



**Insurance Industry  
Committee on Motor  
Vehicle Administration**

VISION

**On Line (Web-Based) Insurance  
Verification – (OLV)**

Phase I & II

Loren McGlade, Chairman

Jon Neiditz, Partner & Info Mgmt Practice Leader, Nelson Mullins 1



# The IICMVA

The Insurance Industry Committee on Motor Vehicle Administration

- The **IICMVA** acts as a liaison between the insurance industry and state agencies, providing guidance in setting and implementing rules pertaining to Compulsory Insurance and Financial Responsibility laws.
- **IICMVA** is a vendor-neutral organization.
- **IICMVA** does not advocate insurance reporting programs as a means of reducing uninsured motorist rates.

\*The national uninsured rate is currently 14.6%.

- However, if required, **IICMVA** membership is committed to implement the best method available.





# Commercial Automobile DMV Reporting Summary

- Currently, there are nineteen (19), down from 21, states that require some type of Commercial Auto DMV reporting:  
AR AL AZ DC FL GA HI KS KY LA MA MD NC  
NM NV NY OR PA UT VA  
CO & ME Cancelled their programs in 2007
- Of these states, currently only three (3) require full VIN specific reporting for all vehicles insured:  
NY, MA & NC
- DC (Effective 5/1/05 – Only when a policy is cancelled & VIN is known)
- KY (Effective 1/1/06 – Only when a policy in cancelled)
- KS (Only when a VIN is known)
- Several states exempt reporting when the vehicle is part of a Fleet Registration Program





# Commercial Automobile DMV Reporting Summary

- Several states have voluntary reporting programs for Commercial Auto Reporting:

CA CO GA KY NE OK SC TX WY

- The following twelve (12) states require VIN Specific Reporting for Non-fleet Commercial Auto policies only:

AR AZ FL GA HI KS LA MD NM NV OR VA

- **Note: The majority of states define a Commercial Fleet policy as one that has five (5) or more vehicles on it**
- **Refer to the state specific web sites for additional reporting information on these states:**



click on the DMV Homepages:

<http://dmvwebsites.com/>





# Comprehensive Database / Cancellation Reporting Systems

- Thirty-three (33) states use some type of verification
- Arizona (EDI; X12) – Personal & Commercial
- Arkansas (EDI; Proprietary) – Personal & Commercial
- California (EDI X12; CA Proprietary) – Personal Only; Used for Online Registration & Proof of Coverage, Law Enforcement use 7/1/06.
- Colorado (X12) – Personal, Commercial Voluntary
- Connecticut – (HTTPS & email; proprietary) Personal at this point
- District of Columbia (Electronic – PIER) – Personal & Commercial (if VIN is available)





# Comprehensive Database / Cancellation Reporting Systems

- Florida (FTP/EDI; proprietary) – Personal & Commercial
- Georgia (EDI; proprietary) – Personal & Commercial (Fleets of 2 or more are exempt)
- Hawaii – Cancellations & List of Vehicles Quarterly
- Kentucky (SFTP; proprietary) – Personal only, Commercial for Cancellations
- Louisiana (Proprietary) – Personal & Commercial
- Maine – Cancelled Program in 2007



# Comprehensive Database / Cancellation Reporting Systems

- Maryland (EDI; X12) – Personal & Commercial
- Massachusetts (EDI; Proprietary) – Personal & Commercial
- Nevada (Tape; proprietary) – Personal & Commercial
- New Jersey (Tape; proprietary) – Personal
- New Mexico (EDI; X12) – Personal & Commercial
- New York (EDI; X12) – Personal & Commercial



# Comprehensive Database / Cancellation Reporting Systems

- North Carolina (EDI; proprietary) – Personal & Commercial; Fleet Registered are exempt
- Oregon (EDI; X12) – Personal & Commercial
- Pennsylvania (SFTP; proprietary) – Personal & Commercial
- South Carolina (EDI; X12; proprietary or Web) – Personal
- Virginia (EDI; X12) – Personal & Commercial
- West Virginia – Personal Cancellations Only



# Book of Business Data Transfers

- Kansas (FTP; EDI)– Personal & Commercial (if VIN is known); Used for Online Registration
- Kentucky (SFTP proprietary; voluntary) Personal; Commercial for Cancellations only
- Michigan (Proprietary; voluntary) – Personal; Used for Telephone Registration
- Missouri (Proprietary; enhanced random sampling with book of business reporting) – Personal; Cancelled their random sampling portion of program in 2005
- Nebraska (Proprietary) – Personal; Commercial is Voluntary. Used for Online Registration.
- Texas (Proprietary; X12) – Personal at this point
- Utah (Proprietary; E-mail) – Personal & Commercial



# Random Sampling Programs

- Alabama (Website) – Personal & Commercial
- Delaware – Personal & Commercial;  
Notification of Cancellations on all Personal Lines Policies than 6 months old.
- Illinois (Tape; proprietary) – Personal & Commercial
- North Carolina (EDI; proprietary) – Personal & Commercial
- Minnesota – Personal; Cancelled program in 2005



# Privacy/Security: A Public-Private Patchwork, with Private Security Standards Beginning to Dominate

	Private Enforcement	Regulatory Enforcement	Enforcement Through Competition	Court Enforcement
Private Standards	e.g., Payment Card Industry Data Security Standard (PCI DSS), AICPA's GAPP, IIA's GTAG, ISO, ANSI	FTC enforcement of APEC Privacy Framework, HIPAA deference to WEDI, "deemers"	new privacy competition between ISPs, "best practices"	private and/or Government Standards become Liability standards
Government Standards	e.g., outsourcing and other vendor contracts (including HIPAA business associate contracts, GLBA service contractor agreements, EU contracts for data transfer)	e.g., GLBA enforcement by "functional regulators," FTC Act Section 5 authority, FCRA/FACTA	e.g., handling of breaches and provision of monitoring/insurance	e.g., e-discovery, attempts at security breach class actions

