VANOC's construction managers haven't uncovered "any scent of fraudulent activity" to date, but if they did, he says, "we wouldn't hesitate a millisecond to bring the RCMP ISU in."

With infrastructure development well under way and most construction contracts for Vancouver 2010 already awarded, the JIG will begin monitoring the large number of service contracts required to feed, transport, entertain and clean up after Games participants.

The work to date has also become a best practice for future Olympic Games, such as London 2012. "They've looked to us for some direction" says Graham. "They're improving on what we have." ■

How does your agency identify its fraud priorities?

The panellists

Supt Stephen Foster, Director, RCMP Commercial Crime Branch
Jonathan J. Rusch, Special Counsel for Fraud Prevention, Criminal Division, Fraud Section, U.S. Department of Justice
Murray Taylor, National Co-ordinator, Economic and Special Operations, Australian Federal Police

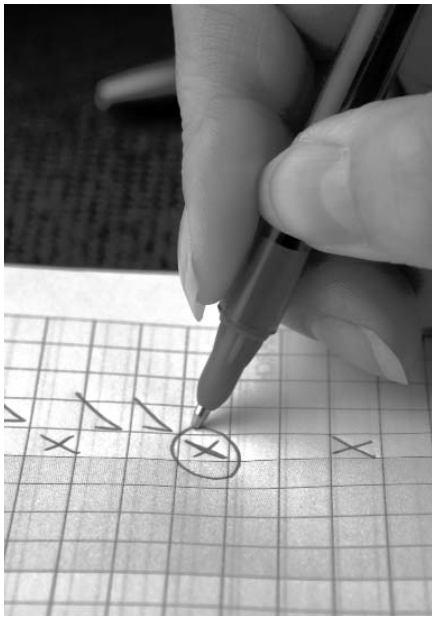
Supt Stphen Foster

The RCMP's Commercial Crime program has 27 operational units located in major cities across Canada. Commercial Crime's enforcement response to the wide variety of fraud-related criminal activities identified in our mandate is multi-faceted. Criminal activities encompassed by our mandate range from major fraud to mass marketing fraud to corruption to identity fraud. As well, the mandate includes crime prevention and deterrence through public education and awareness. Given this context, I think a broad perspective answer is required.

At the organizational level, RCMP senior management identifies national strategic priorities. Economic integrity is one of five such priorities. The other four are organized crime, youth, terrorism, and aboriginal communities.

Through threat assessments, media monitoring and demands for service, the Commercial Crime Branch identifies emerging fraud trends which pose the greatest risk to the public. On this basis, identity fraud and mass marketing fraud are our current enforcement priorities. Other branch priorities are currency counterfeiting, payment card fraud and corruption.

As resources are limited, we need to strike a balance between complaint investigations, intelligence-led investigations, and prevention awareness activities. Prioritizing between these activities is a judgment call. Operational unit managers allocate resources between these activities, often taking local factors and concerns into consideration.



The Priority Rating of Operational Files (PROOF) system is a tool developed by the Commercial Crime Branch to assist unit managers. PROOF is a software system that interprets 12 case-related specifics and assigns an overall numerical value to an investigation. This numerical value is the "PROOF score." A higher PROOF score indicates that a matter should be given a higher priority. For example, PROOF criteria include the following: whether the offence is within mandate; the offence's dollar value (higher yield gives a higher score); the age of the offence (more recent gives a higher score); and ease of gathering evidence (easier gives a higher score).

At the tactical level, our operational units prioritize between investigations. Managers consider several factors: PROOF score; whether the investigation touches one or more of the strategic priorities; Commercial Crime mandate; whether the activity is a branch priority; existing agreements, such as international treaties and memorandums of understanding; the dollar value involved; whether investigative expertise is required; victim impact; whether the offence relates to corruption; and, again, local factors.

The process of identifying RCMP Commercial Crime fraud priorities is well-rounded, taking many factors — both strategic and tactical — into consideration.

Jonathan J. Rusch

The United States Department of Justice identifies and implements its anti-fraud priorities in three ways. First, pursuant to the Department's Strategic Plan for 2007–2012, the Department's Criminal Division adopted a management plan that includes the following priorities:

- Ensuring the integrity of government. Under this priority, the Criminal Division pursues crimes such as election fraud, immigration fraud and procurement fraud, as well as public corruption relating to these and other offences. For example, the Department has established special task forces to pursue procurement fraud and fraud of all types stemming from disasters such as the 2005 hurricanes Katrina, Rita and Wilma, as well as fraud stemming from the reconstruction of Iraq.
- Safeguarding and maintaining

confidence in the marketplace. Under this priority, the Criminal Division pursues crimes such as corporate fraud, mass-marketing fraud, identity theft and cybercrime.
- Reducing violent and organized crime. Under this priority, the Criminal Division pursues crimes (including fraud) that various types of criminal organizations commit to obtain illicit proceeds and to support their operations.
- Transnational criminal enforcement. Under this priority, the Criminal Division pursues various types of crime that are conducted across international borders, such as organized crime and cybercrime, and actively conducts and supports international law enforcement training and institution-building.

Second, senior representatives of the Department and the Criminal Division chair a number of national-level interagency working groups that concentrate on particular types of fraud. These include the Bank Fraud Enforcement Working Group, the Corporate Fraud Task Force, the Mass-Marketing Fraud Working Group, the Mortgage Fraud Working Group, and the Securities and Commodities Fraud Working Group. In addition, the President's Identity Theft Task Force has a Criminal Law Enforcement Subgroup. Each of these working groups convenes regular meetings that enable representatives of the Department and federal investigative agencies such as the FBI, the Postal Inspection Service and the U.S. Secret Service to share information on particular fraud trends and to identify opportunities for interagency co-operation in investigating these types of fraud.

Third, the Department of Justice, under the leadership of the Criminal Division, has initiated and conducted a number of proactive enforcement initiatives that target specific types of fraud. These include Operation Roaming Charge (2004), which targeted domestic and international telemarketing fraud, Operation Global Con (2006), which targeted international mass-marketing fraud conducted by criminal groups, and several operations directed at online economic crime. These operations have become increasingly international in scope, as U.S. law enforcement agencies recognize the importance of building co-operative relationships with law enforcement agencies in Canada and other nations and collaborating in transnational investigations and prosecutions.

Murray Taylor

The Australian Federal Police (AFP) recognizes that in order to maintain public confidence, anti-fraud business practices must be continuously improved and re-engineered to remain abreast of emerging technologies and new vulnerabilities.

In accordance with the AFP Fraud Control and Anti Corruption Plan (FC&AC Plan) 2007-2009, a range of best practice fraud-control and anti-corruption initiatives have been implemented across all functional areas of the AFP.

> **"U.S. law enforcement agencies recognize the importance of building co-operative relationships with law enforcement agencies in Canada and other nations."**

During preparation of the most recent FC&AC Plan, the AFP conducted risk assessments across the organization by devolving the risk management process to the business unit level. Managers and employees were asked to identify, analyze and evaluate internal and external risks and threats to their own business area as they relate to specific categories defined in the Commonwealth Fraud Control Guidelines.

Numerous risks were identified and evaluated across the organization. The highest risk category dealt with managing information technology and information security. Another risk identified was the management of client and strategic partner relationships in support of their respective anti-fraud initiatives. Finally, electronic commerce, electronic service delivery and the Internet were prioritized highly during the risk assessment process.

In accordance with directions provided by a high-level oversight committee, all fraud and corruption control issues are addressed and prioritized based on the likelihood of risks increasing and appearing across a number of business units. Treatments applicable to all fraud and corruption risks are continually monitored for their effectiveness and results are reported to the committee for review.

All medium residual risks identified across a number of business units are given higher priority for management and monitoring. Lower residual risks are managed through existing internal controls and are not subjected to further risk mitigation on the basis that they are at an acceptable level.

Performance monitoring and quality assurance occurs through environmental scanning and a professional standards complaint-analysis system. Emphasis is placed on identifying organizational fraud and corruption trends that can be addressed and treated. Within this model, allegations of corruption are the subject of independent oversight by the Australian Commission for Law Enforcement Integrity.

Externally, AFP fraud statistics are reported to the Attorney-General's Department. Furthermore, in accordance with the Commonwealth Fraud Control Guidelines, the Commissioner certifies to the Minister for Home Affairs in the AFP's Annual Report that he is satisfied that appropriate fraud prevention, detection, investigation and data collection procedures and processes are in place.

The current FC&AC Plan serves to integrate anti-fraud organizational risk assessment and reporting processes by recognizing that identifying risks is an integral part of everyday business across all functions of the AFP. ■

It's personal

Identity fraud and the Canadian consumer

Insp Barry Baxter
Counterfeit and Identity Fraud
RCMP Commercial Crime Branch

Identity fraud — the theft and fraudulent use of personal information for criminal purposes — is one of the fastest growing crimes of the new millennium. It is estimated that the fraudulent use of personal identities costs Canadian consumers more than $2 billion annually.

Our personal and financial information has become a valuable commodity. It can be — and is — captured through sophisticated Internet schemes, computer or database hacking, or organized mail-theft rings, then bought and sold in cyberspace.

Given the potential for high profit and the low risk of detection, identity fraud has drawn the interest and active involvement of organized crime. These crime groups are joining forces with sophisticated cybercriminals who have progressed from flashy notoriety-motivated attacks to stealthier, targeted and sophisticated attacks on government and corporate personal information databases.

Acquiring and using personal information to fraudulently obtain genuine identity documents or create forged identity documents is also a concern.

Identity theft or identity fraud?

The public and media continue to use the term "identity theft" to describe the criminal activity. In fact, your identity is a possession that cannot be stolen from you and you cannot be deprived of it. It can be assumed or taken over for periods of time, but you will always be you. The true criminal activity and the correct term is "identity fraud."

There are two distinct acts in the fraudulent use of an identity. There are also different motivations for each act.

The first act is the actual acquisition or theft of personal or financial data. Sophisticated Internet schemes known as phishing or pharming attempt to deceive the public into revealing account numbers, passwords or other personal data. There have also been hacker attacks directed at mass information storage databases.

Once armed with sufficient levels of personal and financial data, criminals can take over bank accounts, move funds held on deposit or acquire lines of credit.

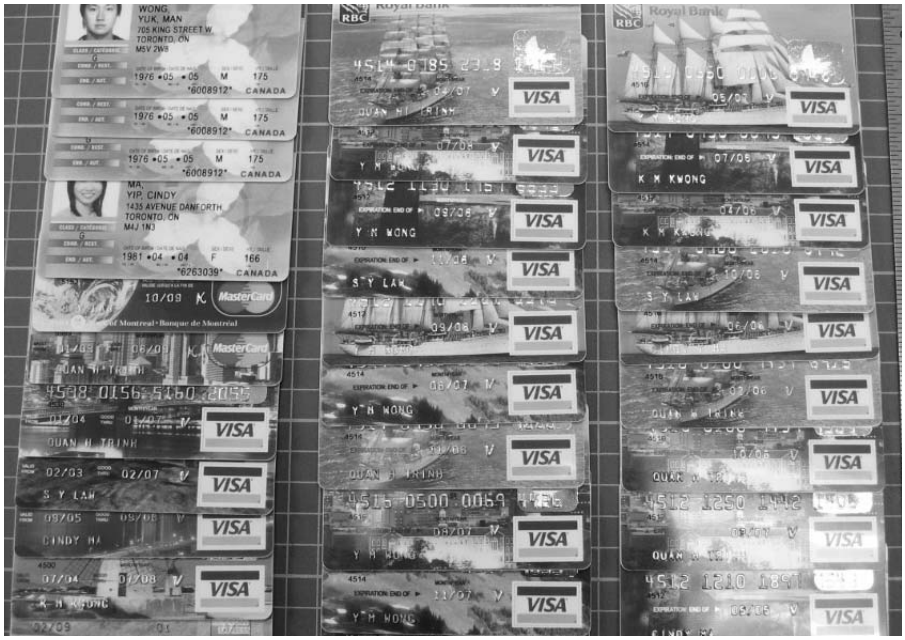
Criminals also conduct research of open-source databases such as vital statistics to create profiles from deceased persons, the so-called "tombstone identities." Once armed with a name and date of birth, criminals can obtain a rental postal box and cellular telephone number from which applications can be made for a replacement birth certificate, Social Insurance Number (SIN) card, health card or other documents as well as credit cards. With these documents a passport can be obtained, resulting in a full tombstone identity being created.

In Canada, the federal government has recently introduced new legislation under Bill C-27 that, if passed, will make it an offence to procure, possess, transfer, sell or offer for sale another person's identity document without lawful excuse, or to knowingly obtain, possess or traffic in another person's personal information for fraudulent purposes.

In the meantime, the second act — fraudulent use of the another person's personal data — is the true criminal activity. This can include falsely applying for government services or programs, obtaining genuine government-issued documents through false applications, or acquiring fraudulent payment cards. Once armed with sufficient levels of personal and financial data, criminals can take over bank accounts, move funds held on deposit or acquire lines of credit — all in another person's name and without their knowledge or consent.

Fraudulent use can also include imper-

Once armed with a few key documents, criminals can apply for and obtain a passport, resulting in a full tombstone identity being created.



RCMP Commercial Crime Branch

sonation as defined in Section 403 of the Criminal Code, when an identity is actually assumed or taken over, usually to obtain goods or services such as an office rental or cellular telephone. The assumed identity is used to hide the true identity of the culprit. Systematically created identity packages including forged or fraudulently obtained documents also facilitate a criminal's ability to travel nationally or internationally in anonymity.

