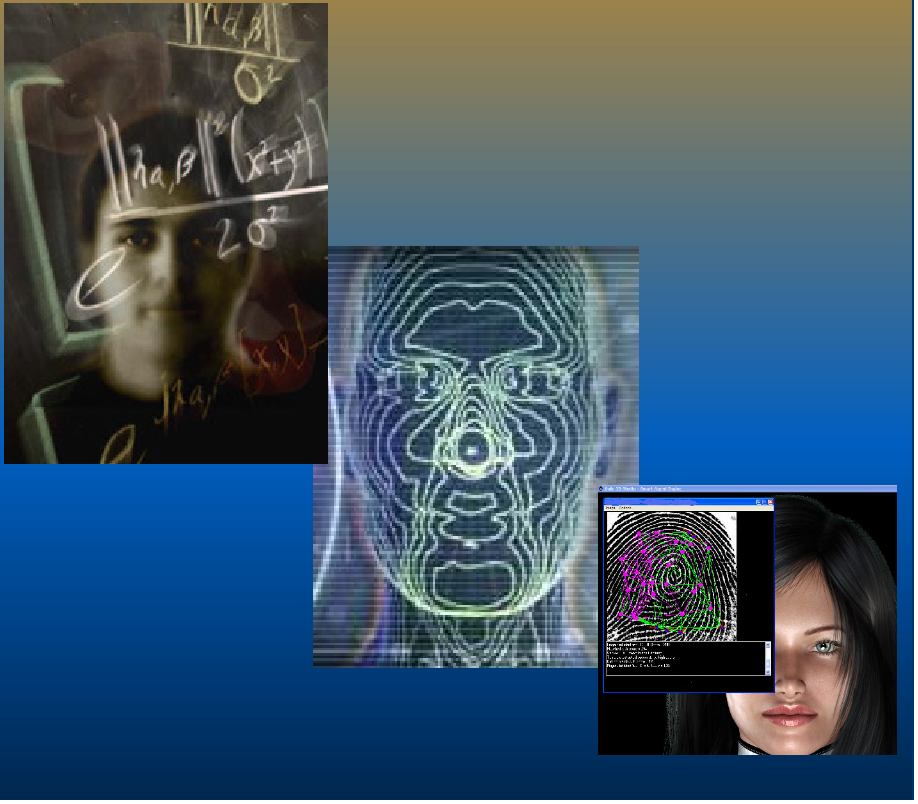
aTrust Inc.

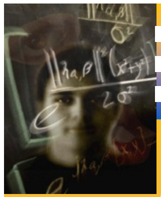


CyberSecurity & CyberAccess

June 29, 2010

“Closing the Human Identity Gap for Digital eCommerce”

Submission to Industry Canada for GoC’s Digital Economy Strategy Consultation

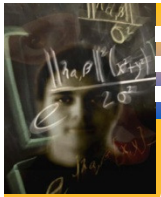


Background

The Government of Canada has committed to “launch a digital economy strategy” to drive the adoption of new technology across the economy.

This document presents 6 Strategic Imperatives which if adopted into policy and products, will:

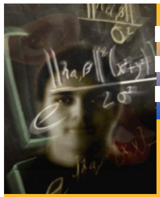
- enhance privacy and CyberSecurity
- prevent identity theft,
- result in a significant reduction in online fraud,
- provide greater confidence in the storage of sensitive data stored online (cloud)
- build trust and confidence in digital identities,
- enhance eCommerce,
- create innovation, new product development, & jobs.



CyberSecurity including CyberAccess and people

the human perspective

- People are the weakest link in computer & internet security (University of Wisconsin-Madison and IT University in Copenhagen, 2009)
- People are the weakest link in cybersecurity *(Sophos July 2009)*
- User is the weakest link in Internet Security *(Katonda News Network on 2010, March 16)*
- Users remain the weakest link in the IT security chain *(UK Computer Weekly Editor's Blog – March 5 2010)*
- Organizations typically focus on Cyber Security threats from the outside – but neglect the even greater threats from within.

