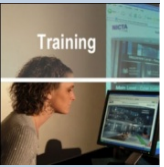


NATIONAL INSURANCE CRIME BUREAU

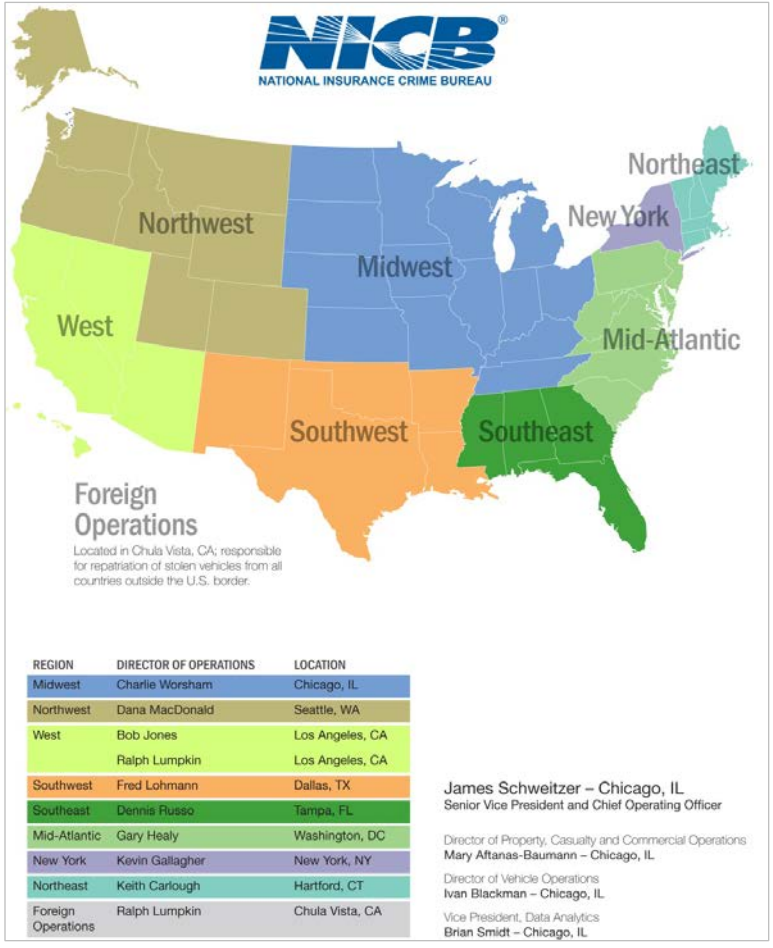
LATIFPA Conference

Fred Lohmann

Director of Operations

October 15, 2014

Regional Field Operations



REGION	DIRECTOR OF OPERATIONS	LOCATION
Midwest	Charlie Worsham	Chicago, IL
Northwest	Dana MacDonald	Seattle, WA
West	Bob Jones	Los Angeles, CA
	Ralph Lumpkin	Los Angeles, CA
Southwest	Fred Lohmann	Dallas, TX
Southeast	Dennis Russo	Tampa, FL
Mid-Atlantic	Gary Healy	Washington, DC
New York	Kevin Gallagher	New York, NY
Northeast	Keith Carlough	Hartford, CT
Foreign Operations	Ralph Lumpkin	Chula Vista, CA

James Schweitzer – Chicago, IL
Senior Vice President and Chief Operating Officer

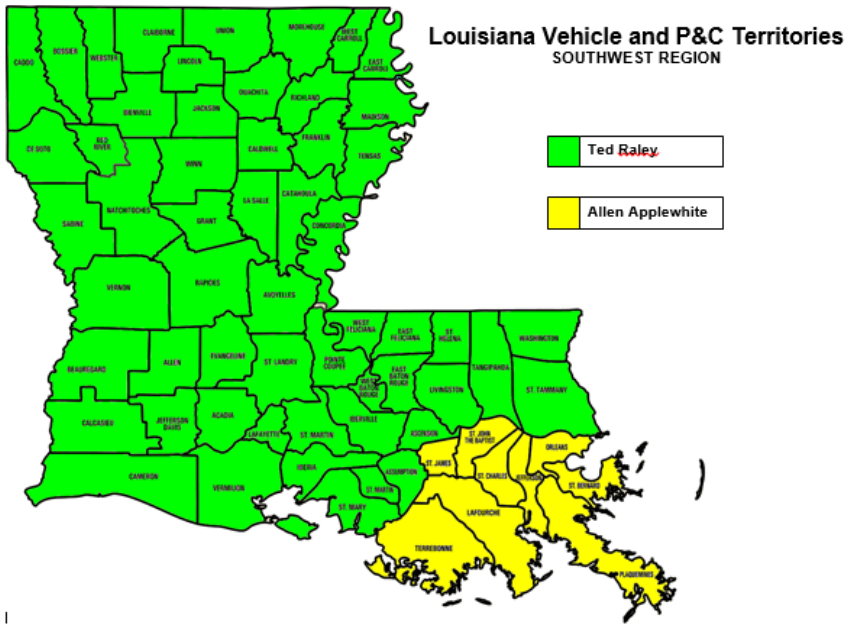
Director of Property, Casualty and Commercial Operations
Mary Aftanas-Baumann – Chicago, IL