Payment cards

Payment card fraud is technically identity fraud. For that brief time period when a forged card is being utilized for a transaction, that person's identity is being fraudulently used.

A payment card is legally defined as either a credit card or a debit card. A card's magnetic data can be obtained by criminals without the owner's approval through a card skimming operation. Your personal identification number (PIN) can be obtained through the use of a pinhole camera or a pin pad overlay. Once armed with your card's magnetic data and PIN, a criminal can create a forged or counterfeit card and use it to obtain goods and services.

Virtually all payment card fraud is related to organized crime. The 2006 combined payment card fraud losses in Canada exceeded $1 million per day. These proceeds fund a variety of criminal activities including drug trafficking, buying weapons, smuggling, loan sharking and prostitution.

If fraud is determined, the account holder's financial institution suffers the monetary loss. There is also a short period of denial of service as cards are replaced. This directly impacts consumer confidence in Canada's economic stability.

Who investigates identity fraud?

All law enforcement agencies are responsible for the investigation of offences under the Criminal Code. Most identity fraud offences relate to some form of deceit, false pretense or false application.

Within the RCMP, the Commercial Crime program is responsible for the investigation of identity fraud offences that are of a national or international significance, such as when the federal government, a provincial government or their programs or services have been victimized or when the integrity of a corporate entity's database has been compromised. Because many of these types of investigations are Internet-related and global in nature, Commercial Crime works closely with the Technological Crime Branch for the information technology aspect and with the National Anti-Counterfeiting Bureau for the examination of documents.

Identity fraud trends

Criminal groups and cybercriminals are using advances in technology to create and deliver very sophisticated attacks. Internet phishing sites are developed to duplicate legitimate user sites and entice unsuspecting Canadians into providing personal and financial information that is later used for fraudulent purposes.

Virtually all payment card fraud is related to organized crime. These proceeds fund a variety of criminal activities including drug trafficking, buying weapons, smuggling, loan sharking and prostitution.

The frequency of the attacks on personal information databases held by government and private industry entities is worrying. These "hacker attacks" target government agencies, credit profile agencies, service providers, financial institutions and other holders of large volumes of data. Statistics indicate private businesses account for 40 per cent of all compromises followed by government offices at 25 per cent, the health care industry at 20 per cent and educational institutions at 15 per cent.

Many Canadians are exposing their personal data on social networks such as Facebook and MySpace, and through online dating services. All of these entities are susceptible to hacking and compromise.

Victims

Instances of identity fraud in Canada are significantly under-reported. Many people who are victimized are reluctant to report the incident to police because of embarrassment at being scammed or a perceived lack of evidence to provide police. Within the payment card industry, once a skim site is identified, all card holders whose card may have been compromised are notified that their present card has been cancelled and that they will receive a new card. The skim site is not identified, so the card holder cannot report the incident to police.

In Canada, the holders of personal and financial data are under no regulation or obligation to publically report breaches of their security — either to those potentially affected or to law enforcement agencies. In the past few years, there have been a number of high-profile database compromises that have resulted in significant Canadian victimization.

Your credit rating is the mechanism by which you can obtain credit, a mortgage or a business loan. If your rating is adversely affected by identity fraud, you are required to provide assurances to the credit services that unpaid bills, defaults on loans, and collection processes instituted against you are not of your own doing. It may take several years before your proper profile can be restored. The newly introduced legislation under Bill C-27 allows a court to order restitution to victims for expenses incurred to re-establish their identity, replace identity documents and correct their credit history and credit rating. ■

For more information and protection guidelines, visit ***www.rcmp-grc.gc.ca*** and follow the links to scams/fraud.

Disaster relief fraud

Lessons learned from Hurricane Katrina

By the Hon. David R. Dugas
United States Attorney for
the Middle District of Louisiana
Hurricane Katrina Fraud Task Force
Joint Command Center

Hurricane Katrina slammed into the Mississippi Gulf Coast in the early morning hours of Monday August 29, 2005. The combination of wind and storm surge destroyed 69,000 homes in Mississippi and devastated entire coastal communities in that state.

Louisiana was spared the worst of the hurricane-force winds, but experienced a significant storm surge. New Orleans, Louisiana, lies mostly below sea level and is protected by an elaborate system of levees and pumps. Soon after the winds abated, word filtered out of New Orleans that the Industrial Canal levee had failed. That was followed by reports of other levee breaches and widespread flooding throughout the city. By nightfall, 80 per cent of the city of New Orleans had flooded and over 200,000 homes were destroyed. Over 1.8 million people fled or were rescued from the devastation of Hurricane Katrina and relocated throughout the United States.

Hurricane Katrina Fraud Task Force

The U.S. Department of Justice created the Hurricane Katrina Fraud Task Force on September 8, 2005, just 10 days after Hurricane Katrina made landfall. The Department anticipated that massive devastation would spawn fraud that would be both multi-faceted and multi-jurisdictional. The challenge for the Task Force was to devise a structure that could co-ordinate thousands of investigations by dozens of federal and state law enforcement agencies and Inspectors General offices in multiple jurisdictions.

The Task Force is led by Alice Fisher, the Assistant Attorney General for the Criminal Division of the Department of Justice, in co-ordination with the Inspectors General and the heads of the key federal law enforcement agencies in Washington, D.C. The National Command Center in Baton Rouge, Louisiana, provides day-to-day co-ordination, lead collection, lead screening, streamlining of investigations, and data management. The districts most affected by the hurricanes created district working groups led by the U.S. Attorneys' offices in those districts. Districts without working groups designated points of contact to interact with the Command Center and the Task Force.

Post-Katrina fraud

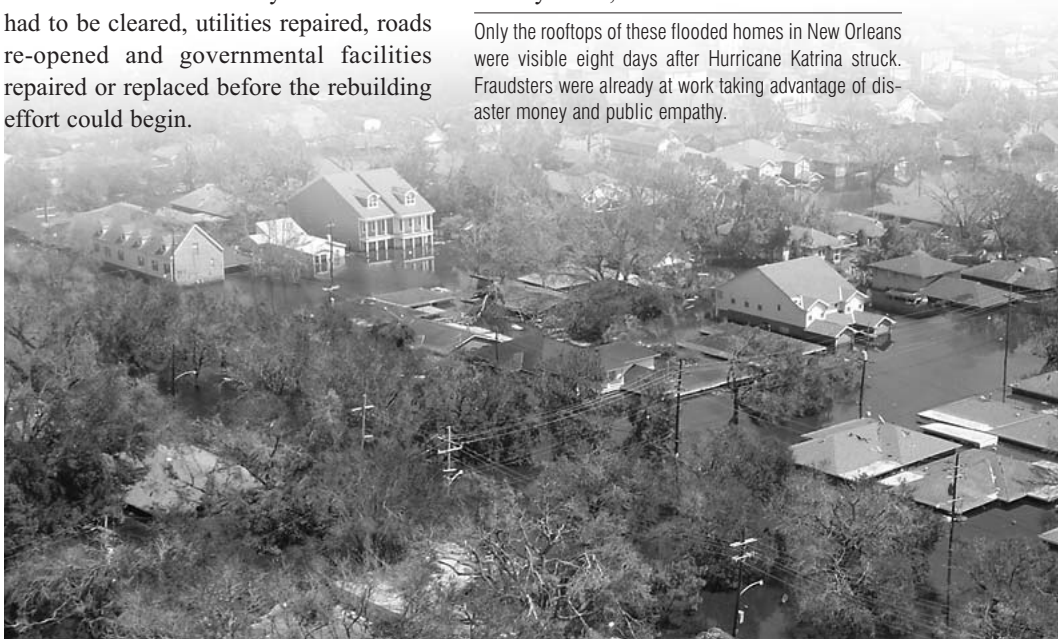
The scope of the fraud following Hurricane Katrina mirrored the scope and reach of the disaster recovery efforts. Residents of the affected area evacuated to every state in the nation. Massive search-and-rescue operations required unprecedented logistical support. Food, water, ice, fuel, generators, communications, medical supplies, temporary housing and transportation had to be brought in to the devastated area to support the relief efforts. Over 100 million cubic yards of debris had to be cleared, utilities repaired, roads re-opened and governmental facilities repaired or replaced before the rebuilding effort could begin.

The first anti-fraud lesson learned from Hurricane Katrina was not a new one, but was driven home by the scope and breadth of the fraud: fraud follows the money. Most disaster relief programs were afflicted by fraud that started as soon as the money began flowing to the affected areas.

Fraudulent schemes

The first fraudulent schemes appeared within days of the disaster. Fraudulent charity schemes attempted to solicit money from a concerned public eager to contribute to any charity that was assisting the victims of the disaster. In Florida, a fraudulent website called www.AirKatrina.com solicited donations for purported medical relief and evacuation flights into the affected areas. In Bakersfield, California, workers hired by the American Red Cross to staff an emergency call center began submitting fraudulent emergency relief applications for themselves, their friends and associates. Over 80 defendants have been charged with fraud related to this call center.

The Federal Emergency Management Agency (FEMA) received over 2.5 million applications for individual emergency assistance from evacuees in all 50 states. Some of those applications were fraudulent. In Oregon, Florida, Illinois, Pennsylvania, California and numerous

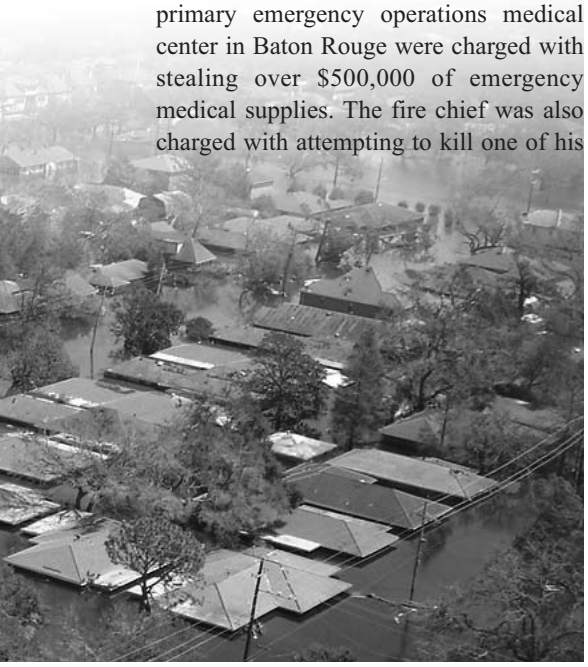


Only the rooftops of these flooded homes in New Orleans were visible eight days after Hurricane Katrina struck. Fraudsters were already at work taking advantage of disaster money and public empathy.

other states, individuals who were not living in the affected areas and were not affected by the hurricanes nevertheless submitted false applications to FEMA or the American Red Cross claiming to be displaced victims of the disaster needing emergency assistance. To date, prosecutions against such individuals have been brought by 41 of the 93 U.S. Attorneys' offices across the United States.

In many cases, the fraudulent applications were successful because the flood of applicants prevented the relief agencies from verifying each application. As criminals realized this vulnerability, the schemes expanded. Some submitted multiple fraudulent applications. Others recruited individuals and submitted fraudulent applications on their behalf in exchange for kickbacks. In Georgia, one individual submitted 51 fraudulent applications for Disaster Unemployment Assistance to the Louisiana Department of Labor. In Florida, Louisiana, Mississippi, Alabama, Texas, and even as far away as Oregon, prosecutions have been brought against organized rings accused of systematically exploiting the emergency relief programs.

In some cases, the fraud was committed or facilitated by insiders. In one such scheme, a fire chief and several co-workers who volunteered to work at FEMA's primary emergency operations medical center in Baton Rouge were charged with stealing over $500,000 of emergency medical supplies. The fire chief was also charged with attempting to kill one of his cohorts whom he believed was co-operating with law enforcement in the investigation of the theft.



David R. Dugas

In Louisiana, prosecutions have been brought against FEMA employees for soliciting bribes from contractors in exchange for allowing overbilling under emergency relief contracts.

Investigative techniques

The challenge in dealing with fraud following a disaster is often more logistical than tactical. Fraud typically follows familiar patterns of "lying, cheating and stealing" that most trained law enforcement officers know how to investigate. However, the scope of the fraud can overwhelm law enforcement agencies in the affected area and surprise law enforcement agencies located in areas remote from the disaster zone. Finding, deploying and maximizing the resources needed to combat that fraud can be the first and greatest challenge that faces law enforcement officials following a disaster.

In order to investigate disaster fraud, law enforcement agents need investigative leads, access to evidence, and the resources to conduct the necessary investigations and prosecutions. The best sources of leads and evidence will be the public and the internal data and records of the disaster relief agencies.

Because the sheer volume of tips and leads can result in overlapping and potentially conflicting investigations by multiple agencies, a task force or working group is needed to co-ordinate investigations. If the disaster is large enough, then a dedicated command center can serve as a centralized lead-collection, screening, and referral vehicle to ensure that overlapping and conflicting investigations are avoided. The task force and its command center can also serve as a central repository for information on where to find and how to obtain the evidence needed to conduct investigations. The task force can establish protocols to streamline evidence collection and assist investigating agents in locating witnesses and documents.

In the case of the Hurricane Katrina Fraud Task Force, the public has provided many of the best leads through hotlines created by the Task Force and answered at the Command Center. The Command Center receives and screens all leads and complaints of disaster fraud from all sources, verifies information through agency databases, collects records that are relevant to the fraud allegations and refers each lead to the appropriate law enforcement field office with a package of information that will assist the agency in conducting its investigation. All leads and referrals are logged in the Command Center's database and cross-checked against the database to avoid duplication of investigations. The Command Center has screened and referred almost 14,000 leads that have resulted in the prosecution of over 830 defendants to date.