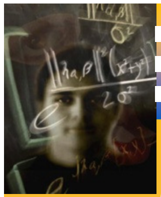


CyberAccess – Authentication is another weak link

1. **Legacy Authentication Systems**
   a. Passwords
   b. PKI
   c. Smart Cards
   d. One Time Password Tokens

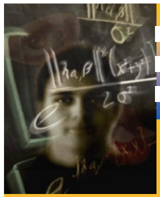
- ➢ Legacy authentication systems do not commit fraud or steal identities
- ➢ Humans commit fraud and steal identities

To stop fraud and identity theft *in e-Commerce, “**Close the Human Identity Gap**” by authenticating the human and providing assurance about the human’s civil identity credentials as part of the online authentication process.*



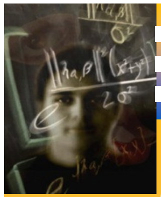
CyberAccess – the weak link

The use of legacy authentication systems has led to an ever increasing amount of financial and medical fraud, a growing number of data breeches and personal information loss, and an ever increasing amount of identity theft.

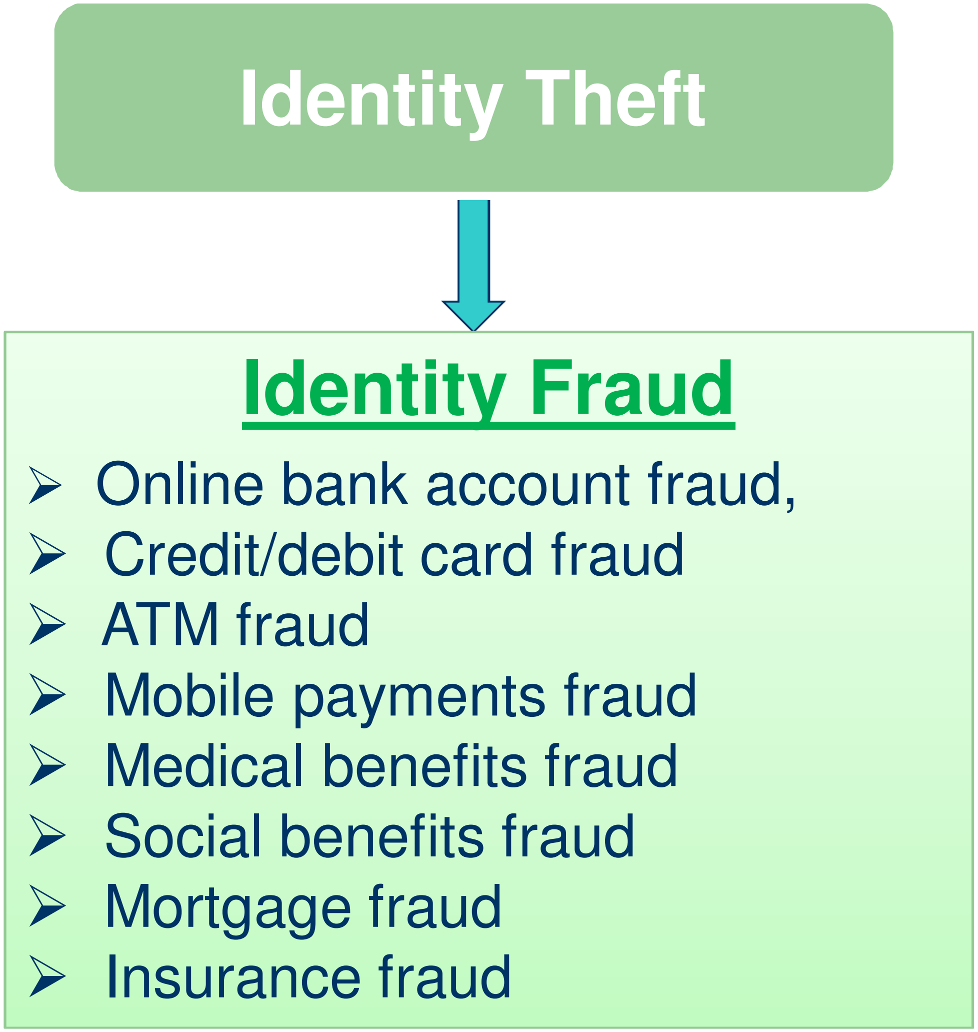


Identity Theft - a major barrier to deploying a successful digital economy strategy

1. **1.7** Million (6.5%) Canadians lost their identity to ID Fraud *(Measuring Identity Theft in Canada, 2008 Consumer Survey – McMaster University)*
2. Victims spent **20** million hours and **$150** million to resolve ID fraud problems
3. Most ID fraud involved **financial transactions**
4. Very few of the cases of identity fraud were reported to the police (13%), credit reporting agencies (6%) or PhoneBusters (0.5%).
5. Fully **20%** of consumers eliminated or reduced the amount of online shopping because of concerns about identity theft and fraud
6. Because of identity theft concerns 1.5 million Canadians pay $15 per month to credit reporting companies & banks, for after the fact Identity Theft Protection



