"Putting speed bumps on the criminal path"

Delivered by: Mhoire Murdoch,
Vice-president eBusiness & Communications Business Solutions

Identity Theft/Fraud Conference, Toronto (June 13, 2002)

Although we are up against an omnipresent, faceless enemy, together, sharing and employing these best practices, we'll get ahead and stay ahead of this identity theft and fraud problem. At the very least, we'll put some big speed bumps in the criminal path. In this paper are insights into Canada Post's strategic understanding of the problem and our place in it; some of the services we offer to help our side; and a few ideas we're thinking about for the future. We recognize that we're only part of a larger effort that must be coordinated to be effective.

Identity theft is nothing new. Vindictive spouses and scorned acquaintances, misguided youth, petty criminals, and professional criminal organizations, engage in it all the time. Still, identity theft alone is really a banal and petty crime. In the words of the US National Fraud Center to the professional criminal, "Identity theft is simply a means to commit a greater crime." What kind of crime? Try terrorism, commercial and every other fraud imaginable, money laundering, and drug trafficking. That's important to understand. It puts mail theft and other decidedly low-tech ways of obtaining information--as well as sophisticated high-tech gadgetry into the proper context. It points us to: why the theft happens, the real value in the act, the criminal's points of pain, and where we can best address the problem.

Since written communication started being passed between people, identity theft has been a fact of life for post offices, couriers, and messengers. Information that has value for an impersonation is a target for thieves. With all the identifying information such as banking, credit, licensing, registration, and health records, among others that post offices transport every day, we face a daunting task in protecting our customers and Canadians at large.

It's an especially difficult task because we live in an extraordinarily open society. Democracies are supposed to be transparent. But that means trading security for freedom. Generally we treasure our freedom and openness despite its potential detriment to our security. For example, it wasn't too long after the horror of 9/11 that our collective appetite for a more permanently locked-down condition waned. Lawmakers retracted earlier anxious measures. Civil libertarians rose again. The mere whisper of the word "profiling" – regardless of context – stirs many a heart. And, most relevant to the theme of this message, it's now coming out that the organizations who could have worked together to prevent that tragedy . . . did not.

For Canada Post it means that while our internal operations are strongly secured, much of our system remains open. Even with last fall's graphic demonstration of how an open system can be sabotaged, you still have the freedom to anonymously throw an item into a mailbox; on a sidewalk; anytime. Mail is still delivered to unlocked, unattended letterboxes. General delivery is an acceptable address. All of this not because Canada Post can't or won't change it, but because it's what our society demands.

Sadly for all of us, it is this openness in our society that criminals prey on. What's more, the achievement of lightning-fast communication channels, such as the Internet, have created a smooth highway for the criminal; one with few potholes, dead-ends, or speed bumps. The opportunity to gain tremendous profit at relatively little risk in a short period of time attracts the criminal. And, his – or her – imagination is usually more clearly focused than ours. Their goal is quick spoils; ours, in this case, is to prevent loss. It's not quite the same incentive – until the loss gets high enough. The FBI estimates that a case of identity theft occurs every two minutes. The cost of identity theft is hundreds of billions of dollars annually. The victims are individuals and large businesses numbering in the hundreds of thousands, if not millions. That's pretty high.

So what about Canada Post? We're particularly concerned because of one indisputable fact: Canadians trust Canada Post. You trust us mostly to get your mail from point A to point B without the contents being seen, and usually without the connection between the two parties being recorded. Then, some sensitive information doesn't reach the intended recipient, possibly with unfortunate consequence. Immediately, and not entirely illogically, that same trusting public concludes that it must be Canada Post's fault. Much more often than not – it's not. Here's why.

On a continuum from the sender through to the receiver, Canada Post's control extends almost completely around the entire process. But, as noted, our induction and delivery processes are often in open environments. We expect that mail inducted into our system has been delivered to us complete and in good faith. Similarly, the choice to have a delivery made to an insecure receptacle is a statement about the receiver's security standards, not ours.

Canada Post has over 150 years of success securing the mail in our possession. Obviously we are not without incident. On the whole, however, our record is without compromise. Still, just as we do not usually control the extremes of the mail chain, neither do we control the informational content of the mail.

When asked why he robbed banks, Willie Sutton allegedly responded, "Because that's where the money is." Similarly, a mailbox or a dumpster is one way to get one identity. Lots of work for a limited payback. The mail *system*, on the other hand, provides an endless rich vein of information. Lots of work, but once systematized, very lucrative. The same goes for online communications and transactions. The mother lode is, of course, a directory of information made readily and rapidly available for theft and criminal use via the Internet. In all cases, our lines of defense are systemic protection, prevention, and proactive incident detection.