Director of Vehicle Operations
Ivan Blackman – Chicago, IL

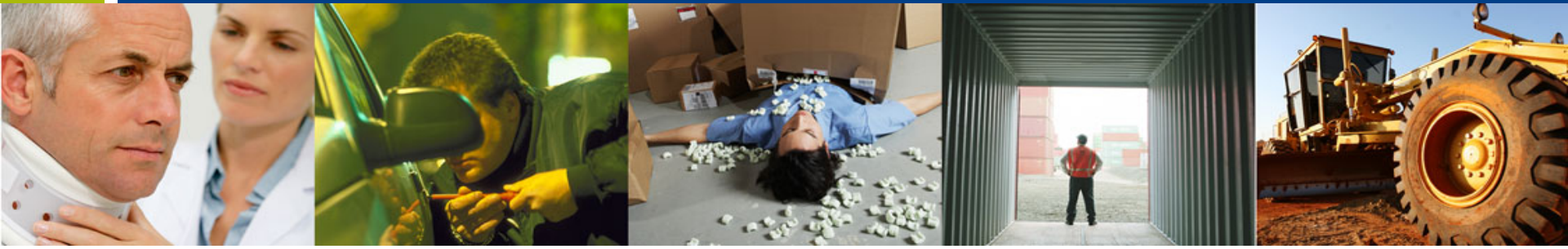
Vice President, Data Analytics
Brian Smidt – Chicago, IL

