



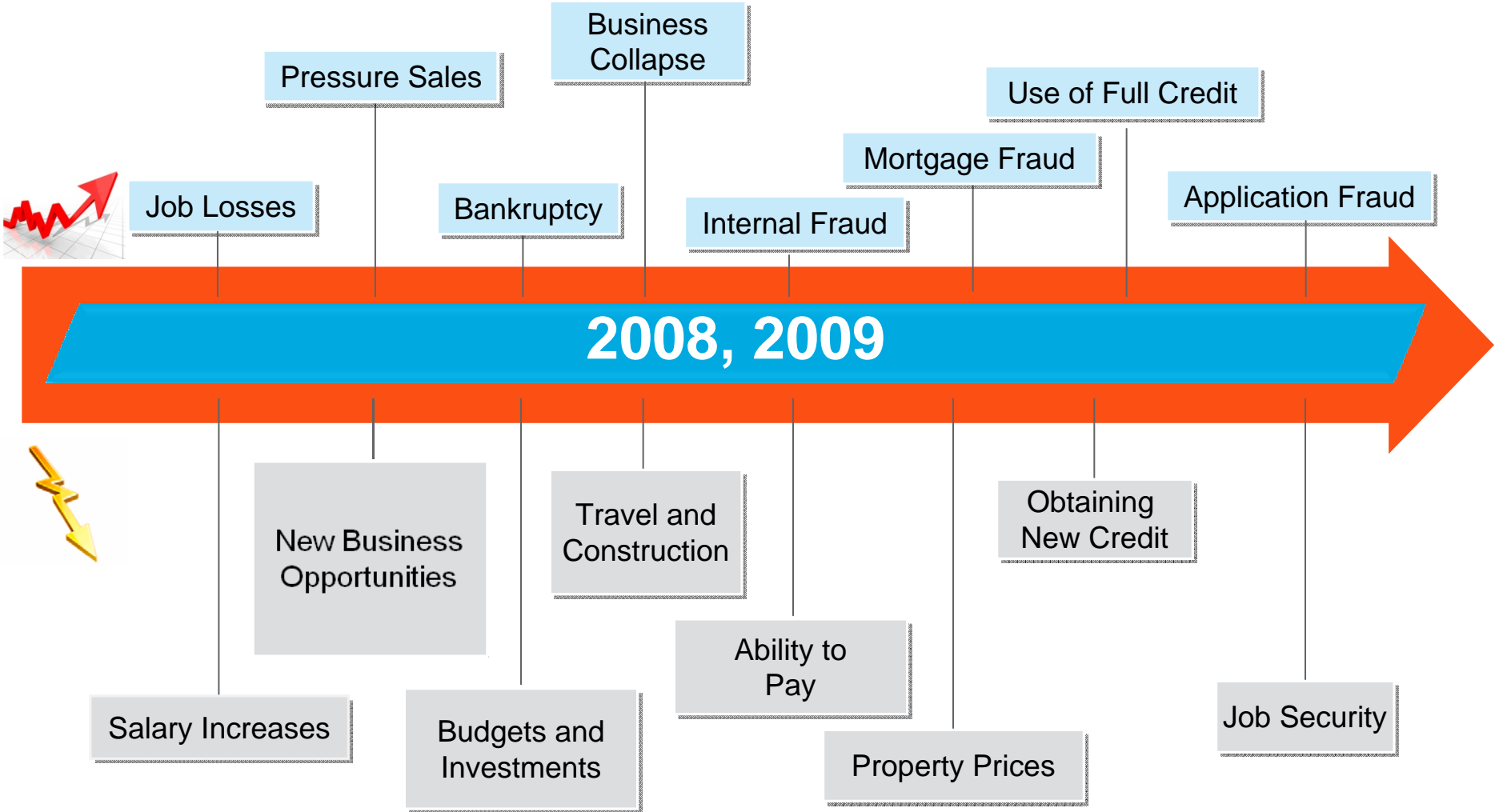
# Multi-Factor Authentication of Online Transactions

Shelli Wobken-Plagge  
May 7, 2009

# Agenda

- How are economic and fraud trends evolving?
- What tools are available to secure online transactions?
- What are best practices for securing online credentials?