There is one additional way to address the problem. While the *system* is attacked and its weaknesses exploited, the *content* is the prize. Security enhancements co-evolve with criminal technique – again, now spread rapidly on the Internet. That kind of defensive battle is essential but ultimately futile. Perhaps one alternate way to address the problem is to play offence by *fundamentally changing the value of the prize*. In other words, the identity information that can be stolen to perpetrate an identity fraud needs to be much less easily used by unauthorized parties. Thus, given that the system remains substantially open, one solution we endorse is making the information itself less valuable to the criminal. For example, extending the use of protective measures such as "split" mailings of identifiable data, and so forth.

We believe that Canada Post can play a significant role in curbing the effects of identity theft and fraud in two fundamental ways.

- First, by making sure addresses are always correct and up to date.
- Second, by securing the information transmission process and providing more rigorous authentication alternatives.

Before addressing a few specific products and services, we have to acknowledge the superb work of Canada Post's Corporate Security team. Like Javert, they relentlessly pursue real and potential security breeches to ensure the highest sanctity of the mail. In this climate of increasing identity fragility, they, with our operations, and retail organizations are taking a number of actions to mar the smooth road to riches for the identity thief . Most immediate, Canada Post is re-enforcing a zero tolerance policy on non-compliance with customer and information protection measures. Nobody should or will access mail or change an address unless they can prove a right to do so. Internally, we are raising an already heightened level of security of both physical and digital assets in our possession. We anticipate these changes alone will create a significant obstacle to the identity thieves and yield immediate benefits.

We are also undertaking an enormous project to clean up our directories of Canadian addresses and increase the informational value of that data store. The magnitude of the project may not be apparent without realizing that there are approximately 13.2-million valid addresses in the country with some 200,000 added every year. To complicate matters further, municipal amalgamations have been creating redundancies and additional address changes. Our initiative begins with a cleansing of addresses so that we can be sure what is and, more importantly, what is not a valid address. Next, it will include attributing valuable information to the address, from the mundane such as what the address is: residence, business, prison, and so on; to the much more meaningful such as historical information about that location. We will be taking steps with our own initiatives, such as our national and electronic change of address databases, as well as with partners, to provide best-in-class data quality solutions to our customers.

Canada Post believes that the future is digital, and that the future is here now. We have a number of products and services that go a long way to address the second fundamental way we can participate in limiting identity theft. They include:

- Volume Electronic Mail is, in the view of some of our largest mailers, a sophisticated way to include our customers securely inside our mail system. Data files for bills, statements, and such are sent to us electronically. We print them within secure facilities, inducting the output directly into the mail stream. VEM very effectively closes one of the attack points in the mail delivery process.
- Our secure electronic courier service, PosteCS, provides customers with a customizable solution to otherwise insecure email. This browser-based system and process is transparent, uses state-of-the-art encryption technology, and allows the user to bypass firewall rules on attachments while maintaining highest security. PosteCS is the electronic complement to the traditional postal service.
- Probably the best-known part of our electronic initiatives is ePost. This electronic bill presentment and payment solution is developing an ever-stronger value offering to both business and consumer users as their respective numbers in the system increase. Within this purely electronic setting we limit the identity thief's attack profile and hence the protection focus to high-end hackers. The level of security and protection of both mailer and consumer data is kept extremely high. Moreover, we've taken our own

advice and split-mail identifying data to users. Again, ePost is a valuable contribution to the *prevention* of identity theft and fraud.

- Canada Post is part of the consortium developing and delivering Government Secure Channel to the federal government. The Electronic Postmark is a sophisticated time-attestation service that adds certainty to the validity of transactions made with the Government of Canada. This is a service we believe to be a critical step in the broad acceptance of robust, non-trivial, online commerce.

As the direct to home connectivity company, Canada Post believes the future of all commerce – online and off – will incorporate digital means of some sort. Not the least of these are digital forms of authentication, encryption of information both in storage and in transit, and further hybridization of electronic and physical transmissions.

The current technological wave is Internet-based interoperability known as Web services. We are convinced that information sharing, standardization, and machine-to-machine transactions will make profound changes in how we all use the Web for business activities.