NICB Personnel in Louisiana

- Special Agent Allen Applewhite – Liaison – LSP – LDI
- Special Agent Ted Raley

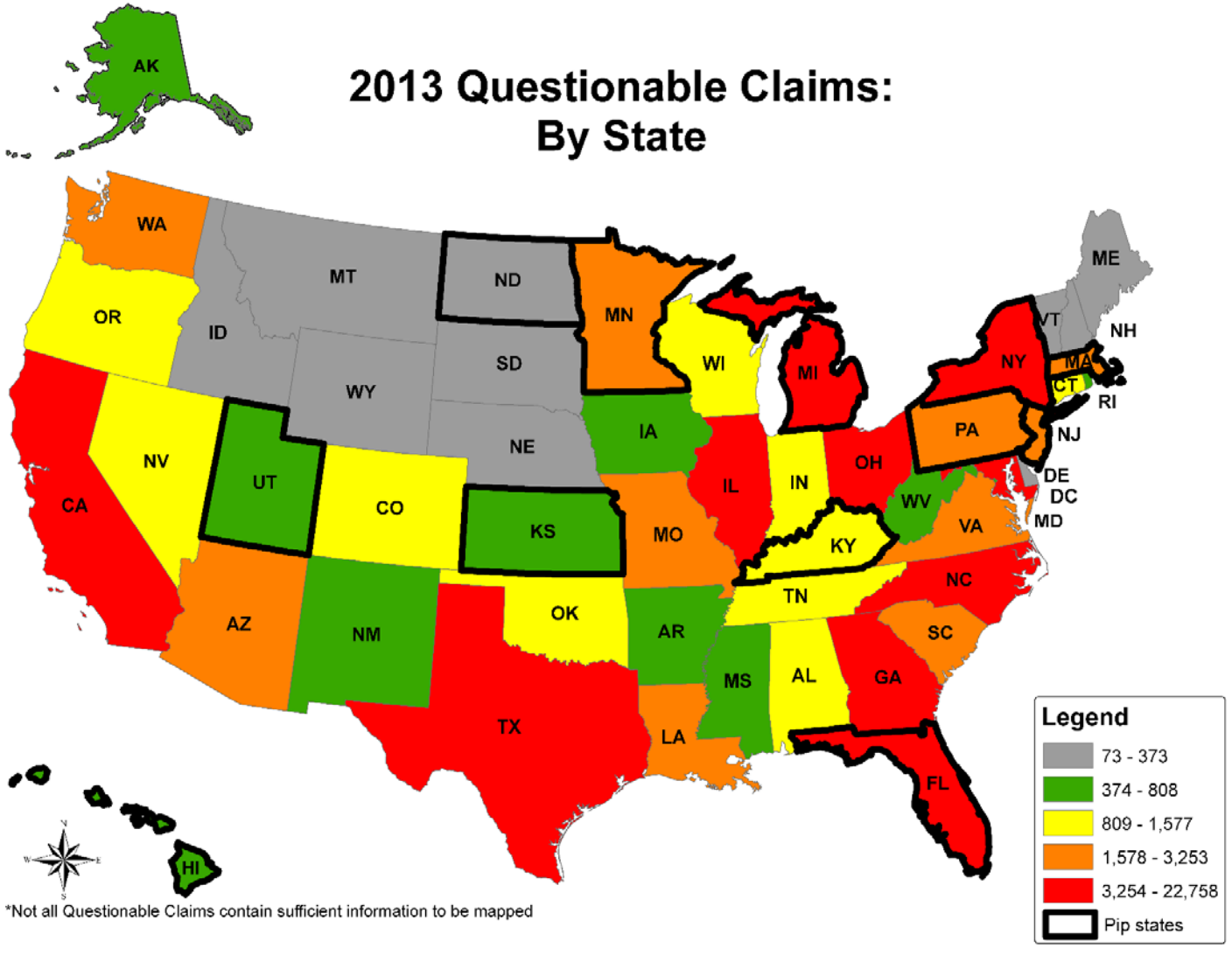


Priorities



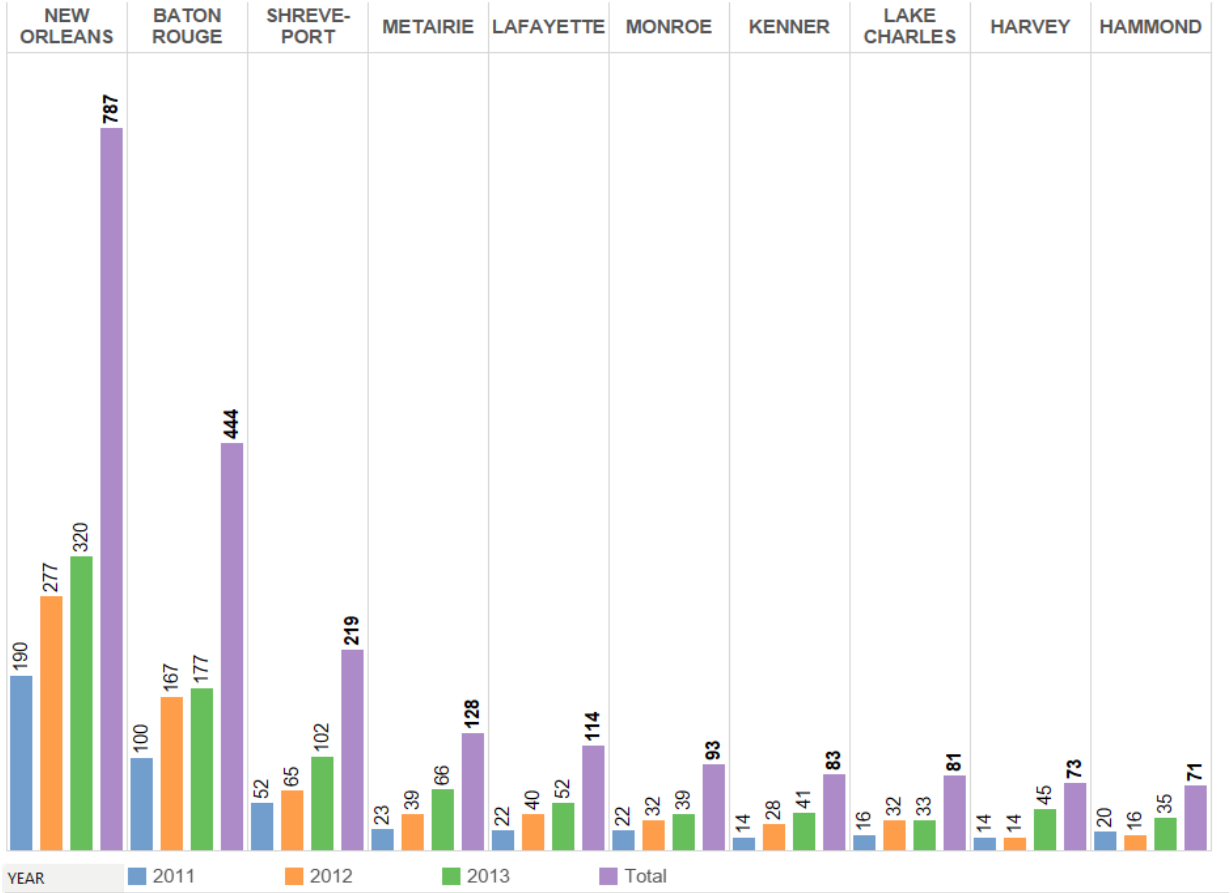
- Medical Fraud
- Commercial Fraud
- Vehicle Crime