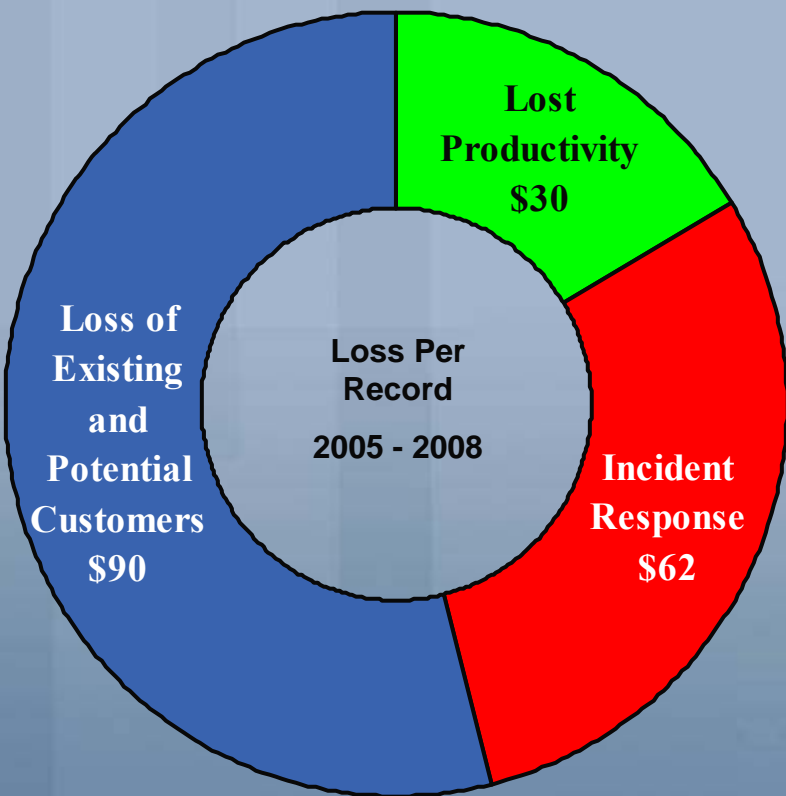




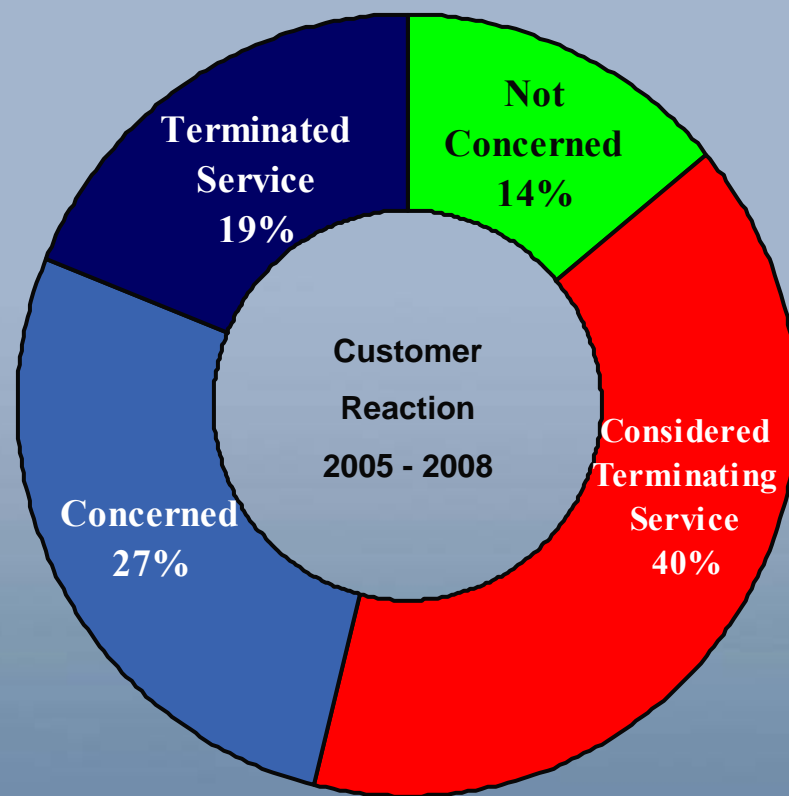
# Real Costs of Breaches

Cost of a Privacy Breach

Customer Reaction to A Privacy Breach



\$182/customer



Source: Ponemon Institute  
(numbers increase from 2005-2008)



Source – Wired Magazine 2/07



# It is about to get worse: ARRA 2009

- Breach notification obligations for not only HIPAA-covered entities but HIPAA business associates turning on "unsecured PHI"
  - The combinations triggering notice under all state laws (initially designed to address the major causes of identity theft) jettisoned
  - Paper and even oral breaches (apparently) included
  - Exceptions
  - 60-day outside limit for notifications, but should be more prompt in the absence of justification
  - DHHS must be notified for breaches involving more than 500 people
- Secretary of DHHS to issue annual guidance on technical safeguards
  - Does not yet appear to favor encryption over other safeguards, contrary to all state breach laws, MA and NV laws, and guidance for federal financial institutions
- Enforcement by state AGs, more stringent remedies and shift in burden of proof



# The FTC Will Fix It (Not)

- The FTC just proposed breach notification rules that apply to non-HIPAA covered entities and non-BAs that are vendors of personal health records, PHR related entities and their service providers (i.e., Google and Microsoft).
- Breach defined as acquisition of PHR identifiable health information **without the authorization of the individual** unless reliable evidence showing there has not or could not be unauthorized acquisition.
- Under the proposed rules, an entity that has suffered a security breach must notify all US citizens (presumably international notification is required) and US residents **without unreasonable delay**, but **no later than 60 calendar days** of discovery unless law enforcement requires a delay.
- Must also notify the FTC after a breach. If the breach impacted 500 or more, must notify FTC **within 5 days** of discovery of breach. If less than 500, must keep breach log and submit it annually to the FTC.
- Applies to breaches that are discovered on or after **September 18, 2009**.
- HHS breach rules still to follow.