A Barrier to Implementing Canada’s New Digital Economy Strategy



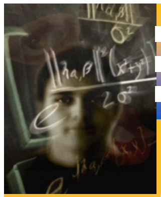
Identity Theft

Identity Fraud

- Online bank account fraud,
- Credit/debit card fraud
- ATM fraud
- Mobile payments fraud
- Medical benefits fraud
- Social benefits fraud
- Mortgage fraud
- Insurance fraud

A Drag on the Economy

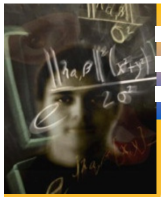
Approximately $5.4 Billion lost to Fraud in 2008



Prevent Identity Theft

Make Identity and Trust Assurance, “The currency of the Internet.”

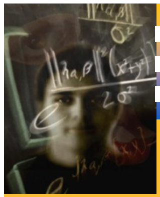
The GoC’s Digital Economy Strategy should include a proactive approach to **prevent** Identity Theft.



Six Strategic Imperatives for Secure Cyber-Access

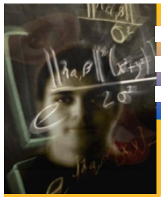
1. non-repudiable Internet access device authentication, (authenticating the Internet access device which is used to authenticate the human);✓
2. non-repudiable Service Provider authentication which prevents phishing and man in the middle attacks;✓
3. privacy compliant, non-repudiable, electronic human authentication (ehAuthentication) that complies with Assurance Levels 1- 4 as defined in NIST SP 800-63;
4. non-repudiable, ehAuthenticated (AL1-4) transaction confirmation and transaction authorization,
5. non-repudiable, ehAuthenticated (AL1-4) business transaction identifier as required by (ISO 15944-eBusiness specs),
6. non-repudiable ehAuthenticated (AL1-4) yes/no decision process to accept or reject a transaction.

✓ Legacy authentications systems ONLY comply with items 1&2



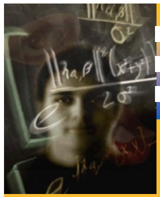
Innovation and Jobs

- development of privacy enhancing technologies is being held back by various market forces in the software industry
- governments should promote privacy enhancing technologies
- the industry will essentially build whatever is demanded
- “if privacy enhancing technologies are a requirement, government should say so and industry will respond.” *Pan-Canadian Strategy for IdM&A Page 33 of 180 IATF Final Report.*
- the development and building of privacy enhancing technologies will create innovation and jobs



The Government of Canada as a model user

"By being an early adopter of emerging and next generation technologies, governments can help drive ICT uptake in the private sector" *(Govt. of Canada's Digital Economy Strategy Consultation)*



Cornerstone Applications to Showcase Canada's Digital Economy Strategy

As set out in the Pan Canadian Strategy for Identity Management and Authentication, & the GoC's Cyber Authentication Renewal Strategy, and to set an example for others in Canada to follow, it is suggested that the GoC take the lead and utilize the 6 Strategic Imperatives for Secure Cyber-Access at the Federal Level to make federal applications cornerstones for Canada's new digital economy.

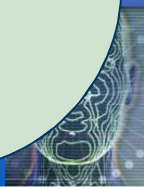
Applications

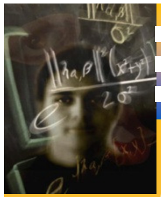
1. Canada Access Key (formerly ePass/Secure Channel)
2. myKey (internal federal government online access system)
3. Canadian Health Infoway (access to electronic health records)
4. Electronic online voting, online referendum, online surveys

Policy

Develop policy to establish Assurance Levels for online access, for example,

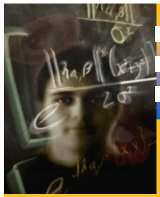
- a) Law Enforcement, DND, Classified Networks (AL4)
- b) Access and transmittal of health information, taxation information, SCADA networks , online banking, ATM, mobile banking/purchasing, online credit/debit card purchasing(AL 3)





A Secure CyberAccess Solution

A recently available, disruptive, privacy compliant, CSEC evaluated, secure CyberAccess solution is now available that meets the six strategic imperatives. This solution prevents identity theft, significantly reduces fraud, furthers consumer trust and confidence in eCommerce, and can help grow Canada's digital economy.



Contact

aTrust Inc.

Contact:

Sal Khan

Tel: 1-613-882-1114

skhan@atrust.ca

www.atrust.ca