2013 Questionable Claims: By State

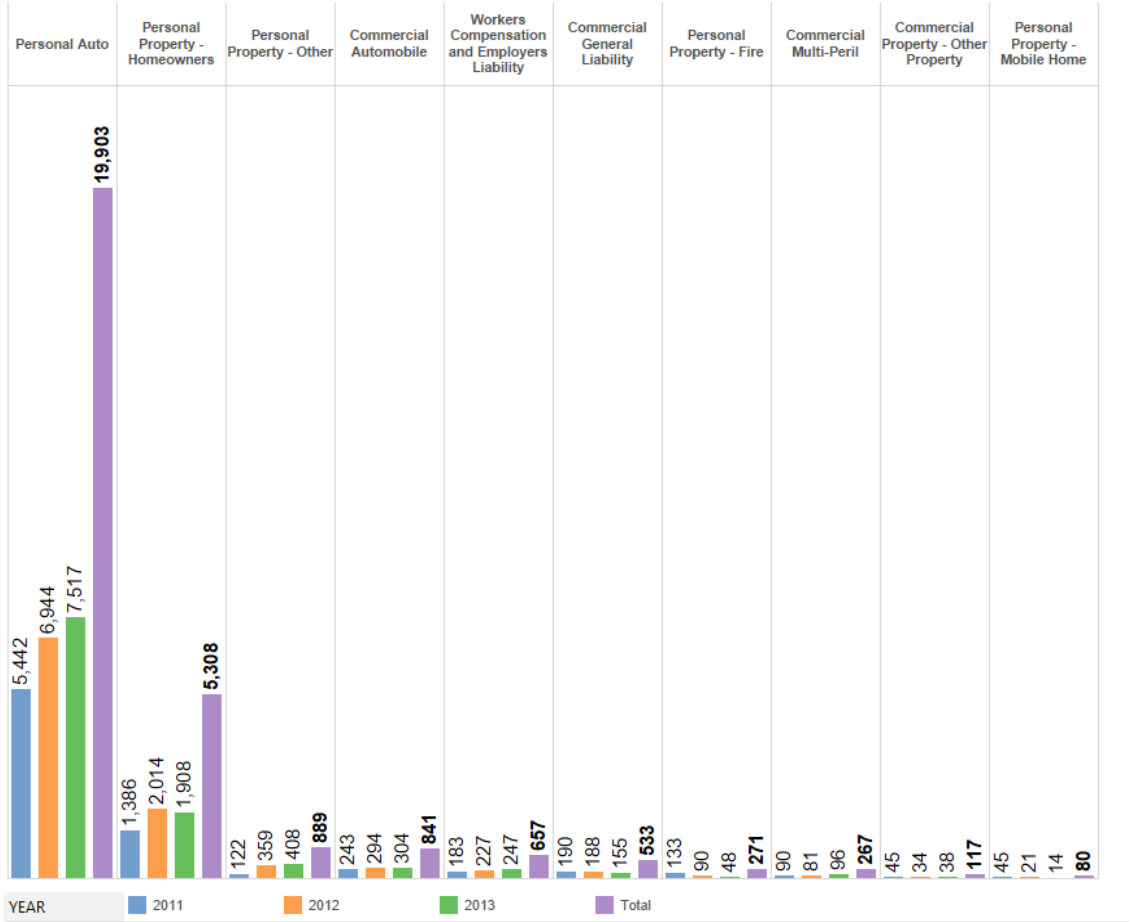


*Not all Questionable Claims contain sufficient information to be mapped