# DHHS Will Adopt Technology-Neutral Requirements (Not)

- On April 17, 2009, HHS issued proposed guidance identifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, as required by the Health Information Technology for Economic and Clinical Health ("HITECH") Act passed as part of ARRA.
- Only 2 approved methods: **encrypt** or **destroy**.
- Generally, for electronic PHI to be encrypted it must be encrypted using "an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might permit decryption has not been breached.
- 2 types of **encryption** specified: for data at rest (with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices) and for data in transit (those that comply with the requirements of Federal Information Processing Standards ("FIPS") 140-2).
- 2 methods of **destruction** specified: for non-electronic media (paper, film, or other hard copy media should be shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed) and for electronic (electronic media should be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved).



# Improving Verification

- Widespread dissatisfaction with current reporting systems prompted an industry search for alternatives
- Industry sought a single, uniform approach that offered:
  - Improved accuracy & consistency
  - Lower development and maintenance costs
  - Significant benefit to the public and jurisdictions



# Improving Verification

- Industry developed the IICMVA Web Services Model Guide to help states adopt a uniform approach that met the objectives.

Phase I & II are now complete.

- That approach has now been implemented in the state of WY as mandatory for Personal Lines as of 7/1/08 and OK as of 1/1/09 voluntary for Commercial Lines in WY, OK, and voluntary for Personal Lines and Commercial Lines in SC.
- The following states are in pilot mode with the IICMVA Model:

FL NM TX & UT

- Florida completed Phase I of the Pilot and has published a press release of its success





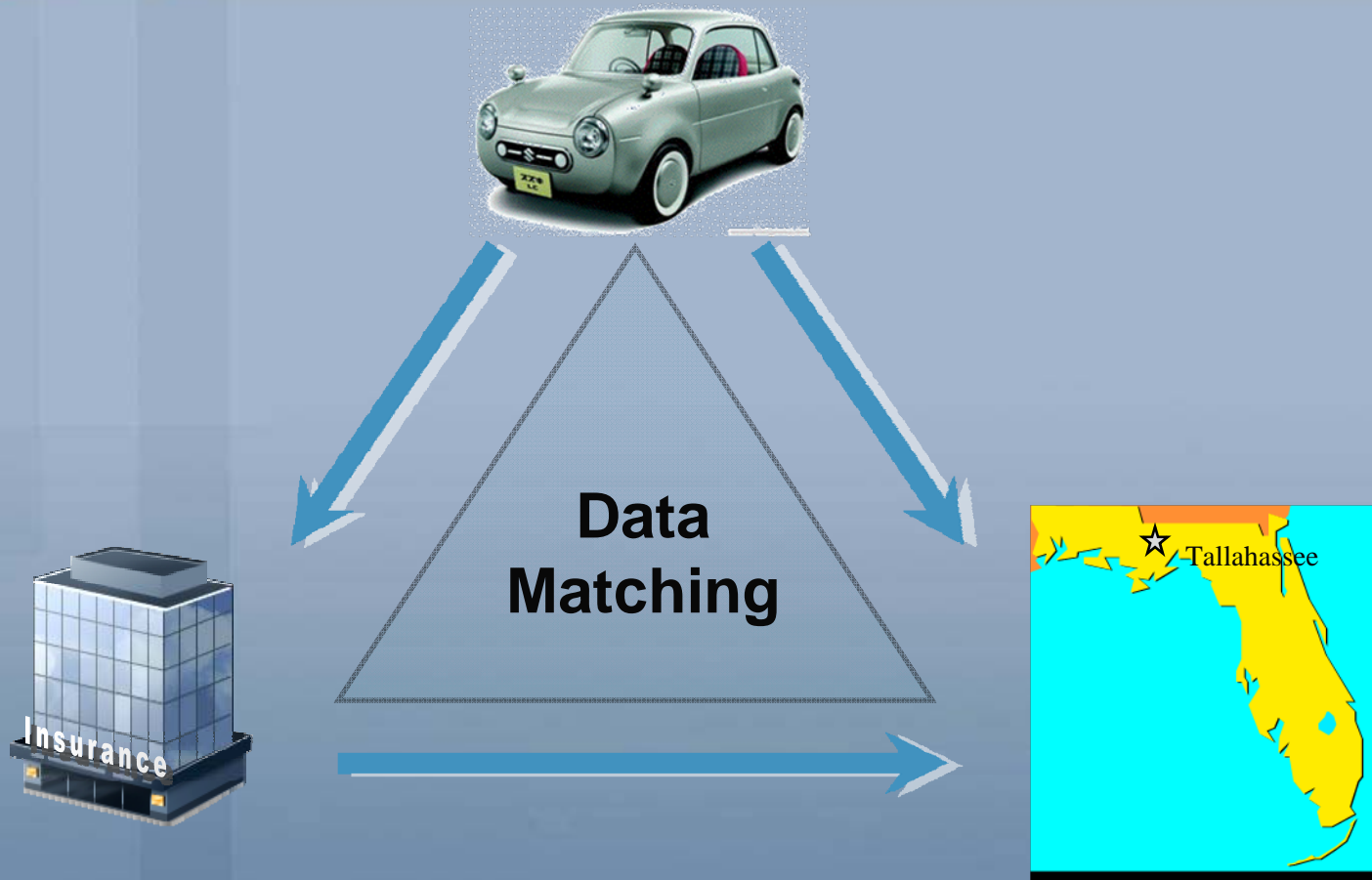
# Improving Verification

- Current activities include a working group formed to implement web services in Nevada. The group is called Nevada Live. The objective is to use the IICMVA Model to replace the current tape system for the information from the insurance industry.
- It is important to recognize the fact that the Insurance Industry is the **SOURCE** of the data necessary to perform the verification.
- The data when acquired from the Insurance Industry is the most current data available for verification.
- See the IICMVA Brochure for more details.