For law enforcement officials charged with investigating disaster fraud, I recommend following three basic principles.

First, do not reinvent the wheel. Your agents, officers and prosecutors know how to do their jobs. Your job is to make sure that they have what they need to do their jobs. Try to provide that within existing and familiar structures and protocols.

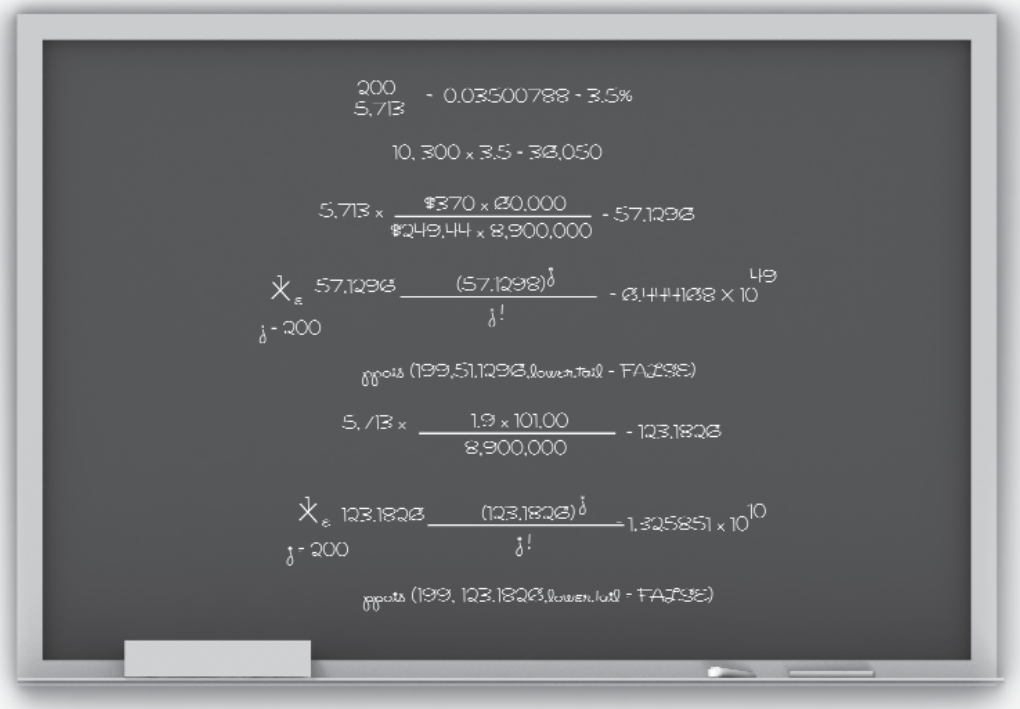
Second, do no harm. Do not create a task force or working group that merely overlays an extra level of supervision or command. In the Hurricane Katrina Fraud Task Force, the Command Center collects, screens and analyzes leads and refers the leads to investigative agencies; however, it does not manage the investigations or ask agents to report on the status of investigations.

Third, leverage your assets through co-operation, communication and co-ordination. A task force can add considerable value by avoiding conflicting or overlapping investigations, distributing leads based on agency expertise and resources, facilitating multi-agency investigations and providing subject matter expertise to assist agents and prosecutors with the unique aspects of disaster fraud cases. With proper communication and a co-operative attitude, the whole of the task force can quickly become greater than the sum of its parts. When that happens, the agencies and the public they serve reap the benefits. ■

LOTTERY FRAUD

Solving crime using math

By Professor Jeffrey S. Rosenthal
Department of Statistics
University of Toronto



On the CBS television series NUMB3RS, crime-fighting mathematician Charlie Eppes boldly declares, "Everything is numbers!"

Well, that might be an exaggeration. But my involvement in a recent investigation into lottery fraud has convinced me that statistical analysis can indeed be used to uncover fraudulent behaviour that might otherwise pass undetected.

Many lottery players simply hand their tickets over to the local store clerk, asking if they have won anything. This opens the door for unscrupulous clerks to pretend that a winning lottery ticket won nothing (or just a tiny prize), then later claim the big lottery jackpot for themselves.

Does such fraudulent behaviour actually occur?

In 2001, Bob Edmonds, a 75-year-old resident of Coboconk, Ontario, claimed that a local retailer had defrauded him out of a $250,000 winning lottery ticket. Subsequent investigation proved him correct, and in 2005 the Ontario Lottery and Gaming Corporation (OLG) finally settled with him for $150,000. However, the OLG fought the case very hard before settling (incurring $425,000 in legal costs), and insisted on a gag order to keep the settlement confidential. This raised suspicions about whether the OLG was hiding other similarly fraudulent wins by other store clerks. The CBC television program The Fifth Estate asked me to look at the numbers.

Through a Freedom of Information request, the CBC ascertained that between 1999 and 2006 there were a total of 5,713 major Ontario lottery wins (of $50,000 or more), of which about 200 (3.5 per cent) were identified as being won by people who worked in stores that sold lottery tickets. (Store clerk wins were only recorded if the lottery winner answered yes when the OLG asked if they worked at a store. Some winners might have lied, so the true figure could be higher than 200.)

Many lottery players simply hand their tickets over to the local store clerk, asking if they have won anything. This opens the door for unscrupulous clerks to later claim the big lottery jackpot for themselves.

The question was: how many major prizes should we have expected these sellers to win? And what were the odds that they would win 200 or more of them honestly — by pure luck alone?

To answer these questions, we first needed to know the total number of retail lottery sellers at any given time. The OLG said they didn't know this figure, so we had to sort through the numbers and figure it out.

There are 10,300 lottery ticket sales locations in Ontario. A Fifth Estate survey indicated there were about 3.5 sellers per location, or about 36,050 sellers total. By contrast, an OLG executive had testified in court that there were "50,000 or 60,000" such sellers. Then, just five days before the Fifth Estate program was to air, the OLG unexpectedly presented a brand new table, now claiming a total of 140,000

sellers. On closer inspection, this turned out to mean 101,000 active sellers plus 39,000 annual "turnover" (former employees, who weren't actually relevant to the count).

We also needed to know how much these sellers spend on lottery tickets compared to the general adult population. Again the OLG said they didn't know. So the Fifth Estate did another survey, concluding that the average lottery seller spends about 1.5 times as much as an average adult. (The OLG later conducted its own survey and got a similar answer of 1.9. And Corporate Research Associates Inc. [CRA] studied this same question in Atlantic Canada and obtained a factor of 1.52 — virtually identical to the Fifth Estate figure.)

From all of these numbers, what can we conclude?

Using the figure of 60,000 sellers (from the OLG's court testimony), together with the spending factor of 1.5 (from the Fifth Estate and CRA surveys), we would expect that, in the absence of fraud, lottery sellers would win about 57 of the major prizes between 1999 and 2006 — far less than the 200 they actually won. The probability of their winning 200 or more by pure luck alone would be unimaginably small — less than one chance in a trillion trillion trillion trillion.

Even taking the largest OLG estimates — 101,000 sellers spending an average of 1.9 times as much as the general adult population — we would still expect just 123 major seller wins over this time period. The probability of their winning 200 or more major prizes would then be less than one chance in seven billion — again, absolutely inconceivable.

It was clear that lottery sellers were winning significantly more major lottery prizes than could be accounted for by chance alone. The statistics proved the existence of widespread lottery fraud.

Regarding store type, only about one-fifth of retail lottery sellers work at independent convenience stores, but a much higher percentage of the defrauding instances occurred in such stores. (The OLG wouldn't tell the CBC precisely how many, but an OLG "FAQ" webpage later admitted that 53 per cent of the recorded insider wins were specifically from sellers at convenience stores.) This large number of convenience store wins could not have arisen purely by chance.

It was also interesting to consider retail store owners as a separate group, disregarding non-owner employees. Those owners won about 83 of the major wins between 1999 and 2006. We didn't know the precise number of retail store owners (and again, the OLG wouldn't say), but even under the most generous assumptions, we would expect at most 25 owner wins — far fewer than 83. This provided still more evidence of fraud.

When the Fifth Estate episode finally aired in October 2006, the story immediately became front-page news. The issue was debated in the Ontario legislature, the government was put on the defensive, and the Ontario Ombudsman launched a full investigation.

At first, the OLG tried to refute the statistical findings. They hired their own consultants, denied there was significant lottery fraud, and insisted that the Edmonds case was simply an isolated incident. But the evidence against them was overwhelming. By the time the Ombudsman issued his report, five additional cases of lottery fraud had been identified, the OLG's handling of the situation was thoroughly criticized and discredited, the OLG's CEO had been fired, and many people agreed that reforms were needed.

On the positive side, the OLG has now instituted some specific policy reforms. Customers are instructed to sign their lottery tickets before redeeming them. And self-checker machines allow customers to easily learn what they've won before handing their tickets to anyone else.

Other provinces also got involved. Soon after the Fifth Estate program aired, British Columbia's Ombudsman launched a similar investigation, which found the British Columbia lottery system "open to fraud by retailers trying to cheat customers," and led to the firing of the British Columbia Lottery Corporation's CEO. A study I later conducted for the Nova Scotia Gaming Corporation found that during the period between 2001 and 2006, the number of major lottery wins by Nova Scotia retail store owners was also inconceivable by pure chance alone — so lottery ticket sellers must have defrauded customers there, too.

Cases like these illustrate that statistics have an important role to play in determining the extent of fraud. We all know that seemingly random occurrences can accumulate into hard evidence. The challenge is to recognize situations where statistical analysis might help, then use careful probabilistic modelling to determine whether or not the observed results could have occurred through pure chance alone. ■

Jeffrey S. Rosenthal is a professor in the Department of Statistics at the University of Toronto. He is the author of the book "Struck by Lightning: The Curious World of Probabilities" (Harper Collins Canada, 2005).

Seduced by the Internet

Joint police effort saves Australian scam victim

A South Australian man who fell victim to an online dating scam is lucky to be alive thanks to the quick thinking of his relatives and the rapid response and collaboration of police.

Des Gregor, 56, travelled to Mali, West Africa, on July 26, 2007, with the intention of meeting the woman he thought he would marry. Instead, Gregor became an unwitting target in a dangerous scam that could have had tragic consequences.

When Gregor arrived in Bamako, Mali, on July 27, he was greeted as planned by two African men who facilitated his arrival. After collecting his luggage, Gregor was led to another person who escorted him to a waiting vehicle.

However, rather than taking him to meet his would-be bride, the three men drove Gregor to a house where he was stripped of his clothes, threatened with a machete and held hostage for a $100,000 ransom. He was permitted to contact his family to request the ransom money under the guise that he was having credit card problems.

Immediately suspicious and concerned for his welfare, Gregor's family contacted the Australian Department of Foreign Affairs and Trade. Authorities with the Australian Federal Police (AFP), the South Australia Police (SAPOL) and the Canadian Embassy in Mali began liaising with the Mali National Police to investigate the situation and bring Gregor home safely.

The AFP's Adelaide office launched Operation Streambank, a joint police operation involving 50 AFP agents and 20 SAPOL officers. The team worked 24 hours a day for 12 days to intercept e-mails and phone calls to Gregor's family. Aviation staff from Adelaide Airport and AFP investigators from Australian Capital Territory Policing were also involved in the investigation.

The AFP dispatched its senior liaison officer based in South Africa to Mali, where the officer worked closely with the Canadian Embassy and local authorities to secure Gregor's release. The rescue involved convincing the kidnappers to allow Gregor to visit the Canadian Embassy in Bamako to pick up a lesser ransom sum (Australia does not have a diplomatic mission in Mali).

The kidnappers fell for the ruse. On August 8, Gregor's captors took him to the embassy, telling him that his girlfriend and two other people — all of them fictitious — would be killed if he did not return. Once at the embassy, Gregor was greeted by the AFP liaison officer and Canadian diplomats. He was told to remain in the embassy and that he was safe. A team of over 25 Mali Police officers from Bamako provided surveillance during the operation. The three hostage-takers were not caught.

Operation Streambank was a successful example of multi-agency co-operation between local state police, national police, and Malian and Canadian authorities through the AFP's international network.

The AFP wants this extreme example to serve as a warning to the public to protect themselves against similar types of Internet scams.

"Criminals are going online and using the Internet to target anyone they can, regardless of age or backgrounds, and people need to be aware that they could be putting their own lives at risk," said Tim Morris, AFP Assistant Commissioner International. "This was a lucky person. While it was a distressing ordeal for him at the time, he survived as a result of the AFP responding to this incident and working co-operatively at a multilateral level."

Federal agent Kevin Zuccato, director of the Australian High Tech Crime Centre, appeared on a national radio show to reinforce the message that scammers will continue to prey on people and trick them into sending money or gifts — or worse, lure them to another country.

"People like Des (Gregor) are seduced by the Internet where websites and conversations appear very realistic. You need to use the same common sense that you apply in the real world on the Internet," said Zuccato. ■

With files from Platypus magazine and the AFP.