This year's major eBusiness focus – apart from Web services – is identity. This coin presents privacy on one side and authentication on the other. Greater security of information and communication requires the certainty of greater authenticity of the parties in a transaction. In other words, identity needs to be defined, captured, managed, and authenticated. The challenge is no longer technology. It's how well that identity is first registered. We are evaluating ways that Canada Post can contribute to a high-quality proofing process that provides you, Canadian businesses and citizens, with the means to acquire, protect, and use strong virtual identities for both online and offline transaction needs. Obviously, our national retail presence, Crown Corporation status, and legislative enforcement muscle ideally positions us to be a universal certificate authority. Migrating our position as a trusted third party in the physical world into the electronic world also seems a natural evolution.

Assume that the identity of the parties to a transaction can be verified by a trusted third party after the registration process. Assume the right technology is in place. The next step is to trap, time-stamp, document, and archive key attributes of online transactions. Whether in a one-step action such as a purchase order form, or a multi-step activity such as a negotiation to a binding contract, these mechanisms would allow it to happen online legally, and conceivably with even greater certainty than exists offline today. We are presently testing several levels of Electronic PostMark for the commercial world. To put it into perspective, the features mentioned can be employed to create digital parallels to our physical stamp cancellation, Registered Mail, and other services. Beyond that, these same functions allow us to achieve electronic notarization and even transaction life-cycle management.

Let's return briefly to how digital technologies can assist us to make identity theft more difficult in the physical world. What if every mailer – large and small – had to identify itself with a strong means of identification, such as a PKI-encoded smart card, to use the postal system? What if open delivery was discontinued and the post office box key was replaced with that same smart card? What if every piece of addressed mail was encoded so that everything about it but its contents was traceable? Orwellian implications aside, such a completely closed system would make getting away with identity theft close to impossible. Our efficiencies in mail processing, including sorting and redirection, would increase dramatically. It's not as far away as you might think. 2-D bar-codes, PKI, smart cards, disposable RF tags, closed

induction and secured delivery technologies all exist. But, while we are exploring the pieces, we're not pursuing the whole. The costs and impositions on the citizen are too great to be palatable right now. The point, however, is that the world is changing. Eventually, even the social pressures within which we live may change. Canadians will value their personal security more than these apparent impositions on their perceived anonymity. That value-shift, as all others through history, will drive changes to our system – and to yours. Canada Post is ready for it.

Obviously, we at Canada Post are active and thinking about products and services that will improve our collective condition in this battle against identity thieves. Since becoming a Crown Corporation in 1981, we have evolved into a much more pro-active and forward looking firm. We have achieved profitability for the last seven consecutive years and have been financially self-sufficient for a decade. We make annual dividend payments to our shareholder and have returned over $300 million in dividends and contributed capital to the federal treasury. The Canada Post team is especially strong at working within the network paradigm together with our suppliers and our customers at the design and development stage so that we can share knowledge, create new best practices, and prosper more effectively. With that in mind, let's sum up the Canada Post strategic position.

First, we recognize that there is a problem. It's been around for a long time, but the stakes are getting higher; the value of the theft greater; and the criminals more imaginative. The speed and anonymity of the Internet channel have changed the pace of play. Moreover, the losses have become untenable. We believe that it is our responsibility to deliver on our brand promise of trust. So we're taking action now and for the future to protect Canadians' private information from this insidious problem – at least while in it's transit.

Second, we're working alone and with other businesses to build speed bumps on the path leading to identity fraud. Most of these bumps will be in the form of stronger personal identification and authentication. Whether in the form of national identity cards or otherwise, validation by a universally-acceptable, disinterested, trusted third party will be critical. We think that "acceptability" rests on the rigor of registration, validation, authentication, and protection of the identities. To date, two problems have stalled this effort. One problem is technological immaturity; the other is cost. The technology is now ready for prime time. So the challenge we are pursuing is how to bring the benefits of greater digital-based security to all of us at a much lower cost collectively using our core competencies, our position within the business landscape, our trusted status with Canadians, and our relationships with customers and partners.

Finally, we are absolutely cognizant of the need for all of us to work together, to collaborate, to network, and to become co-dependent when it comes to protecting ourselves, our economy, and our markets (also known as our fellow citizens) from this problem. At Canada Post we have focused our teams on this urgent problem with the mandate to aggressively pursue all opportunities. If you believe there are other ways that your businesses can work together with Canada Post that have not been addressed here, we invite you to contact us to engage a discussion. The road for the identity thief and defrauding criminal is too smooth. Together we can put in a few speed bumps. Let's start the process today.