# The Database Model





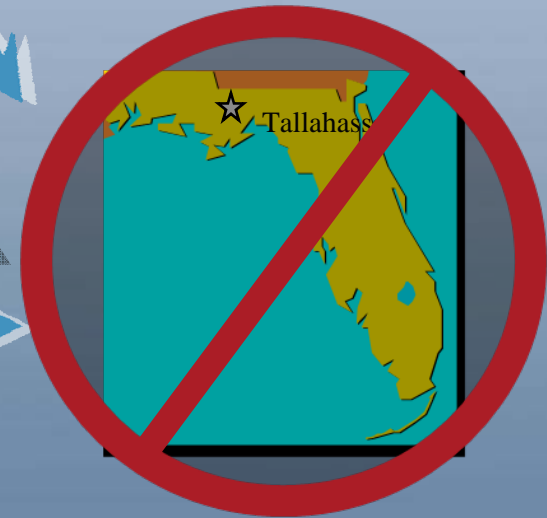
# Issue #1: Accuracy



1Z4GY6L12CD847567

1Z4GY6L12CD847587

Vehicle  
VIN

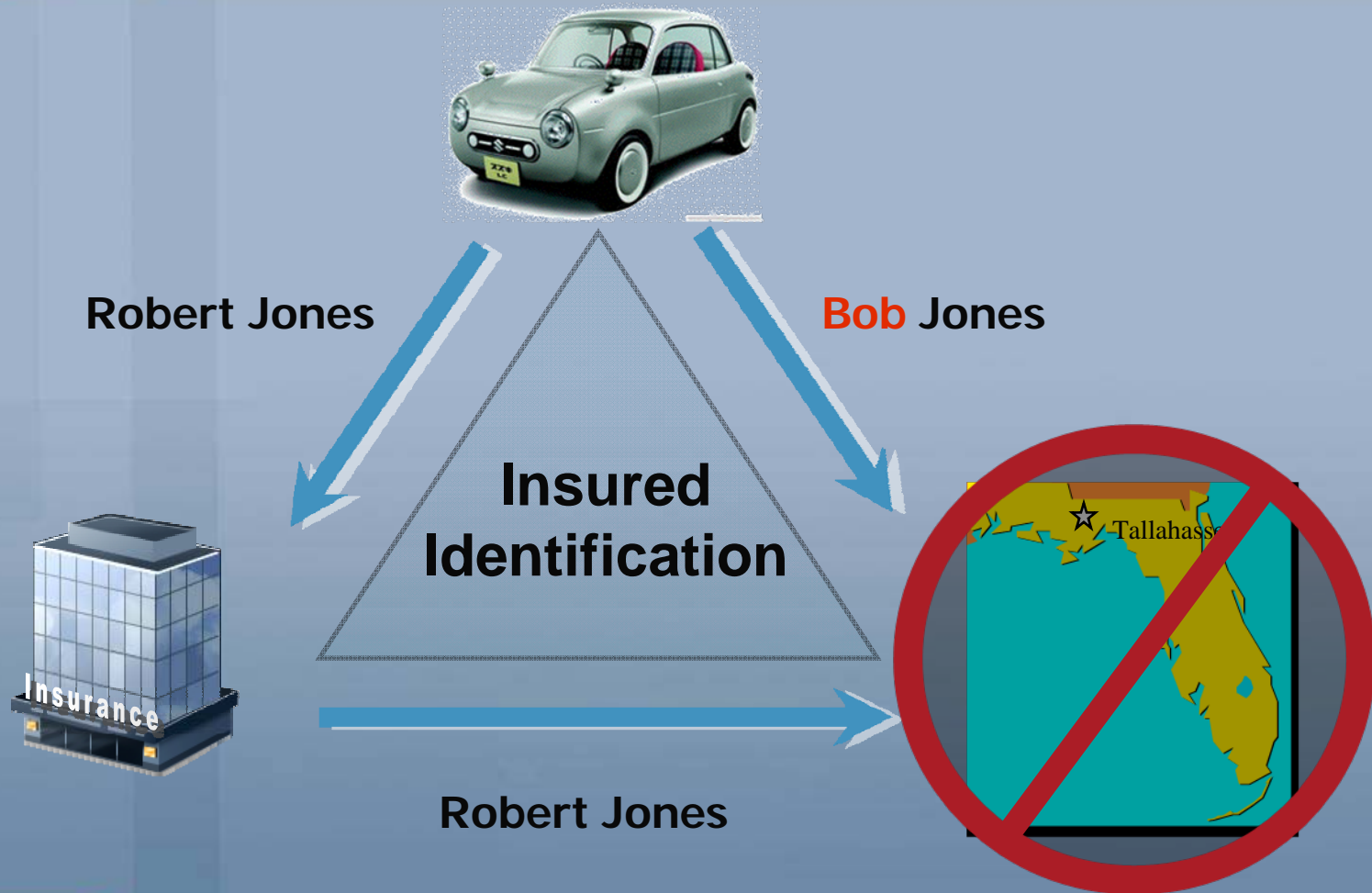


1Z4GY6L12CD847567





# Issue #2: Inconsistency





# Issue #3: Timeliness

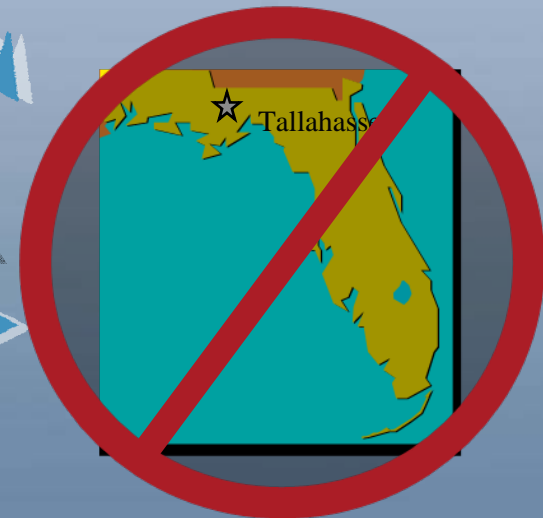


Adds to Policy  
June 5, 2008



Registers with DMV  
June 10, 2008

Reporting  
Timing



Reported  
June 12, 2008





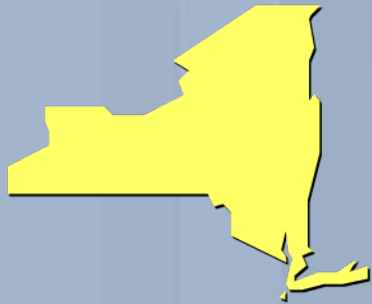
# Issue #4: Expense

- Before any decision is made by a state regarding what type of system to use, a cost/benefit analysis needs to be completed.



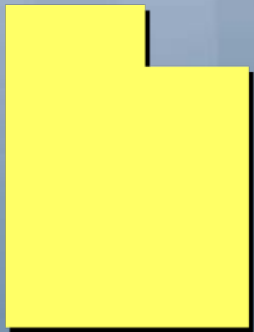


# Issue #4: Expense



- Cost to construct database solution in New York:

**\$4.5 Million**



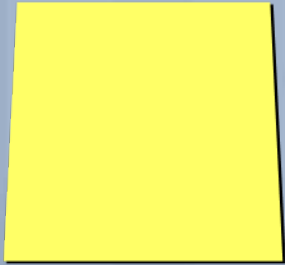
- Cost to construct database solution in Utah:

**\$1.2 Million**





# Issue #4: Expense



- Since 1997, Colorado's investment in their database solution has been:

**\$13 Million**

- Personnel required to administer the CO database verification program: **8 Full-time**

**Employees**





# Issue #4: Expense

- To pay for its database program, Missouri relies on a 6% tax, costing taxpayers...

**\$3.2 Million**

- Unfortunately, the annual cost to maintain the Missouri database system is...

**\$3.7 Million**





# Other Database Problems

- Database reporting designs can not conform to the needs of commercial carriers and their customer
- Databases must be maintained constantly and efforts to correct data errors continue indefinitely (\$\$\$\$)
- Databases raise concern over privacy and security during the transmission process