Skimming scams

Preventing payment card fraud through education

By Cst Lloyd Schoepp
RCMP Commercial Crime Section
Calgary

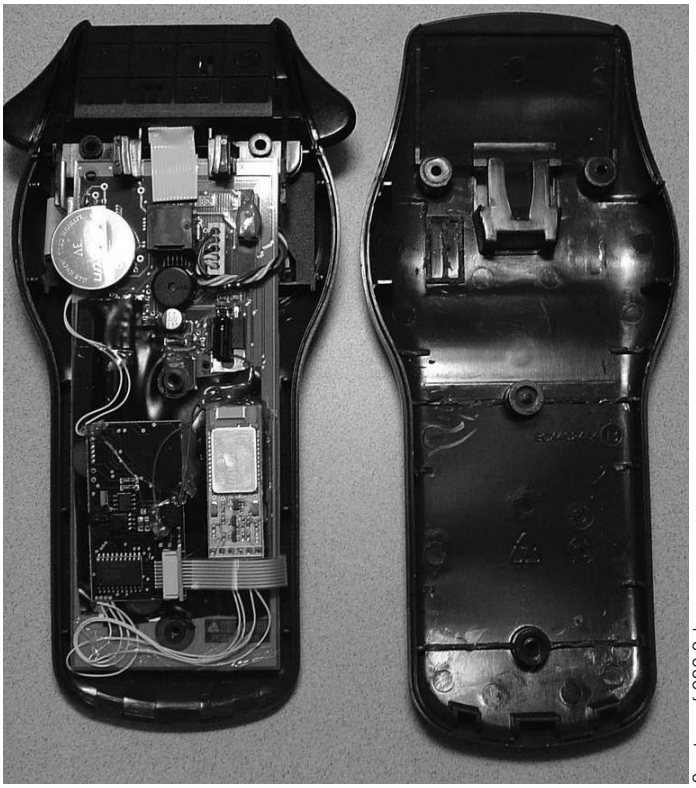
In the spring of 2006, the RCMP Commercial Crime Section (CCS) Calgary and the Calgary Police Service (CPS) Economic Crime Unit met to discuss the growing crime trend of debit and credit card skimming.

Skimming involves the unauthorized copying of electronic data from your payment card's magnetic stripe. Organized crime groups are behind a large portion of the skimming, which is growing at a rapid rate nationally (34 per cent increase in 2005–2006) and annually costs the Canadian economy millions of dollars in losses.

Skimming is not limited to a specific geographic area in Canada, which means an integrated approach is needed to effectively combat skimming at a local, national and international level. In addition to focusing on collaborative enforcement, CCS and CPS discussed the idea of developing an effective prevention program.

After reviewing various prevention programs across Canada, CPS and RCMP investigators focused on Project Protect. Project Protect is a collaborative crime prevention and education program involving law enforcement agencies, Interac Association, payment card partners and other industry partners. Police officers visit retail outlets to educate managers and employees about payment card fraud. The program provides training for front-line officers and equips merchants with valuable tips to prevent payment card fraud at their businesses.

The program was first launched in November 2005 by Peel Regional Police in partnership with eight southern Ontario law enforcement agencies, Interac Association, major credit card companies and participating gas retailers. The program was modelled after a similar program carried out in Quebec in 2002 by the Longueil Police Service. The original pilot focused on gas stations and resulted in significant decreases in skimming — as much as 60 per cent — at retail gas outlets.



Courtesy of CCS Calgary

This tampered pin pad was used in a skimming fraud.

In 2006, the CPS and the Alberta RCMP worked with Interac Association to launch the program in the greater Calgary and southern Alberta areas.

In preparation for the launch of Project Protect, CPS and RCMP members attended training sessions in Calgary and Lethbridge on skimming and Project Protect. In Calgary, the project was initially piloted in one CPS District and at six RCMP detachments, which included a mix of rural and urban detachments.

Police obtained copies of the brochures used by Interac Association in Ontario and modified them to meet the needs of the CPS and the Alberta RCMP

During the summer of 2007, the pilot program was reviewed to determine its successes, with the view of expanding the program throughout Alberta. Merchants' response to the pilot program was extremely positive, and they voiced their appreciation for the efforts of police officers who attended and educated merchants on card skimming. The project also proved successful when a merchant, following the procedures outlined in the project, discovered a tampered pin pad and alerted police.

In September 2007, meetings were held with Interac Association to determine the future focus of the program and locations were identified for continued rollout of the program.

In addition, CPS and RCMP members met with an Alberta-based financial institution to develop a pilot program where corporate-branded Project Protect pamphlets will be delivered to new merchants. This will create an additional distribution channel to assist with disseminating the prevention program.

While challenges remain — such as getting members in busy detachments to sign on and finding alternative delivery channels when resources are limited — members of the RCMP and CPS will continue to work with policing and industry partners to expand the program throughout Alberta and work to increase skimming prevention awareness. ■

Information on Project Protect can be obtained by visiting Interac Association at ***www.interac.ca***.

Nigerian advance fee fraud scams

By Olaolu Adegbite
Advance Fee Fraud Section
Economic and Financial Crimes Commission of Nigeria

Nigerian con men took the world by surprise in the late 1980s with the ingenuity, complexity and sheer scale of their advance fee fraud (AFF) scams. By 1991, a clearer picture emerged of the modus operandi of these sophisticated fraudsters who were taking in hundreds of millions of dollars per year. Their numbers increased at home as did their targets overseas. They reached their victims through regular mail, fax and land phones in every corner of the world.

By 2000, the problem had grown phenomenally, largely from the effective use of information technology. These white-collar criminals became even more bold and brazen due to weak enforcement in Nigeria. They lived in opulence and passed themselves off as benevolent philanthropists. Like the narcotics barons of South America and the mafia dons of Italy in the 1970s, they also became politicians.

The people of Nigeria paid a high price. All citizens were being painted as fraudsters by interests overseas. International business was scared away by Nigeria's dubious reputation, while direct foreign investment fell drastically. By the end of 2002, the intergovernmental Financial Action Task Force against money laundering listed Nigeria as a non-co-operative country. And Transparency International's Corruption Perceptions Index ranked the country among most corrupt nations in the world.

Fighting back

Establishing the Economic and Financial Crimes Commission (EFCC) of Nigeria in April 2003 changed the rules. Vigorous enforcement measures by way of arrest, prosecution, intelligence, prevention, public education, disruption and assets seizure led to a drastic reduction in the prevalence of AFF scams and other economic and financial crimes in Nigeria. The gains were immediately felt through sharp economic growth, improved national image, better political governance and renewed confidence among foreign investors.

The EFCC had made Nigeria less desirable for fraudsters. Many abandoned their illicit vocation, while a few professionals simply relocated to other less hostile environments.

The EFCC had made Nigeria less desirable for fraudsters. Many abandoned their illicit vocation, while a few professionals simply relocated to other less hostile environments where they continue to perpetrate their crimes of greed with less physical risk. The West African sub-region — especially Ghana, Togo, the Republic of Benin, Burkina Faso, Mali and Ivory Coast — has witnessed a drastic upsurge in AFF-related activities since 2004. The same is true in South Africa, the United Kingdom, Holland, Spain, the United Arab Emirates and Canada. It is futile to pretend that a few Nigerians are not involved in these overseas boiler rooms.

Contrary to suggestions by some theorists, we have not yet established any concrete links between Nigerian AFF networks and other international criminal groups such as Eastern European criminal groups, major narcotics syndicates, human trafficking groups or terrorist elements.

The EFCC has charged over 300 AFF-related cases to various Nigerian High Courts and not a single violent act was used by the suspects in any of the cases. There is also no conscious effort by the scammers to ally with any specific foreign criminal group. Their activities are fluid, anonymous and borderless. We have recorded cases where credit card

Police recovered these low-tech materials used to produce counterfeit identity documents in Nigeria.

Courtesy the EFCC

details have been obtained by Nigerian AFF scammers from Vietnamese hackers' sites as well as others from Romania, Russia and the United States.

We can hazard a guess at the future direction of AFF scams based on past experience, current intelligence and the latest trends:

- There will be a decrease in the number of AFF scammers. However, surviving ones will be more potent and effective.
- The current scam pitches, which appeal strongly to the victim's sense of greed (scams involving contracts, fund transfers, black money, inheritances, lotteries, precious stones and crude oil) will shift to emotional ones (scams involving pets, charities, religion and romance).
- Operational bases will most likely shift to Europe and North America to give prospective victims a false sense of security ('Nigeria' will not feature at any stage of the scam). Also, law enforcement in these jurisdictions focus mostly on violent crimes.
- There will be increasing participation of other nationals in AFF scams, especially citizens of countries that currently host boiler rooms.
- Perpetrators will increasingly take advantage of weak international law enforcement collaboration, legislation gaps in certain jurisdictions, bureaucratic bottlenecks with Mutual Legal Assistance Treaty requests, intelligence gaps, cumbersome extradition procedures, poor information sharing in the law enforcement community, strict disclosure laws and threshold requirements.
- There will be an increase in the usage of very small aperture terminal (VSAT) facilities, voice over Internet protocol (VoIP), and proxy servers by scammers to avoid detection.
- Targeted victims will grow larger in number and geographical spread as broadband Internet becomes more accessible, but the aggregate losses for these new users will be considerably lower than for victims in North America and Europe. The Asian, Middle Eastern and Australian regions will record more victims than North America on account of current preventive measures being taken by the United States and Canada.
- AFF scammers will acquire more knowledge and become more technologically sophisticated in carrying out major intrusion attacks to obtain account information on their own, instead of relying on other crackers and hackers.
- Spoofing and phishing attacks will increase with the recent introduction of e-payment systems in Nigeria and as scammers gain more experience.
- E-payment platforms will replace Western Union andMoneyGram as the major mode of receiving AFF proceeds.
- There will be a drastic upsurge in the use of postal and courier services in neighbouring West African countries — especially the Republic of Benin, Ghana and Togo — to export fake financial instruments and receive Internet scam packages.
- Large-scale manufacturing of counterfeit bank cheques, money orders, gift vouchers, travellers' cheques and other financial instruments used in AFF scams will increase in North America and Europe.
- The motive for AFF crimes will always be the money, and perpetrators will continue to keep their safe distance from violent crimes.

AFF scammers are intelligent and adaptive adversaries who will have little difficulty evolving and developing countermeasures to thwart enforcement initiatives. However, it is our view that a strong synergy between law enforcement agencies and industry — particularly providers of postal, courier, banking, money transfer, telecommunications and Internet services — is essential to designing and implementing strategic control measures to eradicate AFF scams, which are better prevented than detected. ■

Keeping advance fee fraud in check: the Canadian perspective

Over the past ten years, cities in Ontario, Quebec, British Columbia and Alberta have become bases for West African fraud activity in Canada. Here's how Canadian law enforcement is combating the problem:

- Enforcement: Six regional partnerships — including three co-located task forces — investigate, disrupt and dismantle mass marketing fraud operations in known fraud hot spots like Montreal, Toronto and Vancouver.
- Interdiction: An interception program stops cash and negotiable instruments associated with fraud in Canada. For example, in 2005, British Columbia's interception program seized approximately $1 million in cash and negotiable instruments and $118 million in counterfeit cheques, many of which would have been acted upon by victims.
- Disruption: A Montreal program pools police intelligence to identify suspected boiler rooms, then sends officers to visit the operations and question employees. Often, the police attention alone causes fraudsters to terminate, move or delay operations. Other times, officers employ search warrants or make arrests.
- Intelligence: An ongoing project will merge the two databases that house fraud-related complaints in Canada (the Canadian Anti-Fraud Call Centre database and the Reporting Economic Crime Online database), creating a single repository that supports global intelligence and information sharing.

Fighting against wine counterfeiters

Industry techniques empower consumers

Fraudulent products not only fund criminal organizations, they also diminish genuine manufacturers' credibility in the eyes of consumers who mistake counterfeits for the real thing. Wine manufacturers have been victimized by counterfeiters for years, but they are now fighting back, using a leading-edge product authentication process developed by the Swiss company Algoril. Algoril's sales director Olivier Gudet describes how the process targets counterfeiting from the ground level.

By Olivier Gudet
Sales Director, Algoril

The globalization of trade activity is good news for counterfeiters. As product manufacturers expand their geographic markets, many products are finding their way into the hands of groups that "specialize" in creating knock-offs. The challenge for manufacturers is to find easy and efficient tools to not only deter counterfeiters, but also detect fakes from the get-go.

Many solutions in the wine and other industries rely on invisible techniques — for instance using special paper or ink as is the case with banknotes. These techniques have become outmoded, costly and difficult to implement because they require the use of special scanners or detectors. Such latent solutions in no way reassure consumers, who often do not even know the measures exist.

The anti-counterfeiting solution being marketed by Algoril for the wine industry is simple and effective: for every bottle of wine produced, Algoril creates a unique ID code which essentially becomes the bottle's fingerprint.

Protecting authentic products

Each Algoril ID code is generated by combining information about a wine's unique characteristics — producer, appellation, vintage and serial number — with an encryption algorithm. The ID code is usually printed manually on the bottle's back label and the associated product information is stored in a highly secure database maintained by Algoril. It is possible to place a second code into a matrix that could be scanned or captured by a cell phone camera.

Consumers can then verify a product's authenticity by submitting a verification query via either the Algoril website or a cell phone text messaging service. Data contained in the Algoril database is compared with the information printed on the product, as submitted by the consumer. This cross-checking of information makes it possible to detect several types of fraud such as parallel market fraud or counterfeiting.

For producers, the coding technique supports "business as usual," since the coded labels are delivered ready for application. The cost is minimal, thanks to printing devices that can produce different sorts of labels without compromising print quality or output.