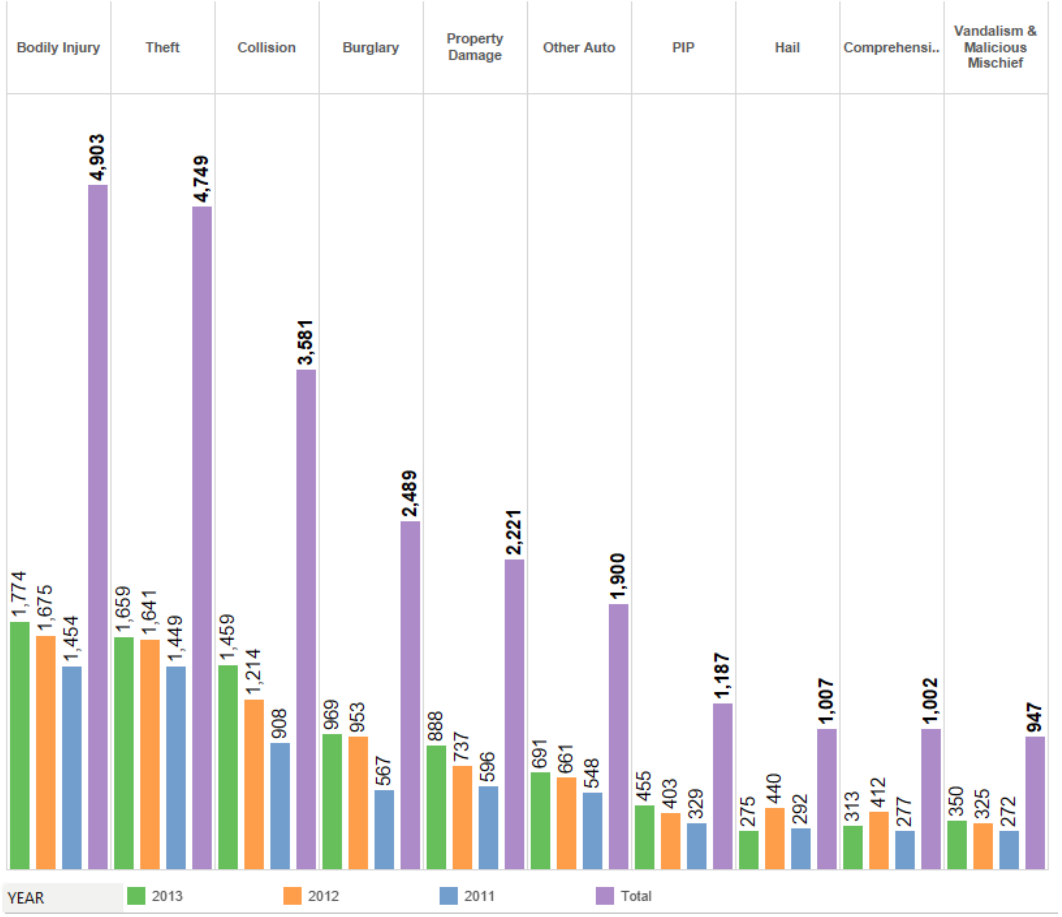
Total QC's Louisiana – (NO& BR)



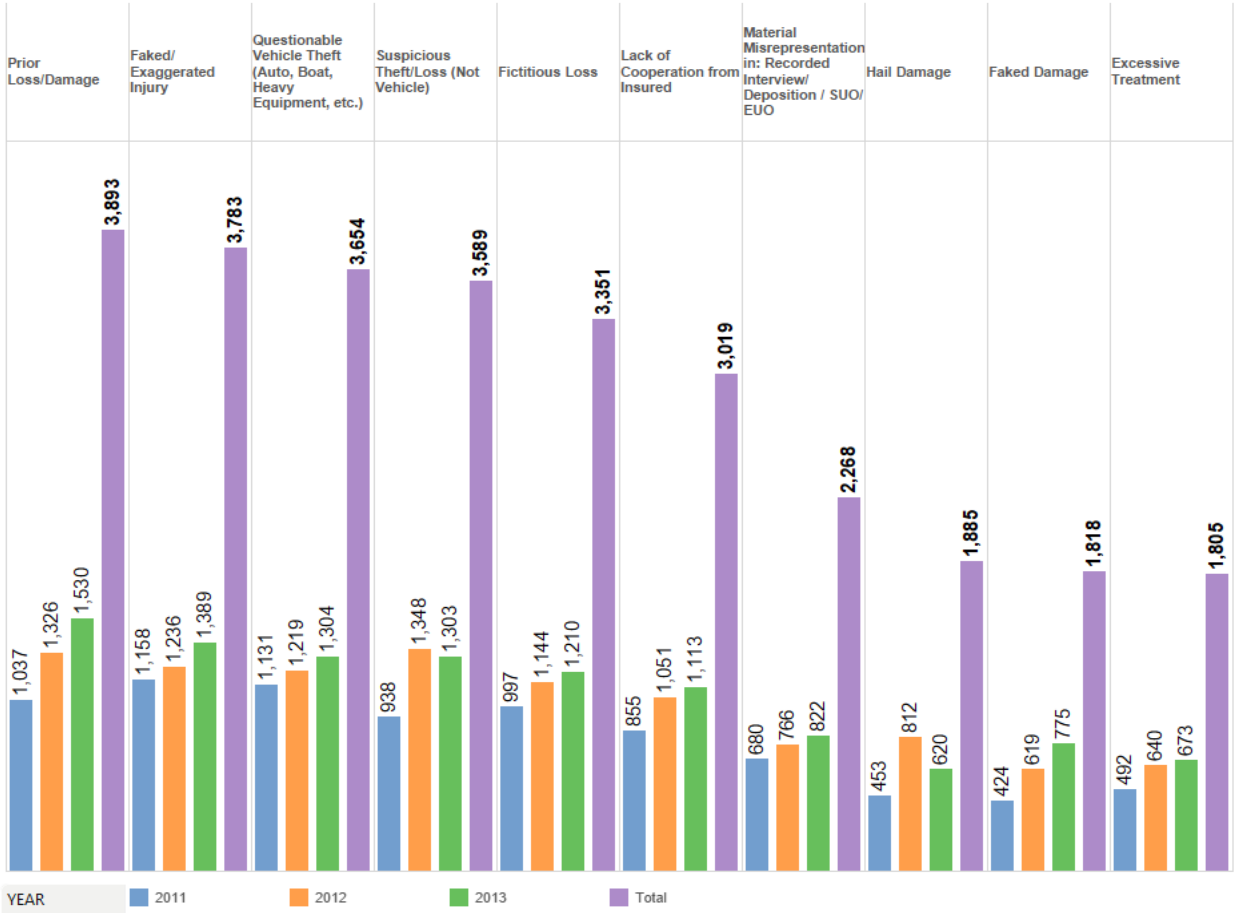
Policy Type – (Personal Auto)