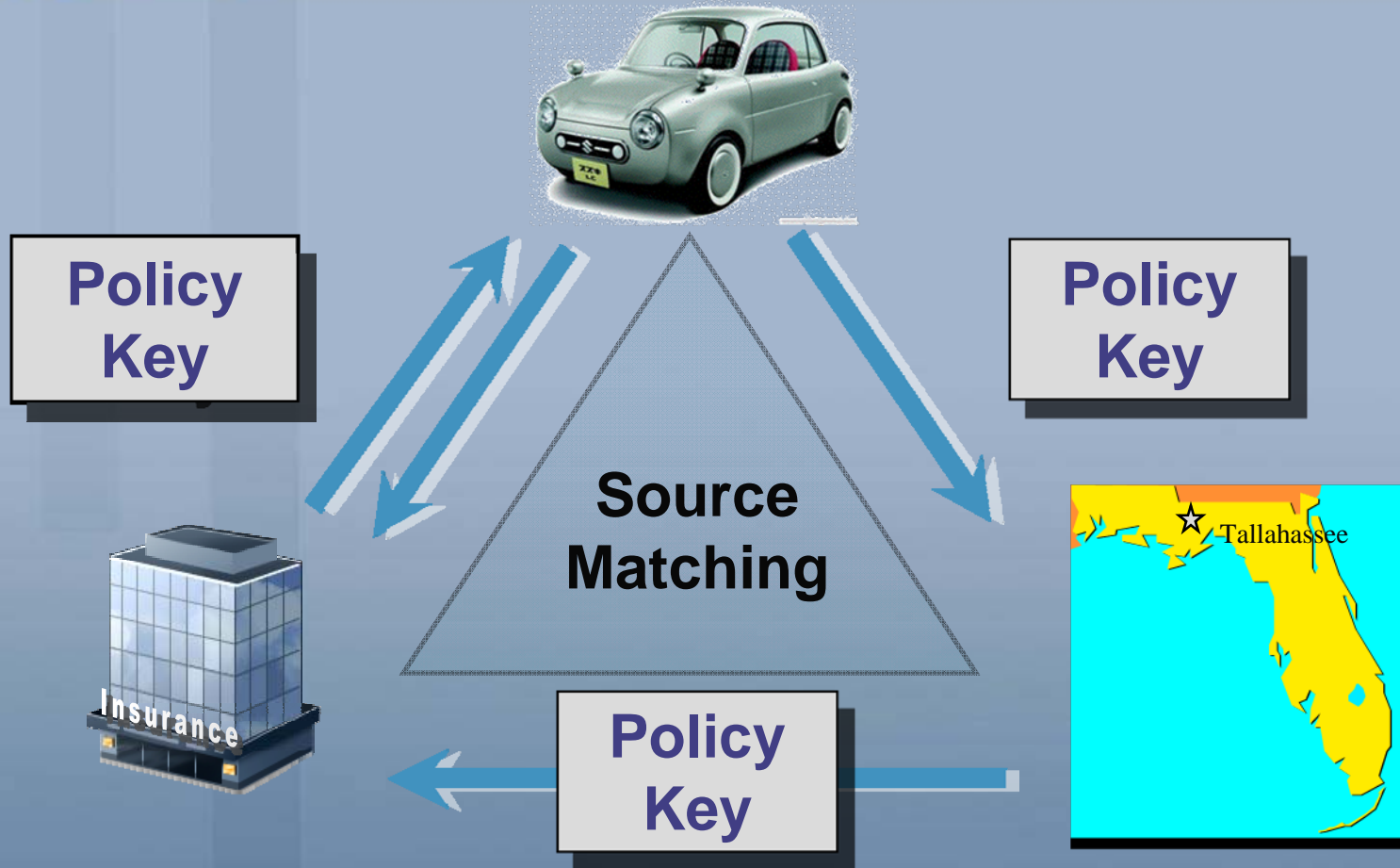
# The Web-based Alternative

- Standardized approach across states
- Simple internet-based tools
- On-demand verification requests are sent to insurers facilitating an immediate, accurate response as well as corrections
- Secure
- Lower cost, better performance for all customers
- Allows states to focus resources on the uninsured, rather than the insured