# Economic Crisis Is Driving Consumer Hardship



# Consumer Hardship Increases Fraud Activity

The 10:80:10 principle, which has been consistently supported by research into criminology, says that in *any* given population

- 10% of people will never steal
- 10% will steal at any given opportunity
- The remaining 80% can move in either direction **depending on the pressures they are under** and how they rationalize a particular opportunity



# Identity Fraud is Rising

## IN 2008

- Identity fraud victims increased 22% to 9.9 million adults
- The total annual fraud amount increased by 7% to \$48B

## THE BAD NEWS




- One in every five identity theft victims leaves his/her bank
- One in every six victims leaves his/her card issuer

## THE OPPORTUNITY

- More than half of online banking consumers believe that security is a shared responsibility with their bank

Source: Javelin 2008 Banking Identity Safety Scorecard

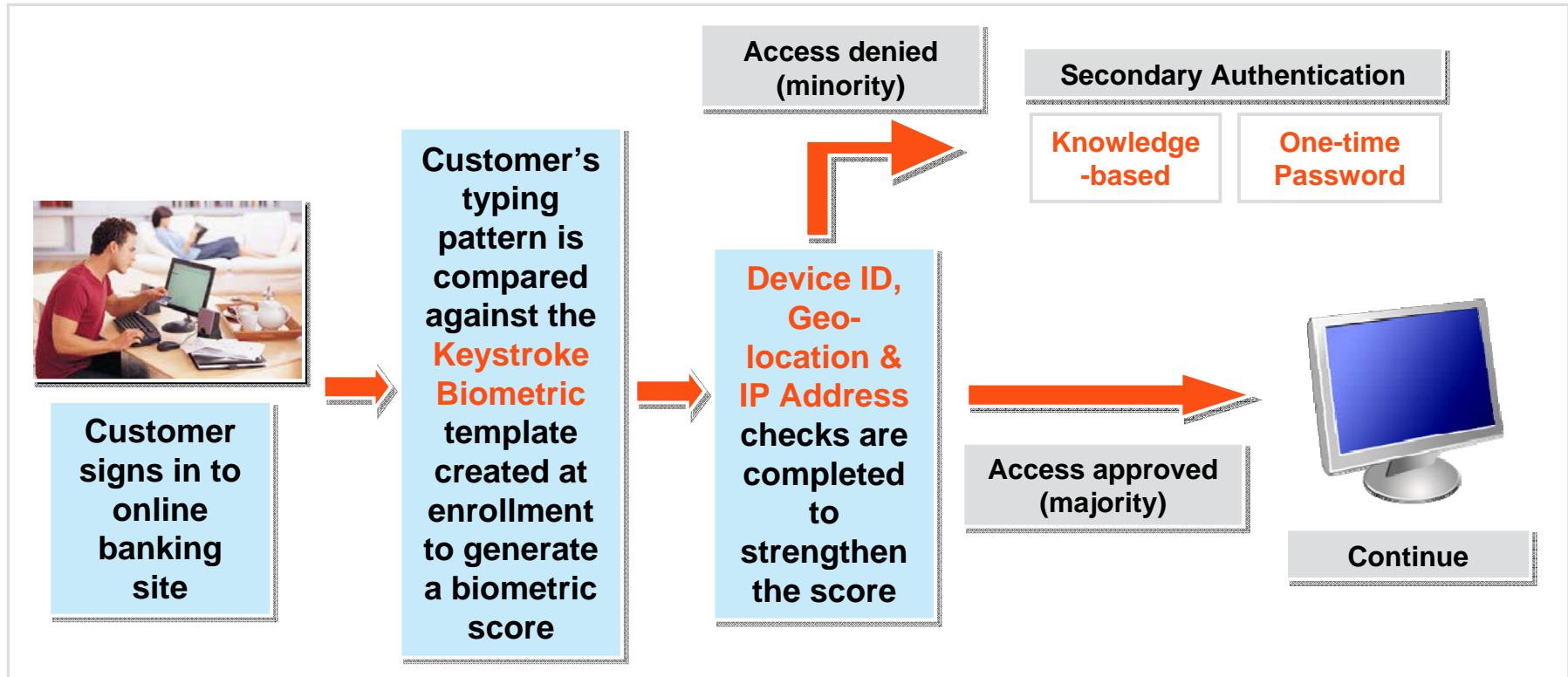
# The Three Factors of Strong Authentication