Loss Type – (BI & Theft)



Referral Reasons

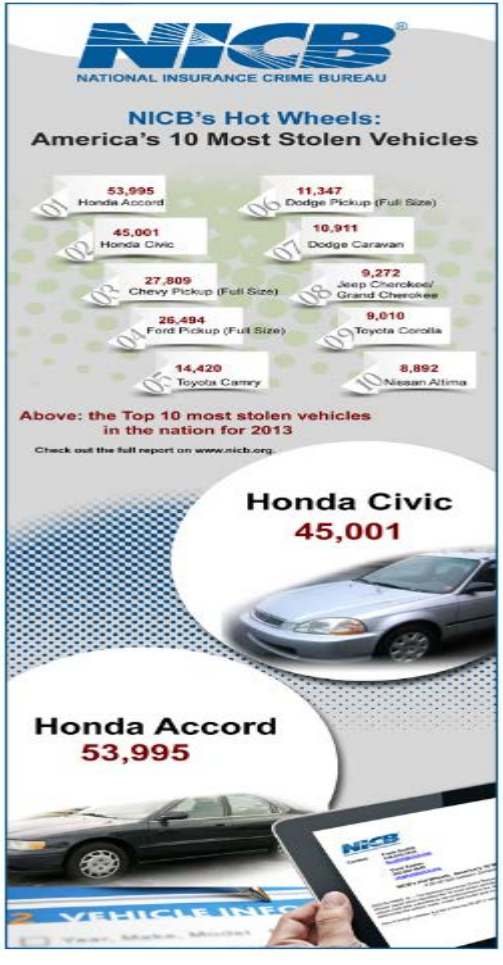


Louisiana "Hot Spots" 2013

2013 Rank	CBSA	MSA Name	2013 Thefts	2013 Rate
51	35380	New Orleans-Metairie, LA Metropolitan Statistical Area	3,763	303.23
87	29340	Lake Charles, LA Metropolitan Statistical Area	492	243.52
91	25220	Hammond, LA Metropolitan Statistical Area	301	240.01
106	10780	Alexandria, LA Metropolitan Statistical Area	335	216.47
120	33740	Monroe, LA Metropolitan Statistical Area	344	192.65
139	43340	Shreveport-Bossier City, LA Metropolitan Statistical Area	798	178.74
156	12940	Baton Rouge, LA Metropolitan Statistical Area	1,390	169.48
223	26380	Houma-Thibodaux, LA Metropolitan Statistical Area	278	132.45
240	29180	Lafayette, LA Metropolitan Statistical Area	588	122.73