And consumers can access product information anytime from almost anywhere — which is a big plus compared to current anti-counterfeiting measures that

sometimes require waiting for the producer or a specialized device to confirm fraudulent activity.

Detecting knock-offs

You will know that your bottle is a fake if you submit a verification query and your bottle ID code is not registered or does not match product information in the Algoril database.

Another sure sign of fraud is if several verification queries are received for the same bottle, which usually means that a counterfeiter has "cloned" one or several codes. In cases such as these, it is possible to track exactly where the original bottle was purchased using traceability data provided by the manufacturer for each batch made available for sale. These data include information about the production of the wine as well as shipping details, such as country of destination, the importer, the exporter and finally the retailer.

By cross-checking the traceability data against the information in the original verification query, we can also identify parallel markets and determine if a given batch has been diverted from its original destination. If the information does not match, the system generates an alert and sends an e-mail to the producer. In such a case, the producer must control each link in the distribution chain to identify who is behind the diversion.

Consumer participation required

The success of Algoril's anti-counterfeiting measures will depend on the extent to which consumers are encouraged to use ID codes to obtain information. Initially, a customer in a wine retail outlet has the opportunity to make sure a product is authentic before making the purchase. Checking a code also provides consumers with a range of other useful information regarding the specific bottle of wine — for instance ideal temperature for serving, what food to serve it with, etc.

These consumer queries constitute the anti-counterfeiting system's advanced radar. There is no need for overly sophisticated means to identify knock-offs, since fraudulent activity is detected either directly or indirectly by the actions of consumers.

The extent of information provided for viewing depends on who is querying the system, since end buyers and industry authorities do not require the same details. For instance, information for the end consumer will focus on the "value" of the product whereas information for the *autorités sanitaires* will be oriented more on content composition and consumption date. Each requester, if identified, will receive information formatted for their own use.

Looking to the future

Most of the media hype surrounding counterfeiting operations is due to knock-off batches of well-known wines being sold at auction. Unfortunately, not much can be done about bottles that are already in circulation and do not have ID codes. To check the authenticity of such products, you must open the bottles to taste or test the wine, and that is problematic because doing so permanently spoils the wine. Even if you test just one bottle in a batch, there is no guarantee that the rest of the bottles are authentic.

Seals made with safe paper can be used to protect bottles against tampering, but this is still not a foolproof solution. In one case, counterfeiters made a hole in the bottom of a bottle, emptied the contents, refilled the bottle with another wine and filled the hole in with acrylic glue. To the naked eye, it was impossible to detect any form of tampering. Even if the bottle had been sealed, the seal would still be intact.

Nowadays, the only true deterrent is to ensure reliable traceability from start to finish. Upon detecting any form of fraudulent activity, Algoril will conduct an investigation to determine the exact stage of the logistics chain where the illicit intervention occurred.

Action has to be taken at the source — by producers. Consumers must then be encouraged to take advantage of the anti-counterfeiting measures made available to them in order to help put an end to counterfeiting activities. ■

...Continued from page 2

Fraud and the Factor of Fear / Warigon, Slemo D. Fraud Magazine Vol. 20, No. 5 (2006), pp. 28-31, 47, 58.

Fraud Investigations: A Case Study in Economic Evaluation / McFadden, Michael. Policing: An International Journal of Police Strategies and Management Vol. 25, No. 4 (2002), pp. 752-761.

Global Fraud: Investigating Suspected Fraud in the Middle East / Svenson, Torleif. Fraud Magazine Vol. 20, No. 5 (2006), pp. 24-27.

Illegal I.D.s / Poulos, Andrew. Law Enforcement Magazine Vol. 34, No. 4 (2007), pp. 104, 106-111.

Insidious Side Letters: Shady Business on the Side / Gober, Thomas D. Fraud Magazine Vol. 20, No. 4 (2006), pp. 25-27, 50.

Latest Debit Card Fraud Schemes: Part 1 - Security Breaches Allow Data Thefts / Holtfreter, Robert E. Fraud Magazine Vol. 20, No. 4 (2006), pp. 32-35, 52-53.

Latest Debit Card Fraud Schemes: Part 2 - Industry Initiatives, Technology and Global Legislation / Holtfreter, Robert E. Fraud Magazine Vol. 20, No. 5 (2006), pp. 42-43, 50-53.

Natural Catastrophe and Disaster Fraud: Calamity Criminals / Brody, Richard G. Fraud Magazine Vol. 20, No. 6 (2006), pp. 28-31, 51.

Pharmacy Fraud: A Clear Prescription Part 1 / Luby, Dwayne. Fraud Magazine Vol. 21, No. 3 (2007), pp. 24-27, 47.

Pension Fraud: Nabbing Bosses Who Crack Nest Eggs / Lautischer, Pierre E. Fraud Magazine Vol. 21, No. 1 (2007), pp. 32-35, 50-51.

What Asset Forfeiture Teaches us About Providing Restitution in Fraud Cases / Linn, Courtney J. Journal of Money Laundering Vol. 10, No. 3 (2007), pp. 215-276.

Websites

Association of Certified Fraud Examiners
http://www.acfe.org

Fraud and Scam Reference
http://www.nettrace.com.au/resource/reference/fraud.htm

e Investigator.com
http://www.einvestigator.com/links/insurance_fraud.htm

National Consumer League Fraud Information Center
http://www.fraud.org

The U.K.'s Serious Fraud Office and international co-operation

By David Jones
Head of Communications
Serious Fraud Office
United Kingdom (U.K.)

The U.K. Serious Fraud Office (SFO) is a prosecuting body with an investigative capability. It concentrates its resources on the biggest and most complex incidences of fraud. Because of this, it has a high profile and is constantly under the glare of media scrutiny.

As one of the Attorney General's departments, the SFO is a civilian body but one that works with the police on the majority of its cases. Local police forces contribute officers to particular investigations, adding their skills to the cases and assisting with arrests and searches.

Not all fraud cases come our way, or are accepted — only those that are big and complicated, and require legal, accounting and investigative skills to be brought together as a combined operation. We have 63 cases and these collectively represent in excess of £2 billion at risk. (Lesser frauds are dealt with by other parts of the U.K. criminal justice system, as are revenue and customs frauds.)

Before the office takes on a case, we assess whether the investigation should be handled by those responsible for the prosecution. We also consider whether the case is likely to attract national publicity, cause widespread public concern or require special powers to obtain information and documents under compulsion. If documents are not produced as required, or we suspect they might be tampered with, we can apply to a magistrate for a search warrant to secure them. Failure to comply with an order can result in a prosecution and prison sentence.

Investigators and prosecutors must work together from the earliest stages of the investigation right through to sentencing and confiscation proceedings.

Another important consideration is whether or not the case has a significant international dimension such as victims, evidence or assets in other countries that need to be traced. This might also determine if we need to gain co-operation from foreign investigation authorities to achieve our objectives in their jurisdictions.

Multidisciplinary investigations

The conduct of each case falls under the direction of the SFO. We appoint a case controller, who is an experienced prosecuting lawyer and is responsible for managing the case. He or she puts together an appropriate team to investigate the allegations based on the demands of the case and the resources available.

The team typically consists of accountants or financial investigators drawn from the SFO itself, supported by outside accountants or investigators brought in on a contractual basis and by police officers. Other key members include forensic computer specialists and information technology experts, who decipher, explore and recover computer material. Together with the police, they analyze financial information, including statutory accounts, management accounts and cash flows. They also supervise searches of offices and homes and, most important of all, trace the money. The team might involve former police fraud squad officers who join the SFO after retirement as civilian investigators. Most will have gained special financial expertise in their former occupations. We also consult with forensic accountants from external firms.

This range of specialists requires a team approach. Investigators and prosecutors must work together from the earliest stages of the investigation right through to sentencing and, now, to confiscation proceedings.

Fraud is often committed across a number of jurisdictions. Identifying which

jurisdiction should take the lead in investigating and prosecuting each case is not always obvious. Different rules regarding jurisdiction apply. By working closely together, we are able to disclose information to overseas prosecutors and investigators in the course of our investigations. Co-ordinated searches are vital, and we have had excellent co-operation with many other jurisdictions.

International co-operation

A very large proportion of our cases involve evidence abroad. To obtain such evidence, we need to make enquiries overseas, which can only be done by invoking the assistance of overseas judicial and police authorities. Likewise, when overseas administrations want to make enquires into frauds committed in their own jurisdictions where there is a U.K. angle — whether the evidence or even the defendant is situated within our jurisdiction — they need to invoke our help. This is done on a reciprocal basis through the Mutual Legal Assistance Treaties, and the SFO is able to provide expert investigative help to enable overseas partners to carry out these enquiries in the U.K.

Courtesy the U.K. SFO

Assistance to overseas authorities is provided predominantly by the SFO Mutual Legal Assistance Unit. It currently carries over 50 cases. These include some of the most important and sensitive international cases in the world, involving major political figures, organized crime and corruption on a huge scale. For example, the unit assisted the Government of Nigeria to trace millions of dollars that had been looted by Nigerian ex-president Sani Abacha and his family.

Mutual legal assistance of this kind is essential for swift and effective support to countries that have acute and chronic problems with corruption and Mafia-type organized crime. We have provided assistance to locations as diverse as Italy, Zambia, Costa Rica, Russia and Canada.

Under Section 2 of the U.K. Criminal Justice Act, compulsory orders are issued to obtain vital banking evidence and to demand answers to questions. Our investigators and lawyers work closely with their colleagues from the requesting countries. Some countries are relatively inexperienced in the law and practice of international mutual legal assistance, and we endeavour to provide them with the technical advice and guidance they need to formulate an official request.

Co-operation is two-way traffic. Without assistance from overseas authorities, many of our cases would flounder. Our investigators are "global travellers." At both the official and more informal working levels, obtaining cross-border assistance is a crucial element of our investigative processes. Recently, for example, we conducted a series of raids on a number of premises in Spain with the full co-operation and participation of the Spanish police.

Canadian connection

In 1997, an angry Canadian citizen caught up in an advance fee fraud scheme (operated by a sham business loan service in England) travelled to the U.K. to report his complaint. He had placed an advertisement in the Globe and Mail newspaper asking if other Canadians had received unsatisfactory dealings with the bogus loans operation. More than 100 people responded. He brought the evidence with him to England to discuss the matter with police, kick-starting an SFO investigation that also involved two British police forces — one in Brighton and the other in Durham. We subsequently identified a number of people in Canada, the United States, Australia and New Zealand who had been similarly affected.

Following an official request, the RCMP provided support throughout our Canadian strand of this case. When we sent our people to gather evidence from victims, one of our investigators — Ian Wilson, a former Durham police officer — recalls that he had barely set foot in his Toronto hotel when an RCMP officer whisked him away for a briefing. By all accounts, after a few hours, a good collaborative relationship had been cemented. The case outcome proved the power of such co-operation: the fraudsters ended up in jail.

At the SFO we have to be pragmatic about what is achievable. Major frauds are invariably complex and difficult to investigate and, where they are international, they pose extra challenges for investigators. After nearly 20 years of operation, we have gained much experience in working with fellow fraud fighters in other jurisdictions. Catching international criminals requires international co-operation. We must all exercise and overhaul our procedures to ensure that co-operation is not only given, but given swiftly. ■

Just the facts

The high school years are supposed to be the best years of a young person's life, but violent incidents on school grounds threaten to compromise those years — or even cut them short. Assaults, rapes, hazings and other violent incidents are an unfortunate reality for many high school students. Here's a look at the facts.

In the United States (U.S.), 22 of every 1,000 students aged 12 to 18 were victims of violent crimes during the 2004 school year — including 4 victims of serious violent crimes such as rape, sexual assault, robbery and aggravated assault.

Seventy-four per cent of all assaults that injured Canadian students on school grounds in 2004 involved physical force, nine per cent involved weapons like whips or vehicles, and two per cent involved clubs or blunt instruments.

Secondary schools in France reported 14,780 incidents to police in 2001-2002: 34 per cent involved physical violence without weapons, 3 per cent involved knives and less than one per cent involved firearms.

In 2005, six per cent of U.S. students in Grades 8 through 12 reported that they had carried a weapon on school property during the previous 30 days.

In 71 secondary school shooting incidents recorded by wikipedia.org since 1995, 137 people were killed and 232 were injured. The average shooter was a 16-year-old male.

Two per cent of U.S. public schools required either students or visitors to pass through metal detectors during the 2003-2004 school year.

An Australian Government study found that violent incidents are most likely to occur in schools where more than 25 per cent of the teachers have less than five years experience.

Seventy-two per cent of respondents to a Phi Delta Kappa survey on public attitudes towards schools identified the growth of youth gangs as a very important cause of violence in schools, second only to the use of alcohol and drugs.

In 2003, eight per cent of Canadian sexual assault victims between the ages of 14 and 17 were assaulted at school.

According to one American study, over 50 per cent of high school boys and 42 per cent of high school girls believe that there are times when it is "acceptable for a male to hold a female down and physically force her to engage in intercourse."

Twenty-two per cent of high school students surveyed by Alfred University in 2000 were subjected to dangerous hazing activities — including being physically abused, beaten, branded, tied up, forced to harm others or forced to harm themselves.

Nearly three-quarters of hazing victims will suffer at least one negative consequence such as getting into a fight, hurting someone else, committing a crime or considering suicide.