AUTH FACTOR	FORM FACTOR	ATTACK METHOD
<p>1st : Something you <b>KNOW</b></p>	<p>Login ID + Password KBA /challenge questions Secret images &amp; pa:</p> 	<p>Attacker must discover the known information.</p>
<p>2nd: Something you <b>HAVE</b></p>	<p>Hard tokens: OTP, smartcard... Soft tokens: Certificate, encrypted keys...</p> 	<p>Attacker must obtain or copy the token.</p>
<p>3rd: Something you <b>ARE</b></p>	<p>Fingerprint Iris scan Keystroke dynamics Heartbeat signature</p> 	<p>Attacker must replicate what you are.</p>

# Additional Authentication Techniques

- Alerts via a telephone call, e-mail or text message
- Internet protocol intelligence
- Geo-location
- Mutual authentication
- Mobile location identification
- Customer verification
  - Positive verification
  - Logical verification
  - Negative verification

# Leverage a Multi-Layered Approach



**MAJORITY OF USERS AUTHENTICATE INVISIBLY.  
MINORITY OF USERS AUTHENTICATE VISIBLY THROUGH  
SECONDARY METHODS.**

# Identity Verification Solution

Next-generation verification solution that use multiple up-to-date data points to deliver an actionable risk score on 100 percent of transactions.

## 3 powerful components that work together to deliver one definite decision

### Verification

#### Multiple sources of information to verify data

- Credit Bureau Headers
- Cell Phone Directories
- Phone & Utility Directories
- Direct Mail Sources
- Change of Address Directories
- Others

### Access-Point Intelligence<sup>SM</sup>

#### Dozens of sources to feed Access-Point Intelligence technology

- Demographics** - age, income, length of residence and credit activity
- Criminal Index** – analysis measures criminal tendency for the particular address
- Address Statistics** – structure type, associated with known fraud, seasonal use, and more
- Velocity** – every event seen by the system is tracked and updates the overall reputation

### Analytic Scoring

#### Verification and reputation information is fed into the system to create a score

- 100% of transactions receive actionable scores
- Developed from known fraud and identity theft cases
- Optimal means for analyzing the vast array of information available



# Risks and Opportunities

- Risks: the majority of financial institutions are in compliance with the FFIEC guidelines, but...

- Compliance does not equal security; weaknesses have been proven for many of the widely adopted methods

- Criminals have and will compromise credentials used to access your systems; a multi-layered security approach is a must

- Opportunities: online banking has stalled at around 35%

- Consumers continue to associate ID theft with online banking and online shopping yet fraud resulting from online data access only represents 11%

- Javelin found that 38 million additional consumers would bank online if their FI would adequately address their security concerns about unauthorized access of their accounts online

Source: Javelin 2008 Banking Identity Safety Scorecard

# Best Practices for Financial Institutions

- Perform a risk assessment to identify the most appropriate solution for the level of risk
- Balance security with minimal inconvenience to the consumer
- Leverage a multi-layered approach
- Engage the customer in setting online access controls and educating them on safety awareness
- Apply consistent solutions across multiple channels

# Contact Information

Shelli Wobken-Plagge  
Vice President, Risk and Fraud  
First Data  
(402) 777-8106  
[shelli.wobken@firstdata.com](mailto:shelli.wobken@firstdata.com)