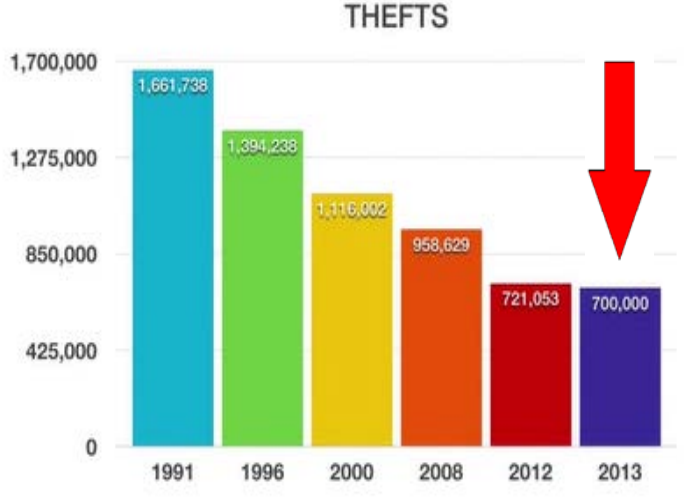
Louisiana "Hot Wheels" 2013

1		
	Chevrolet Pick-Up (Full Size)	1999
2		
	Ford Pick-Up (Full Size)	2006
3		
	Dodge Pick-Up (Full Size)	2001
4		
	Honda Accord	1995
5		
	GMC Pick-Up (Full Size)	1999
6		
	Chevrolet Impala	2008
7		
	Nissan Altima	2012
	Toyota Camry	2012
8		
	Chevrolet Tahoe	2001
9		
	Nissan Maxima	2006



Good News!

- FBI predicts a reduction in national vehicle thefts of 3.2 percent when final 2013 statistics are released later this year.
- FBI's preliminary 2013 vehicle theft estimates indicate thefts will be under 700,000—a number not seen since 1967 and a reduction in vehicle thefts of over 50 percent since 1991.



Why the decrease in thefts?

- Manufacturers Vehicle Anti- Theft Systems
- Public Awareness
- Vigorous & Effective Law Enforcement Investigation and operations

- *"The drop in thefts is good news for all of us," said NICB President and CEO Joe Wehrle. "But it still amounts to a vehicle being stolen every 45 seconds and losses of over $4 billion a year. That's why we applaud the vehicle manufacturers for their efforts to improve anti–theft technology and pledge to continue to work with our insurance company members and law enforcement to identify and seek vigorous prosecution of the organized criminal rings responsible for so many of these thefts."*

Emerging Threats - Vehicle Theft – ID / Finance Theft

- One of the newest schemes involves the use of stolen forms of identification.
- Crooks use stolen IDs to fraudulently lease or obtain loans to purchase new vehicles.
- Once they drive the vehicle off the dealer's lot, they skip out without ever making scheduled payments.
- Often, the cars are then sold to unsuspecting buyers after the Vehicle Identification Numbers (VINs) have been switched, or exported out of the country.
- Detroit, MI - Crooks used stolen IDs to fraudulently lease five vehicles worth more than $300,000 which they later planned to sell.
- Noticeable increase in this type of auto theft but no central database that quantifies these crimes.
- "Trying to put a number on these kinds of thefts is a challenge," said NICB President and CEO Joe Wehrle"
- Most of these thefts don't show up in traditional crime reporting numbers and become financial losses for lenders, car rental companies and others.

Port of Long Beach – Luxury Car Thefts

- 4,384 luxury class vehicles were stolen during the period covered by this report.
- Of the 4,384 luxury vehicles stolen, 713 remain unrecovered at the time of the report.
- Not all "hot" cars are boosted in the dead of night. Some are driven right off the showroom floor by people who appear to be legitimate buyers.
- Those thefts often involve financial fraud and don't wind up in the stolen car reports.
- http://www.consumeraffairs.com/news/car-thieves-favor-mercedes-benz-073013.html

Emerging Threats

Thieves defeat keyless entry to break into cars

Chris Woodyard, USA TODAY 6:12 a.m. EDT August 6, 2014

More thieves are using high-tech electronic devices to break through the keyless-entry systems that lock up modern cars, the **National Insurance Crime Bureau** reports.

The thieves are using electronic "scanner boxes" that allow them mimic the signal emitted by key fobs that open car doors with the click of a button, the NICB says.

Keyless Entry BMV

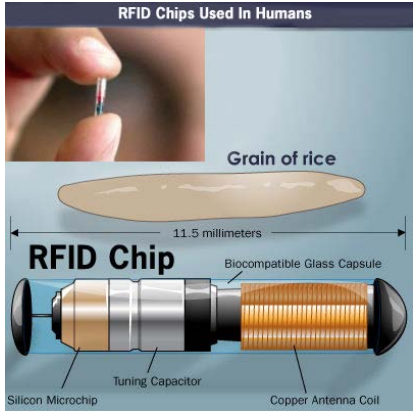
"Our law enforcement partners tell us they are seeing this type of criminal activity and have recovered some of the illegal devices," NICB CEO Joe Wehrle says in a statement. "And unfortunately, some of these devices are available on the Internet."