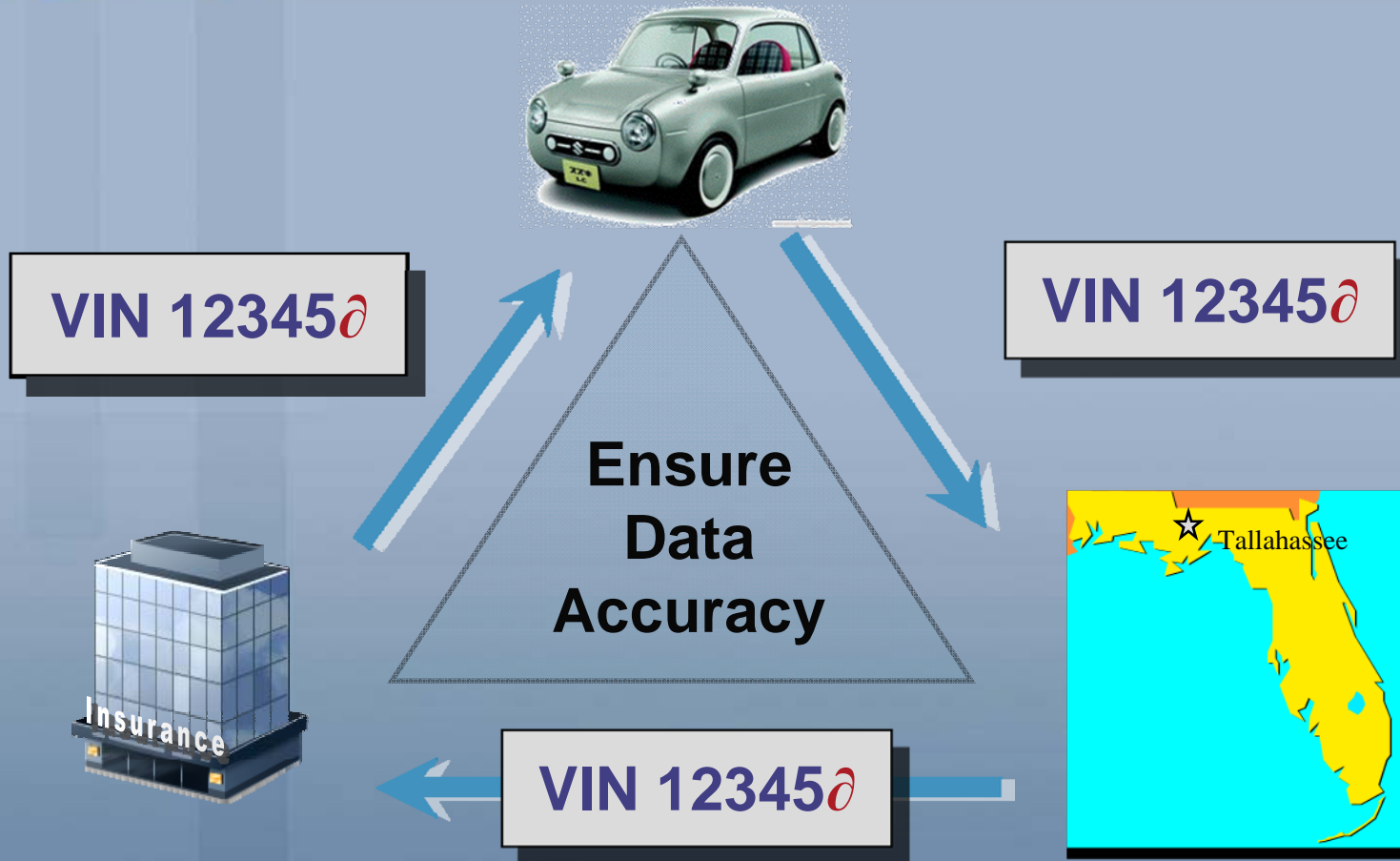


# The Web-based Model



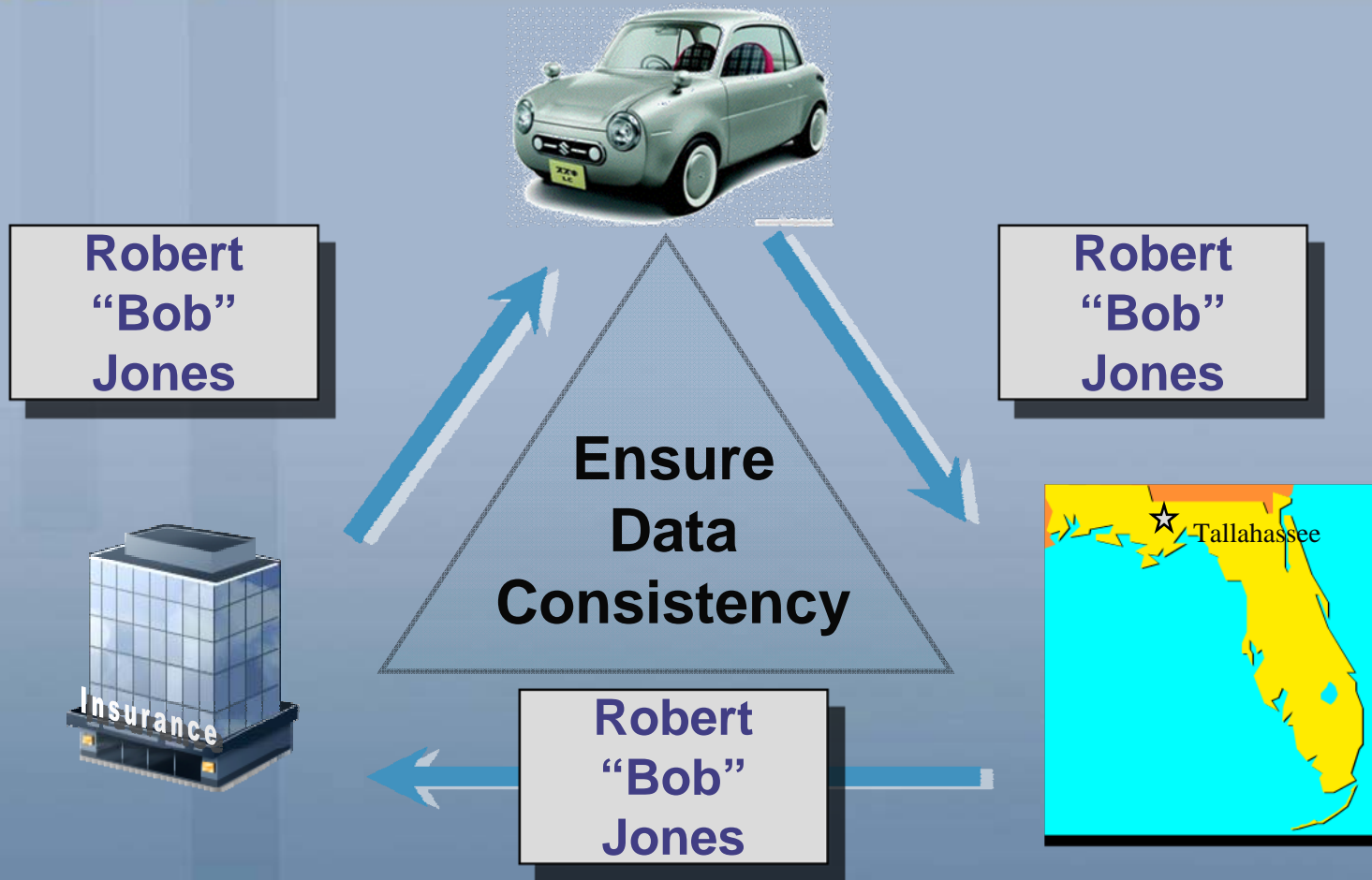


# The Web-based Model



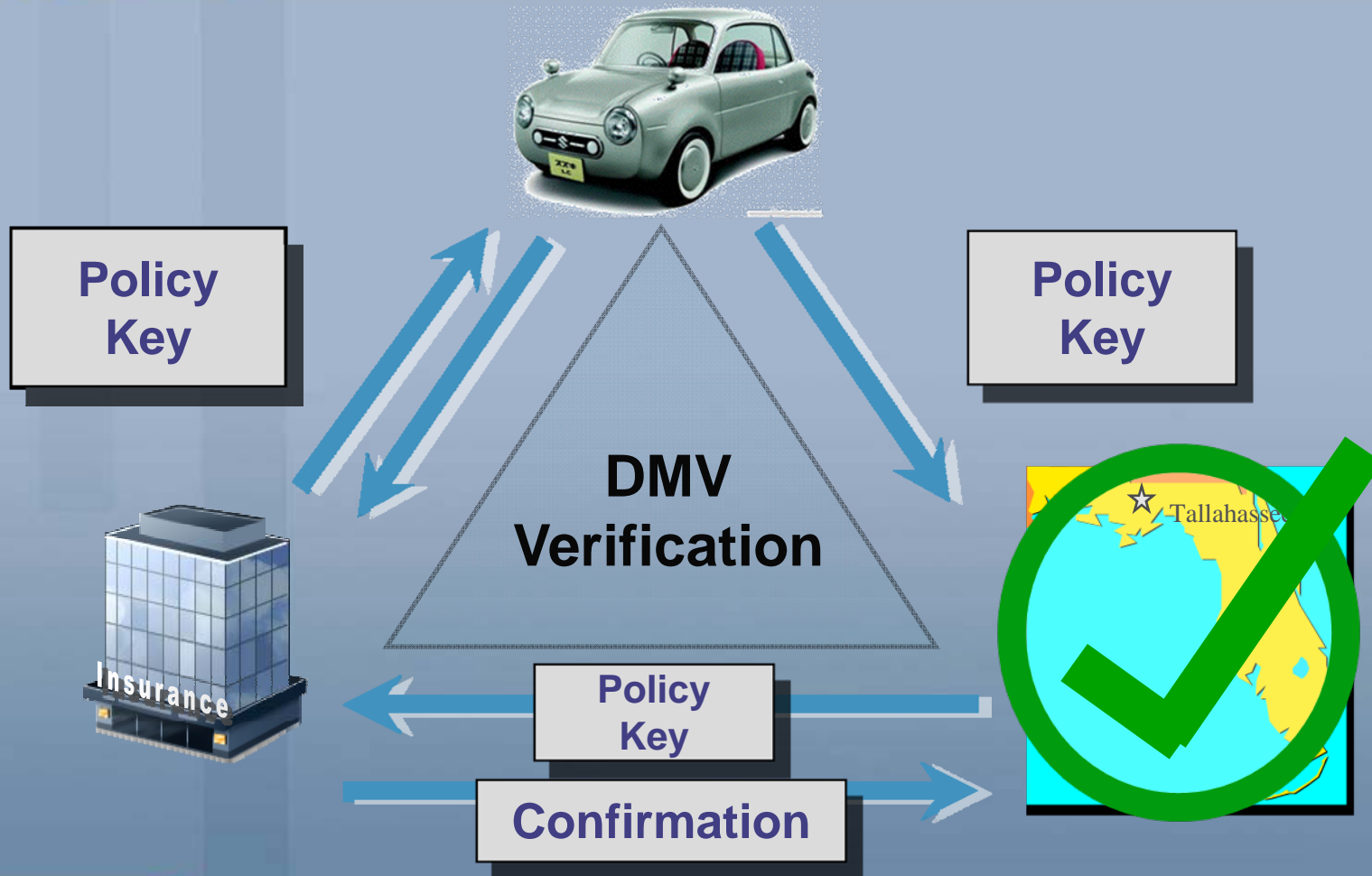


# The Web-based Model



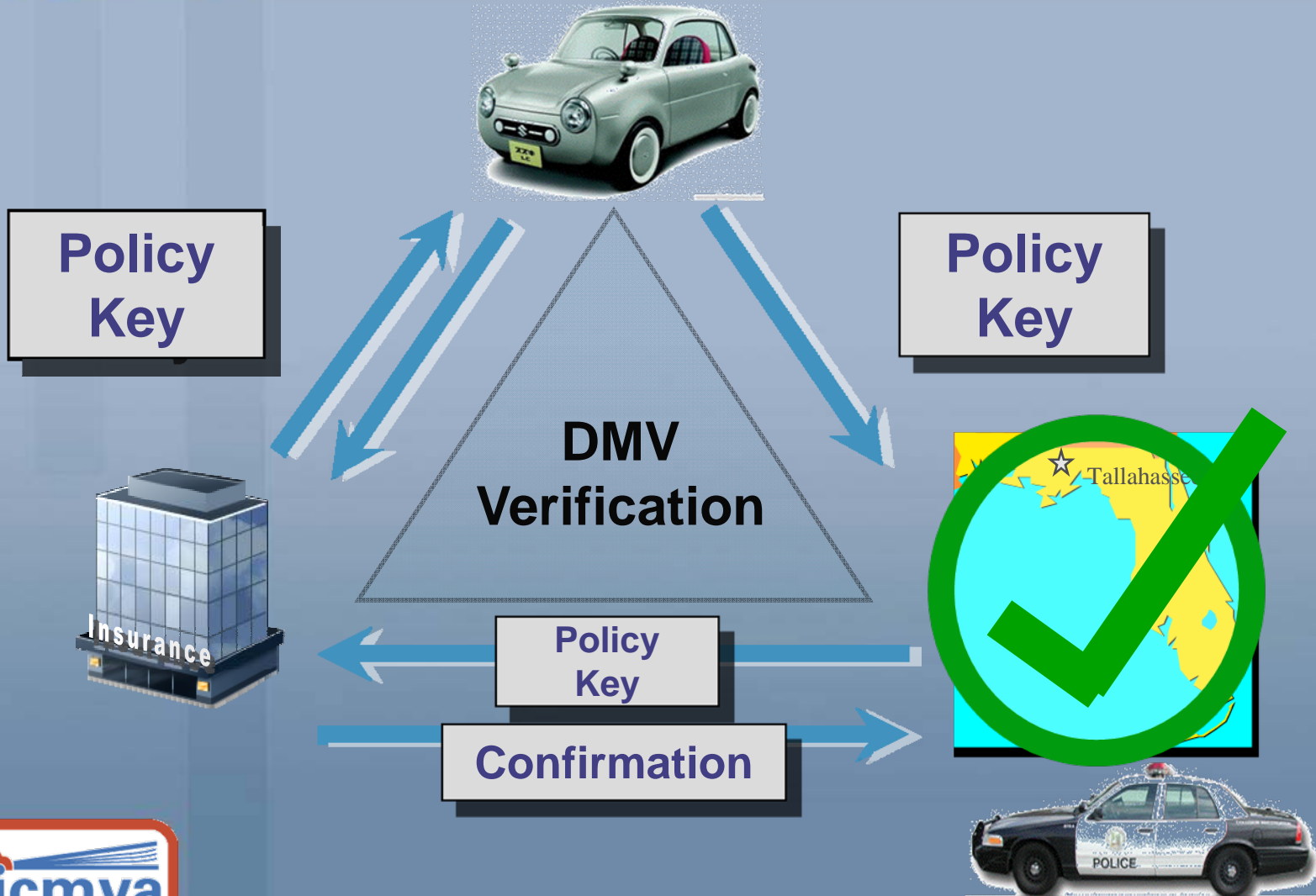


# The Web-based Model





# The Web-based Model





# The Technology

- Uses inexpensive internet connectivity
- Built on proven, web-based protocols (XML) widely in use
- Ensures secure transactions with SSL and user authentications
- Meets ANSI and ACORD standards



# The Benefits

- Real-time verification anytime
- Eliminates timely correction of data errors
- Ends creation and maintenance of another data repository
- Standardization means future advances are shared by all jurisdictions
- Bottom Line:

**Lower cost for a better system**



# For More Information:

- Visit [www.IICMVA.com](http://www.IICMVA.com)

- Questions? Contact:

Doug Traeger – IICMVA Vice Chair  
c/o USAA

9800 Fredericksburg Road

San Antonio, TX 78288

210-913-4499

[doug.traeger@usaa.com](mailto:doug.traeger@usaa.com)