SOURCES: *U.S. Department of Justice, Indicators of School Crime and Safety, 2003 :* **http://www.ojp.usdoj.gov/bjs/abstract/iscs06.htm**; *Journal of Educational Administration, Vol. 41, No. 6 :* **http://www.emeraldinsight.com/info/journals/jea/jea.jsp**; *Statistics Canada, Children and Youth as Victims of Violent Crime :* **http://www.statcan.ca**; *Wikipedia :* **www.wikipedia.org**; *New South Wales Bureau of Crime Statistics and Research, School violence and its antecedents: interviews with high school students :* **http://www.lawlink.nsw.gov.au**; *University of Arizona, College of Education :* **http://www.drugstats.org**; *North Carolina Coalition Against Sexual Assault :* **http://www.nccasa.org/teen/GetTheFacts.html**; *Alfred University :* **http://www.alfred.edu/hs_hazing**

"Auto Theft Capital" no more

Targeting prolific offenders in Surrey, B.C.

By Carly Paice
Communicatons and media relations
Surrey RCMP

Until recently, Surrey, British Columbia, was known as the "Auto Theft Capital" of North America — a label that was quick to catch on but slow to fade. In 2003 alone, 8,105 vehicles were reported stolen, a 120 per cent increase from four years earlier, giving Surrey one of the highest per capita auto theft rates in Canada.

Among other factors, the emergence and increased usage of "crystal meth" was partly to blame for this sharp increase. Most vehicles were recovered, with over 90 per cent eventually turning up. But of concern to police was the time period in between the theft and the recovery. This time frame generally allowed for a combination of other crimes to be committed by the auto thieves: robberies, drug dealing, break and enters, and dangerous driving often resulting in fatal collisions or serious injuries.

In spring 2004, Surrey RCMP embarked on a new crime-reduction initiative focusing on reducing auto theft and property crime through the identification and targeting of prolific offenders. Two target teams — the Auto Crime Target Team and the Property Crime Target Team — were created to direct efforts toward the small percentage of offenders accounting for a disproportionately large number of crimes.

By implementing the Target Teams, developing key partnerships and strengthening the Crime Analysis Unit, auto theft decreased in Surrey by 38 per cent from 2003 to 2006.

Strategies

Part of the new approach involved building and expanding on key partnerships. This meant police worked more closely with the Correctional Service of Canada, provincial corrections and probation services, the Integrated Municipal Provincial Auto Crime Team (IMPACT) and the Surrey Crime Prevention Society.

In consultation with Crown counsel, police prepared a template incorporating the elements required for a bail hearing. In addition, all requests for information from Crown counsel were received in a timely fashion and were immediately taken on by a Target Team member.

Technology also played an important role in the installation and use of tracking devices in stolen vehicles. With members of the Target Teams trained in how to use the equipment, they made a number of high-profile arrests directly as a result of the devices. The teams also developed a more co-ordinated approach to checking the vehicles for fingerprints by immediately following up on any incidences of multiple hits by an offender.

Crime analysis

As part of the ongoing strategy to combat auto theft, the Surrey RCMP's Crime Analysis Unit was expanded in 2005 to a strength of five. The mapping analyst, responsible for identifying "hot spots," crime trends and predictive analyses, played a key role in identifying where vehicles were being stolen and dumped. This helped to guide operations and ensure strategic deployment of resources.

For example, in fall 2006, the mapping analyst identified a trend where several stolen vehicles of the same make were being dumped and recovered by police in a small area of the city. The Target Teams were concentrating their efforts in this hot spot when they noticed a shirtless man with a large tattoo on his back that read "Grand Theft Auto" walking in the area. Members of the Target Teams observed the man steal a car of the same make identified in the trend by the analyst. The 27-year-old man was arrested, charged and remanded to custody. He pleaded guilty and received a 26-month jail sentence.

Courtesy of Surrey RCMP

Surrey's Auto Crime Target Team hit the target with this suspect sporting a Grand Theft Auto tattoo on his back. The suspect pleaded guilty and received a 26-month jail sentence.

Results

By implementing the Target Teams, developing key partnerships and strengthening the Crime Analysis Unit, auto theft decreased in Surrey by 38 per cent from 2003 to 2006. Furthermore, out of the 737 arrest and surveillance operations from April 2004 to December 2006, 100 per cent of charges recommended to the Crown were approved, with an 87 per cent remand success rate (95 per cent of the cases resulted in guilty pleas).

Members of the Auto Crime and Property Crime Target Teams were proud to accept the 2007 International Vehicle Theft Award of Merit, presented by the International Association of Chiefs of Police in New Orleans, Louisiana, on October 16, 2007. ■

NEW ZEALAND'S WIKI POLICING ACT

Public has a say in shaping legislation

By Supt Hamish McCardle
Police Act Review
New Zealand Police

In March 2006, the New Zealand government agreed to a comprehensive review of the legislative arrangements for policing in New Zealand, leading to a rewrite of the 1958 Police Act and its accompanying set of regulations. As the organization most directly affected by the existing legislation, and with unique insights into its strengths and weaknesses, the New Zealand Police was given responsibility for leading the review.

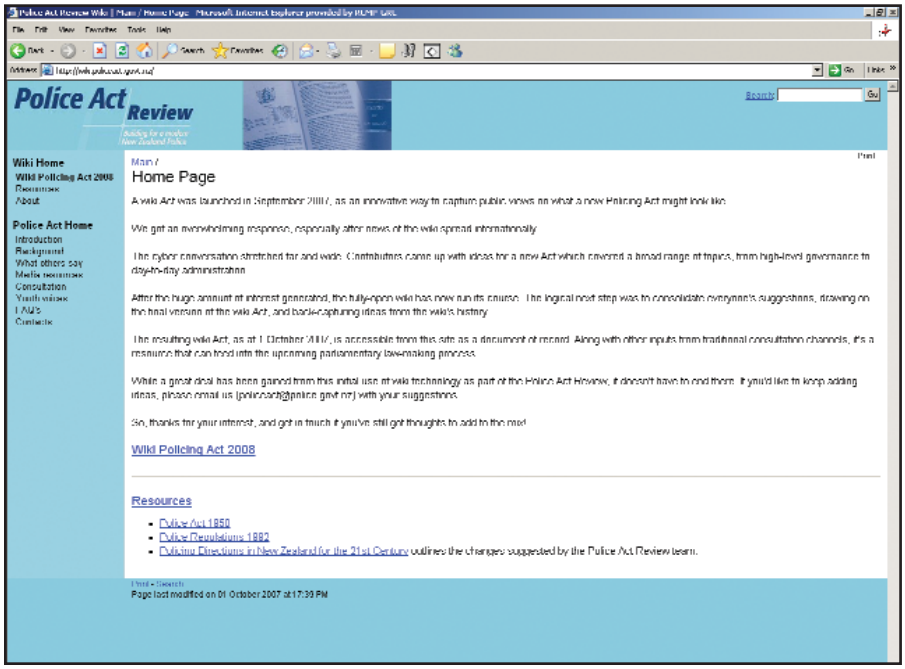
The Police Act Review had a broad-ranging mandate, signalling a desire for a national conversation with New Zealanders about policing. The review team had a green light to go back to first principles, to challenge things taken for granted, and to encourage public debate.

The review team decided to adopt both traditional and innovative communication and consultation methods so as many voices as possible could be drawn in to the review process. As such, online and electronic engagement have been important features.

The shape of future legislation

To allow New Zealanders to have a say in shaping future police legislation, the Police Act Review featured three phases of public consultation. The first two phases involved respondents making submissions on a series of discussion documents. Simple online forms were developed to allow respondents to directly answer the questions posed in the documents electronically or via more conventional methods. In both phases, the majority of respondents selected electronic formats to make their submissions.

Developing a wiki format to consult on ideas for a new Policing Act was seen as a natural next step for capturing views from not only citizens in New Zealand, but also expatriate New Zealanders and other international citizens interested in policing and law making. While the review team judged previous uses of online consultations as relatively successful, the team felt that a wiki discussion would allow for ideas to be stretched in new and inventive ways. The team preferred an open wiki with no password or registration because of its ability to generate dynamic, user-created content.



To make the moderation process manageable, the wiki was only open for editing during New Zealand office hours. After hours, interested people could view the wiki Act and prepare their comments offline, ready to post at the next opportunity.

The review team initially populated the wiki Act with a few ideas to fast-start the process and provide contributors with a framework. However, contributors were quick to begin making changes to the wiki by adding in new sections or clarifying what they wished to see in a new law. It became clear that many participants also wished to discuss the material they were adding to the wiki or comment on that of other contributors. Facilitating this discussion is an important aspect of using wiki technology, so the review team added separate notes pages to each section of the wiki to allow this discussion to take place away from the main pages.

The wiki Act received nearly 26,000 visits, with the vast majority of hits coming as referrals from embedded links in online news stories. Given that most people were visiting the site from a media referral, the distribution of visitors to the wiki seemed to follow media pick-up of the story, and interest in the wiki Act was international, particularly following the BBC publishing an article about the wiki on its main web page.

Foreign language articles about the wiki Act also appeared in mainstream media in numerous countries: Germany, Norway, Spain, Hungary, the Czech Republic, Thailand, Italy, Finland, Poland,

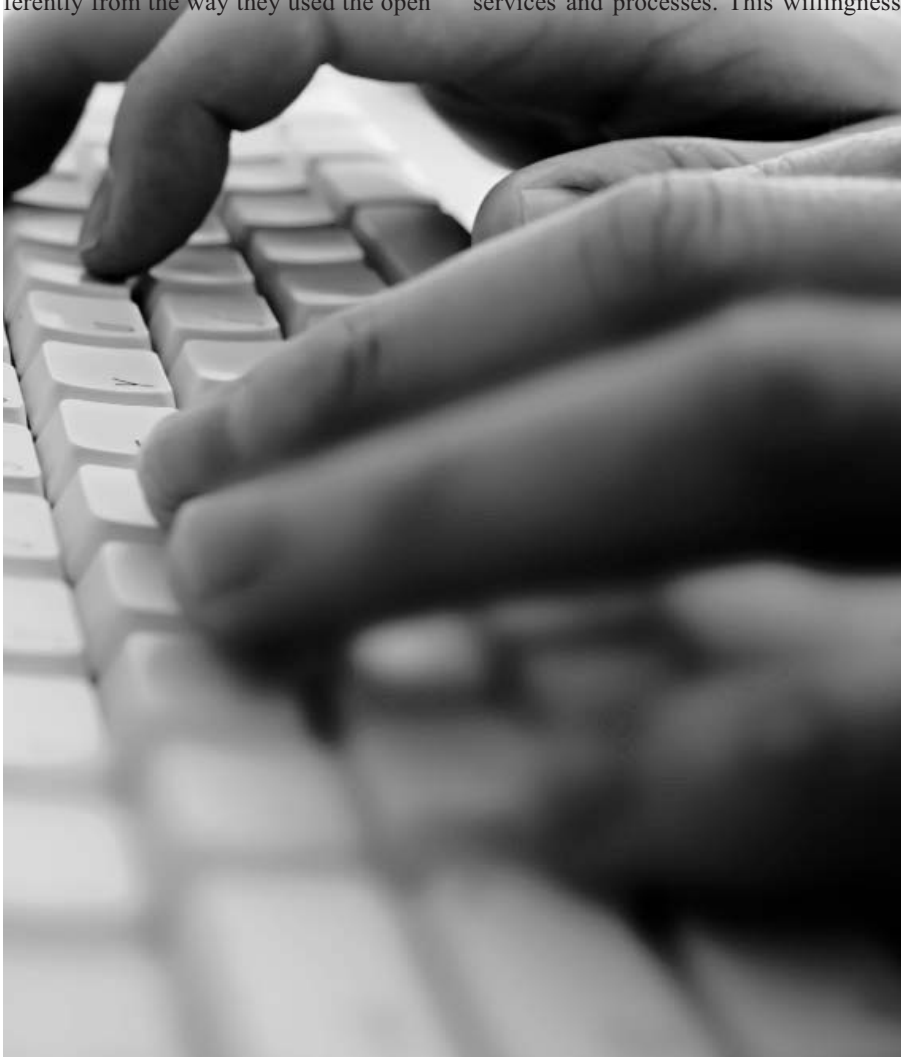
Malaysia, Chile and France. A large online community, Slashdot.org, publicized the story following the BBC article and hits from American IP addresses rose rapidly (by over 7,000 per cent) immediately after the Slashdot referral.

The open wiki was closed on September 30, 2007, with the resulting conversation being moderated and edited before reopening as a document of record on October 1, 2007. The site ***http://wiki.policeact.govt.nz*** is still receiving a large number of hits per day, with visitors viewing an average of almost four pages per visit. Individuals are also invited to directly contact the team with any further comments, and we are still receiving feedback in this way.

Current statistics indicate visitors are using the document-of-record wiki differently from the way they used the open wiki. Visitors are now spending more time on the site and are viewing more pages while they are there. The proportion of visitors accessing the site directly, without a referral from a media site, has also increased.

As a result of the international coverage, members of the Police Act Review team have been approached for further information about the wiki from a variety of international observers and researchers. Many have asked questions about the lessons other law enforcement agencies could learn from the New Zealand experience.

The Police Act Review has been fortunate that the use of the wiki was in line with New Zealand's e-government goal that information and communications technologies should be integral to the delivery of government information, services and processes. This willingness to support new technologies was of great benefit in initiating such a novel consultation strategy and was, arguably, vital to the success of the wiki.



What is a wiki?