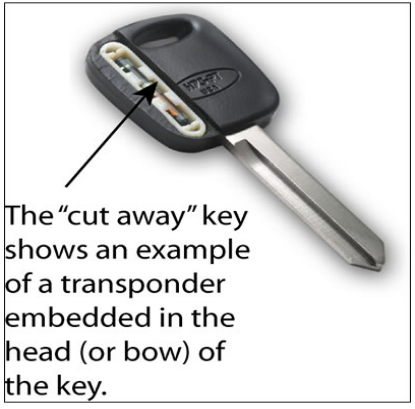
The phenomenon is coming on fast. It was only last year that police in Long Beach, Calif., asked for the public's help trying to identify three suspects wanted in connection with a series of auto burglaries. At the time, they used what police called "unknown technology" to gain entry to cars without the keys. Apparently now, it's known.

To protect themselves, consumers should take the usual precautions, like making sure they don't leave valuables in sight within their cars.

Passive Anti-Theft Ignition System

- Automobile manufacturers use magnetic coupled transponder systems.
- “Passive in nature” - No electricity or self power source
- Operate in the frequency range area of 125 kHz.
- Limited range of communication - 1 cm to 15 cm.
- Radio frequency can penetrate materials such as the plastic or rubber in the bow of a key.

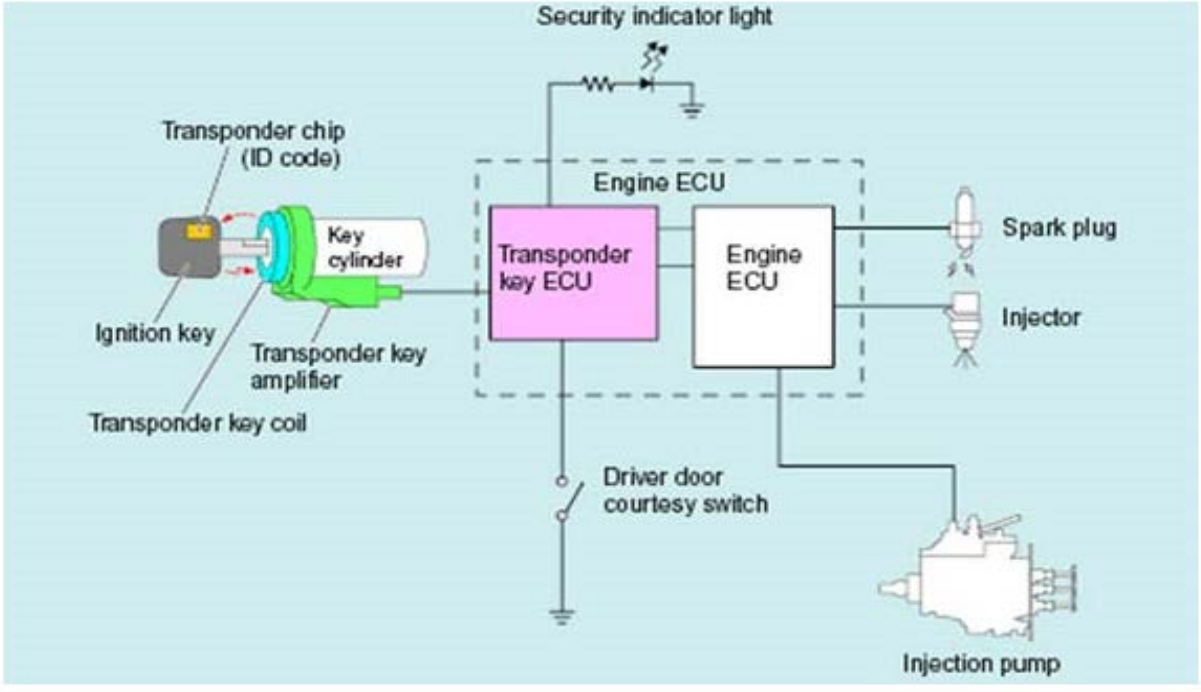



The “cut away” key shows an example of a transponder embedded in the head (or bow) of the key.

Passive Anti-Theft Ignition System

- Process of key identification is similar in most automotive transponder systems.
- Key is inserted into the ignition lock and turned to 'on' or 'run' position.
- Induction coil mounted around the ignition lock sends out electromagnet field of energy.
- Windings in the transponder chip absorb energy and power electronic chip to emit a signal.
- Signal is usually an **alphanumeric sequence** which is considered the identification code.
- