Knowledge Based Authentication and Privacy

Can Standards Help?

Stephen P. Howard, President & CEO
SPH Systems, International

10.Feb.2004
Agenda

- Objectives
- Lessons learned from industry
- Regulatory
- Standards efforts
- Recommendations
Objectives

- Enhance relationship between service provider and the customer it serves
  - Deliver services accurately and easily
  - Friendly to “citizen”

- Stop fraud

- Reduce risks and losses
What Works?

➢ The most successful KBA implementations are found in financial processes
  ▪ Credit scoring
  ▪ Risk/fraud mitigation
  ▪ Applications (for mortgage, credit, etc.)
  ▪ Merchant web transactions

➢ It’s a process
  ▪ Highly adaptive
  ▪ Rules driven – it is a system
Whose Knowledge?

- Supplied by the “consumer” or “citizen”?
  - What they know that can be verified
  - Public sources

- Driven by application intelligence
  - Verification methods
  - Knowledge of behaviors
  - Driven by business risk management processes
Lessons Learned

➢ The first need is

“Know your enemy”

➢ So we can be

“Customer Focused”
Lessons Learned

- It’s based on massive data - your data
- Three steps to success
  - Know your enemy - metrics
  - Based on forensics, develop a rules set that mitigates risk
  - Exception processes for questionable transactions
- Accepted by the market place
  - Visible leader setting the tone on KBA: Citibank

- Fraud is unacceptable so can Federal agencies successfully use KBA?
  - Do industry authentication risks/rules apply in G2G, G2B and G2C situations?
  - Privacy is a driver based on need to “know your enemy”
Success Driven by Focus

- Start at one agency application
  - Maintain KBA risk scores from service providers on transactions
  - Analyze information about transactions and fraud rates
  - Determine rules to mitigate (translation: metrics)
  - Apply rules
  - Repeat

- As this works, add additional agency apps
  - Introduce risk scoring across applications
Which Sector Applies?

- G2G and G2B have a level of certainty and trust – typically involve
  - Verifiable, direct relationships
  - Low – medium volume of transactions
  - Higher level of trust in relationship

- G2C presents opportunities
  - “drive by” authentication
  - No prior relationship
  - Needs managed fraud services
  - Potential for very high volume transactions
  - Potential is high for fraud to gain access to entitlements
Traditional Inhibitors / Enabler and Mandates

- Privacy Act
  - Restrictions perceived on inter-agency sharing

- GLBA
  - Restrictions on financial records sharing without notice

- HIPAA
  - Restrictions on transport of private identifying information

- eGovernment Act Section 208
  - Mandates Privacy Impact Assessment
Standards Efforts

- Direct support for eGovernment Act’s section 208
  - X9.99 Privacy Impact Assessment
- Provides a neutral process for assessing privacy issues
  - What is the citizen/consumer giving you?
  - How are you managing it?
    - Throw away sensitive data, maintain the score!
  - Where is the data going?
- Formalizes the process to protect service delivery based on sensitive information
Recommendations

- Fraud is unacceptable

- KBA is a focus on process – look *inside* 
  - Rules based – each rule is a *metric* specific to Government

- Support standards to enable KBA risk scoring on large scale 
  - Engage in X9.99

- Deliver on Privacy Impact Analysis 
  - Enable use of federated KBA scores to reduce frauds perpetrated on Government applications 
Thank You!

Stephen P. Howard
SteveHoward@cox.net
703.319.3171