Based on the Hawaiian-language word *wiki wiki*, which means quick, a wiki is a collection of websites or other online resources that allows visitors to quickly add, delete or edit content collectively. It is the ease of interaction and the speed of operation that make a wiki an effective tool for mass collaborative authoring. Although vulnerable to abuse and vandalism, wikis are self-correcting because of their number of users.

Initially some questions were raised about using a wiki in the law-making process, as this had not previously been attempted in New Zealand or any other country. However, these concerns were alleviated by clarifying the role that the finalized wiki would play in subsequent policy development work. Other challenges around the wiki were more practical — the moderation of posts (as noted above), managing mischievous edits and contributors, general maintenance of the site and so on.

Positive outcomes

Overall, the wiki Act produced hundreds of constructive edits, ranging from single-word suggestions through to lengthy paragraphs of commentary about a wide variety of topics. It has yielded at least three positive outcomes: firstly, a number of fresh ideas were raised; secondly, awareness of the review and engagement in it were significantly increased; and thirdly, while not a direct objective of the Police Act Review, a deeper conversation has developed around government use of web-based technologies and online social networking spaces.

Given the success of the open wiki, a second-generation wiki has been developed. This password-protected site allows participation in a wiki community to further develop the first generation Wiki Policing Act 2008. ■

Internet child exploitation investigations

Coping with emotional challenges

By Carolyn Burns

Internet Child Exploitation (ICE) teams around the world not only investigate the rape and torture of innocent children, they often must watch it happen. As one investigator said, "it's like standing in front of a window watching it happen and there is nothing you can do to stop it."

As part of ongoing criminal investigations, members of ICE teams are required to view graphic images depicting the sexual abuse and torture of children in an effort to identify victims and suspects and obtain evidence for eventual prosecution. The content can range from still photographs of young children to explicit video with sound of very young infants being tortured and raped. The amount of time spent viewing these images varies; however, it is a substantial component of the investigation and can have a significantly negative impact on investigators.

In order to understand the impact ICE investigations can have on individuals, a study was conducted with the help of the RCMP ICE team in British Columbia to explore what helps and hinders coping with ICE work. The results, taken from the experiences of ICE investigators, identified some unique and important findings relating to the impact of the work and suggested personal strategies that team members can employ to help them cope more effectively.

Impact of work

Investigators' personal experiences, coping strategies and the graphic nature of the material they are exposed to all affect the degree to which they are impacted by ICE work. It is common for investigators to feel overwhelmed by the sheer volume of investigations and the level of depravity and harm perpetrated against children and infants. Society, the criminal justice system and policing organizations lack a complete understanding of child exploitation, which frequently creates barriers to investigations and leads to intense frustration. In addition, despite the value and necessity of the work, the level of discomfort about the topic of child exploitation in general has made it extremely difficult for team members to share their work and concerns with others, leading to feelings of isolation and stigma.

The physical and emotional reactions to ICE work described by several team members include frequent headaches, fluctuating moods and extreme fatigue, which often prevents them from engaging in their normal outside activities and leaves some feeling like they were not able to fulfil their responsibilities to family and friends.

Those exposed to particularly graphic and traumatic images often experience nightmares, flashbacks, intrusive images, difficulty sleeping and problems concentrating. Compounding the problem, the sheer horror of the images they witnessed prevents team members from discussing or debriefing with others outside of the team, depriving them of a valuable and necessary outlet.

Many found that this work made them far more protective of children. Several described constantly being on guard when they were out, continually watching the behaviour of people around children. Others described having an overwhelming need to teach every parent and child about Internet safety and the inherent dangers of using the Net. Some who were parents also found they were far more restrictive of what their children were allowed to do because of the horrifying knowledge they carry.

Over the three years that this ICE team has been in existence, its members have gained knowledge about what helps and hinders coping with the work and have developed a number of strategies. The strategies outlined below are some of the techniques used by team members to cope with the difficult images and material they are exposed to on a regular basis.

Viewing strategies

A gradual introduction to the images was found to be helpful to those new to the unit. Those who experienced a gradual introduction reported that it helped them prepare for increasingly difficult materials.

The opportunity to prepare mentally before viewing the images helped ICE team members cope with what they were about to see. Several described the importance of getting into the right "head space," where they could prepare for seeing the worst images imaginable.

Another helpful viewing strategy described by team members was to make a deliberate choice to change how they perceived the images. Some said it helped to pretend they were not real children being victimized; others found they were able to shut down their emotions, which helped them to view more objectively. Not looking the victim in the eyes or making connections between the child victim and another child they knew was also very important.

Several found that being aware of how they were reacting while viewing was critical. Taking a break, going for a run, and talking to others were all described as helpful strategies to assist when they began viewing from an emotional perspective.

Regardless of the difficulty of the content being viewed, remaining analytical and focusing on the evidence within the images was key. By working systematically to gather the investigative information required from the images, individuals were able to remain more objective.

Participants also talked about specific factors that influenced their ability to cope with viewing, including viewing in the morning (to allow several hours for the images to fade before leaving for home and family), limiting the amount of viewing done each day, mixing viewing with other investigative tasks, and not viewing when tired or emotional. Having a private environment, team members to touch base with, and the ability to take breaks and talk to others when viewing particularly horrific images was also helpful.

Personal strategies

In addition to specific approaches used when viewing, team members described a number of personal strategies that helped them to cope with the work.

- Engaging in hobbies that distract the mind
- Regular, often intense, exercise
- Grounding activities such as yoga, taking walks, listening to music
- Putting a limit on viewing each day
- Leaving work at work at the end of the day
- Setting personal boundaries and knowing when it is time to transfer out of the unit and move on to other work
- Being aware of personal limitations

ICE team members can become overwhelmed and develop unrealistic expectations of themselves as they know there are so many child victims who continue to be harmed. Team members must learn that they cannot carry the responsibility for all of those children alone. In order to remain healthy, they must realize they can only do their part, and then give themselves permission to leave the work behind at the end of their day.

Support of supervisors

One of the most significant factors mentioned by team members was having supervisors who understood the impact of ICE work. Such supervisors automatically supported team members in doing what they needed to remain healthy. Having the support to step away, limit viewing, go for a run, or seek out others to laugh or talk to during particularly difficult moments was identified by all as critical to their well-being.

Given the nature of the work and the inability to talk about the images they see to prevent traumatizing others, a great deal of importance is placed on team. Team members described the importance of having a solid team of individuals who work well together and can support one another. Selecting the right individuals in relation to suitability, emotional stability and capacity to handle ICE work was identified as key to the healthy functioning of the entire team.

To better support ICE teams as they conduct these often complex and difficult investigations, it is important that the appropriate information, tools, and resources are made available to them. ■

Carolyn Burns, M.A., has worked in the field of victim services since 1989 and is a Registered Clinical Counsellor.

Have you been "ID'ed" yet?

ICE team members in British Columbia now have access to a support program that helps them understand and cope with the emotional aspects of their work.

The Inoculation/Defusing (ID) program, developed by the RCMP Behavioural Sciences group in B.C., is a voluntary and confidential course available to every new ICE team member, with followup sessions every six months thereafter.

"Group members are shown some short video clips of child exploitation images," says Teal Maedel, one of the psychologists who developed the program. "The group members discuss their thoughts, feelings and the most 'gut-wrenching' part or part they would most like to erase in viewing the images.

"The group then shares what coping strategies have worked for them, and the facilitators (trained psychologists) contribute to this discussion if necessary." The session closes with each participant sharing "something valuable about the work that they do."

The sessions also include an educational component, where external psychologists speak about subjects like sexuality, family dynamics, cognitive denial and other coping strategies.

Feedback from B.C. ICE teams has been positive. The Behavioural Sciences group now offers the program to other police departments.

—Caroline Ross

Latest research in law enforcement

The following are excerpts from recent research related to justice and law enforcement. To access the full reports, please visit the website links at the bottom of each summary.

Guidelines on cell phone forensics

By Wayne Jansen and Rick Ayers
National Institute of Standards and Technology (U.S.)

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. When a cell phone is encountered during an investigation, many questions arise: What should be done about maintaining power? How should the phone be handled? How should valuable or potentially relevant data contained on the device be examined?

This guide provides basic information on the preservation, acquisition, examination, analysis, and reporting of digital evidence on cell phones, relevant to law enforcement, incident response, and other types of investigations. The guide focuses mainly on the characteristics of cell phones, including smart phones having advanced capabilities. It also covers provisions to be taken into consideration during the course of an incident investigation.

The objective of the guide is twofold: to help organizations evolve appropriate policies and procedures for dealing with cell phones, and to prepare forensic specialists to contend with new circumstances involving cell phones, when they arise. Organizations should use this guide as a starting point for developing a forensic capability in conjunction with extensive guidance provided by legal advisors, officials and management.

Digital evidence by its very nature is extremely fragile, especially that found on cell phones. A phone's contents and the evidence it contains can be affected or lost any time it is on.

The situation with forensic software tools for cell phones is considerably different from personal computers. While personal computers are designed as general-purpose systems, cell phones are designed more as special-purpose appliances that perform a set of predefined tasks. Cellular phone manufacturers also tend to rely on assorted proprietary operating systems rather than the more standardized approach found in personal computers.

Digital evidence by its very nature is extremely fragile, especially that found on cell phones. A phone's contents and the evidence it contains can be affected or even lost any time it is on. It may not be obvious when an investigation is initiated that court action may ensue. Important evidence might be overlooked, improperly handled or accidentally destroyed before the seriousness of the incident is realized.

Whatever the type of incident, the various types of roles involved are similar. They include first responders, investigators, technicians, forensic examiners, forensic analysts and evidence custodians. Forensic professionals, especially first responders to incidents, should understand their roles and responsibilities for cell phone forensics and receive training and education on related forensic tools, policies, guidelines and procedures.

To access the full report (publication date May 2007), please visit :
http://csrc.nist.gov/publications/PubsSPs.html

Police and augmented reality technology

By Thomas J. Cowper and Michael E. Buerger

One of the 21st century's emerging and potentially powerful technologies is augmented reality (AR). Sports fans view one popular use of AR technology each weekend: the major networks augment their coverage of professional football by superimposing yellow "first-down" lines over the gridiron. While not interactive, this is AR in its simplest form. Another easily recognizable form of AR technology is the heads-up display (HUD) used by fighter pilots.

Unlike virtual reality, where the user is totally immersed in a computer-generated virtual world, and augmented virtuality, where real-world objects are included as part of a virtual simulation, AR combines real and virtual objects and displays them in real time to an individual operating in the real environment in a way that is beneficial to accomplishing specific tasks or missions. Situational awareness is greatly improved, theoretically allowing one person equipped with AR technology to do the same amount of work as three unequipped individuals.

It will also afford criminals and ter-

Augmented Reality technology will have a dramatic impact on policing, creating innovative methods for combating crime and terrorism.

rorists new opportunities for exploiting, disrupting and harming society. In order to be used effectively, police personnel need to fully understand current AR capabilities and what will emerge in the coming decades.

The purpose of this research paper is to provide the policing profession an introductory source document and overview of AR. Fundamental principles and components of the technology are examined, along with research developments occurring today that have the potential to directly enhance individual human performance through the augmentation of reality. The implications of AR and some potential applications for its future use as a law enforcement tool are offered.

Some possible AR applications for policing include the following:

- Facial, voice-print and other biometric recognition data of known criminals to allow instantaneous identification
- Integration of chemical, biological and explosive sensors to immediately notify officers of any local contamination and recommend appropriate protective measures for themselves and the public
- Patrol car operator data and regional traffic management information on a heads-up display to make driving safer and more efficient, especially in pursuit and rapid response situations
- Advanced optics to provide zoom, thermal and infrared imaging for the location and apprehension of fleeing criminals, buried or concealed disaster survivors, or missing persons
- Advanced optics to allow investigators to lip-read from great distances in situations where listening devices are impractical
- Realistic training scenarios to simulate dangerous police environments while blending real-world equipment and fellow trainees into the scenario
- Supervision of critical incident response to include the monitoring of the physiological status of all personnel, permitting the assignment of dangerous tasks to those who are mentally and physically best able to perform

To access the full report (listed under the "law enforcement services" section), please visit :
http://www.fbi.gov/publications.htm

National study on neck restraints in policing

By the Canadian Police Research Centre

Within Canada (and North America generally) there continues to be an increasing number of events in which police officers encounter subjects who are not responsive to standard law enforcement compliance control techniques. Typically, these subjects are under the influence of central nervous system stimulants or hallucinogens, which presents a challenging restraint and control problem for responding police officers.

Even considering the advancement of less lethal technologies such as the conducted energy device (TASER®) and other devices such as impact projectiles, it is clear that in many occasions officers are required to know and utilize effective empty-hand physical techniques to garner subject control. A vascular neck restraint (VNR) is an empty-hand control technique which does not rely upon the subject's ability to feel and respond to pain stimulus to be effective.

Many Canadian police agencies have a vascular neck restraint control technique within the use-of-force framework. However, vascular neck restraints, like many other forms of police restraint, have been subject to intense public and media scrutiny. Controversy surrounding the use of neck holds in general has resulted in dramatic variance amongst police agencies with respect to policy, course training standards and lesson plans pertaining to the neck restraint.

A review of the legal history of the neck restraint in policing as well as previous medical literature shows that there is little agreement among professionals as to the risk of the neck restraint technique, the type of neck restraint that is "safest" and the threshold at which an officer can legally apply the technique.

As a result of these inconsistencies, the Canadian Police Research Centre (CPRC) was tasked with facilitating a review of the current research pertaining to neck restraints in the policing environment and thus the National Study on Neck Restraints in Policing was commissioned.

The intent of this review is to provide a multidisciplinary report evaluating police use of neck restraint, with specific attention to vascular neck restraint. Ultimately, the final report on neck restraints in policing provides a framework around which administrators can make informed decisions regarding the following:

- Evaluation of the current level of risk associated with police officers utilizing VNR
- Authorization of the use of VNR
- Development of policy on the use of VNR, including its position on the use-of-force continuum
- Draft training, certification and requalification policy
- Development of course training standards, plans and manuals
- Development of ongoing risk management strategies (data collection and analysis)

To access the full report (TR-03-2007), please visit :
http://www.cprc.org/index.cfm?sector=static&page=library

Cross-border policing and the "shiprider" program

By Brad Kieserman
Chief, Operations Law Group
United States Coast Guard
Headquarters

During August and September 2007, 50 RCMP and United States Coast Guard (USCG) officers operating in support of existing International Border Enforcement Teams (IBETs) conducted a pilot project that may change the course of traditional policing along the shared maritime boundary between Canada and the United States.

For two months, in two locations, these officers became "shipriders" — riding together on the same patrol boats and fully empowered by the laws of both Canada and the United States to enforce the laws of both countries.

Boarding over 187 vessels, these officers seized 214 pounds of marijuana, over 1 million contraband cigarettes, six vessels and $38,000 Cdn intended to fund smuggling activities. They also conducted several search-and-rescue missions and collected intelligence for shore-based investigators on both sides of the border. Viewed by most participants in the operation as a successful and rewarding policing operation, the future of shiprider looks bright.

Why shiprider?

The links between place, crime, control measures and national identity are becoming more complicated, especially at the border. To a greater extent than ever before, crime and control measures are not always linked to a common national territory. Instead, criminals often exploit international borders, turning the seams between sovereigns into operational barriers for police. Shiprider was designed to remove the international maritime boundary as a barrier to policing and to deny smugglers and other criminals the illicit use of shared waters.

How does it work?

For the proof of concept, about 25 officers from each country participated in nearly two weeks of joint training during July 2007 at the USCG Maritime Law Enforcement Academy in Charleston, South Carolina. Using a special curriculum jointly developed by the RCMP, the USCG and U.S. Immigration and Customs Enforcement (ICE), the officers attended lectures and conducted numerous practical exercises to explore and compare their respective authorities, tactics, techniques and procedures.

Working and living together on the campus in the same binational teams as they would use to operate on the water, the officers built trust and partnerships in preparation for combined operations. Upon graduation, each officer was cross-designated as a law enforcement officer for the other country — RCMP members were cross-designated as U.S. officers of the customs and USCG officers were cross-designated as supernumerary constables of the RCMP.

Following joint training the officers reported to one of two IBET locations: Blaine, Washington–Vancouver, British Columbia, or Cornwall, Ontario–Massena, New York. Once they arrived in their operating areas and conducted area familiarization on the water, the officers began daily patrols on RCMP and USCG vessels.

Officers of both services crewed each vessel together so that operations in Canada were conducted under the direct supervision of an RCMP officer and operations in the United States were conducted under the direct supervision of a USCG officer. When operating in Canadian waters, the USCG shipriders assisted their RCMP partners in the enforcement of Canadian laws, and vice versa. Through this mechanism, the RCMP and USCG removed the international maritime boundary as a barrier to policing and created a force multiplier: for the cost of one vessel, the teams were able to effectively police the boundary waters of two countries.

Courtesy of the U.S. Coast Guard

The shiprider land and maritime teams seized more than 200 pounds of marijuana on September 26, 2007.

How did it begin?

While protecting the Canada–U.S. border from criminality has always been a major focus for law enforcement and public safety agencies on both sides of border, border integrity took on an even greater focus in the wake of the September 2001 terrorist attacks and law enforcement partnerships between the two countries began to evolve rapidly. By early 2002, RCMP and USCG officers were putting their heads together to develop innovative and effective models to ensure the (4,800-km) 3,000-mile Canada–U.S. maritime border stayed open for business, but closed to crime.

In 2003, the RCMP's then-Chief Superintendent (now Assistant Commissioner) Mike McDonell and I came up with the idea of taking IBETs to the next level in the maritime domain. In addition to developing and sharing law enforcement intelligence, we proposed to undertake joint intelligence-led patrol operations along the waters of the shared border.

By September 2005, the RCMP and USCG secured approval for a two-week proof of concept in the Windsor–Detroit

area. The proof of concept generated an evaluation that articulated the potential benefits of the program, but urged more training and a longer test period. The agencies "floated" the program again as a special maritime security measure during Super Bowl XL in February 2006.

After considerable study, staffing and review, RCMP Assistant Commissioner Raf Souccar and USCG Vice Admiral Brian Peterman proposed to ministers and cabinet officers at the Cross-Border Crime Forum in November 2006 that the concept be given a full pilot project. After considerable legal and policy work by the relevant agencies in both countries, the governments of Canada and the United States agreed to give it a go in June 2007. RCMP Superintendents Blair McKnight and Joe Oliver in Ottawa partnered with their USCG, ICE, and Customs and Border Protection counterparts to field an effective pilot project on the Great Lakes and the West Coast.

Keeping with the intelligence-led policing model championed by the IBETs, the RCMP and USCG formed a Joint Operations Center (JOC) at the RCMP detachment in Cornwall, where an existing and robust IBET was already in place. Enjoying the participation and contribution of all IBET partners, the Cornwall –Massena shiprider team successfully met many of the unique law enforcement challenges presented by the multi-jurisdictional nature of the aboriginal territory bridging the Canadian–American border in that area. Criminals in this border area often commit crimes in the adjacent territory and then retreat via the water to their own territory, believing that the water is a safe haven where they cannot be pursued. Shipriders reported the look of stunned surprise on the faces of the first group of smugglers fleeing across the border when they encountered a USCG vessel with RCMP shipriders on board that continued to pursue them across the maritime boundary line!

What are the other benefits?

The shiprider program also fosters a fully integrated policing model between shore-based and maritime law enforcement officers. This is especially important because the ebb and flow in enforcement activity in the region almost always leads to the displacement or re-appearance of criminal activity elsewhere.

In Cornwall–Massena, enhanced shiprider presence on the water pushed a considerable amount of smuggling ashore to the bridges and ports of entry, where IBET partners were ready and able to take full advantage of this phenomenon, making increased contraband seizures in the surrounding land areas.

Evaluators reported that shiprider activities enhanced border integrity and that the visible presence of shipriders afloat and ashore had a direct impact on deterring criminal marine activity, either through the disruption of routes or the temporary cessation of criminal operations. Shipriders in British Columbia –Washington also used their increased presence on the water to extend boating safety and enforcement of small boat regulations to areas that previously were not regularly serviced.

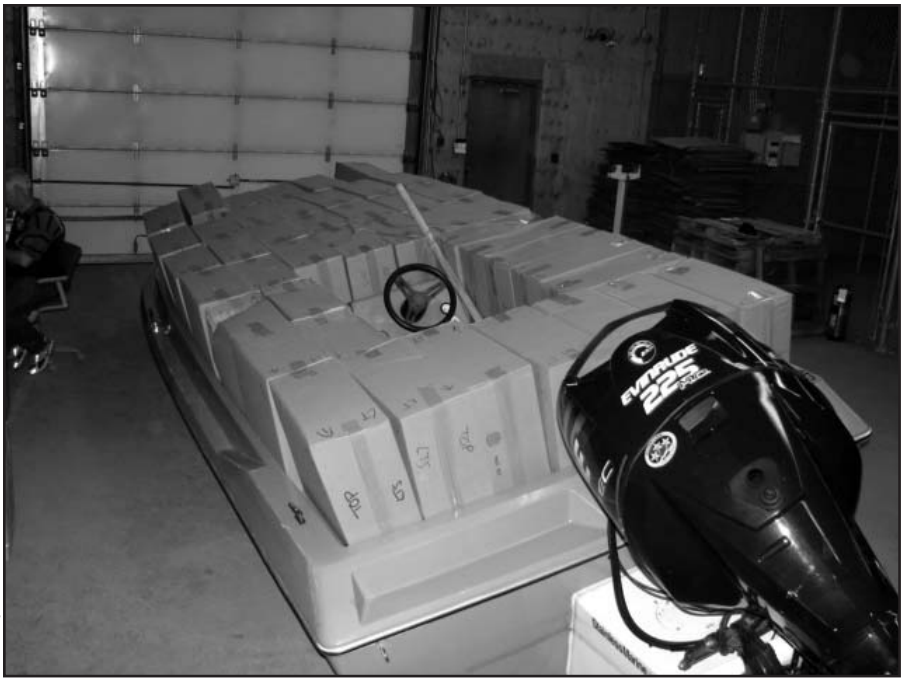
Next steps?

The safe and successful two-month pilot project ended in late September 2007. The RCMP and USCG are currently seeking approval from their respective governments to establish shiprider units on a full-time basis on the East and West Coasts and in the Great Lakes–St. Lawrence Seaway. Both agencies anticipate that formal treaty negotiations will begin in early 2008 to establish a formal bilateral framework for sustainable shiprider operations.

Going forward, the RCMP and USCG plan to refine their joint training program and expand the shiprider partnership to other Canadian, American and police agencies with maritime capacity and capabilities.

Throughout the world today, police within and between countries increasingly know what their counterparts are doing. On the maritime boundary between Canada and the United States, shipriders from both countries don't just know what their counterparts are doing — they're actually doing the work together as one to prevent the continued exploitation of the shared Canadian–American border by those engaged in cross-border criminal activities. ■

Cornwall shipriders seized this vessel loaded with 91 cases of contraband cigarettes.



Courtesy of the U.S. Coast Guard

Radicalization and the RCMP Community Outreach Program

Insp Wayne Hanniman and Angus Smith
National Security Criminal Investigations

A number of recent domestic and international cases, including Project O-SAGE (an RCMP-led counterterrorism investigation that resulted in the arrest of 17 suspects in 2006), the London Bombings of July 7, 2005, and the 2004 killing of Dutch filmmaker Theo Van Gogh, have demonstrated that the extremist threat is not always an external one.

There are native born citizens — of Canada, the United States, Britain, the Netherlands and a host of other countries — who are influenced by the siren call of radicalism and violent extremism and who are prepared to engage in direct action.

High-risk groups in this regard may include the children of immigrants who find themselves trapped between the traditional world of their parents and the often confusing and contradictory stimuli of modern western society.

Agents of radicalization can be religious figures or political ideologues who take advantage of anger and dismay over world events, foreign policy and the perceived plight of co-religionists or cultural groups in other parts of the world. Many individuals effectively "self-radicalize," whether alone or in small groups.

While popular opinion often equates radicalization with Muslim communities, there is no single religious or cultural group that is more prone — or more vulnerable — to radicalization than any other. Converts to Islam do not present any particular risk in this regard. The vast majority of such individuals (like the vast majority of Muslims) have no interest in either supporting or carrying out terrorist acts.

Violent groups of all kinds employ similar strategies and target similar demographics — particularly vulnerable and impressionable young people — and have done so throughout history. Over the past 50 years, police and security agencies have dealt with a wide variety of groups and individuals that have been radicalized to the point of extremist action. In Canada, these have included the Front de libération du Québec (FLQ) and the Squamish Five; in the United States, the Weather Underground and the Black Panthers; and in Europe, the Baader Meinhof Group, the Red Brigades and Action Directe.

Community outreach

The RCMP has developed a centrally coordinated National Security Community Outreach Program as one of its key responses to the radicalization threat. Deeply rooted in the RCMP ethos of bias-free and community policing and its Terrorism and Youth strategic priorities, community outreach is a critical component of the RCMP's overall National Security Program.

Since 2005, the Community Outreach Program has included a discrete Youth Outreach Program, intended to address the issue of youth political violence and radicalization by including young adults in the continuing dialogue on national security and policing matters.

The Community Outreach Program is a direct response to the concerns minority communities raised during a variety of public hearings, particularly the O'Connor Commission of Inquiry and the Anti-terrorism Act Review. These concerns included perceptions of being marginalized or branded as terrorists because of race or ethnicity, and fears of being victimized by any anti-minority backlash that might follow a major terrorist incident.

The Community Outreach program is intended to engage all of Canada's diverse ethnic, cultural and religious communities in the protection of Canada's national security, through understanding of mutual goals and concerns and appropriate and informed communications in times of crisis.

In order to open channels of communication between the RCMP and specific communities, the Community Outreach Program sponsors ongoing community meetings across the country. The meetings move beyond the "three Cs" of coffee, cookies and compliments, focusing instead on explaining the duties of the RCMP and its national security law enforcement responsibilities, as well as engaging participants in a frank discussion of community concerns.

In times of particular crisis — as in the aftermath of the O-SAGE arrests in 2006 — Community Outreach and Integrated National Security Enforcement Team (INSET) members meet with community representatives to apprise them of developments and to respond to any questions or concerns around the investigation and its potential impacts.

The tremendous diversity of the RCMP constituency requires real flexibility in any program aimed at communities and groups within those communities. The Outreach Program has evolved to suit specific regional needs. In Toronto, INSET investigators have designed and delivered a series of highly successful "Citizen's Academies" — short courses introducing the public to basic police procedure and enabling legislation. The INSET in Vancouver has also developed a "Youth Academy."

The RCMP Community Outreach Program is another example of how the RCMP works with individuals and communities to help ensure that high-risk groups and individuals find their place in Canadian society, without compromising their cultural and religious values. ■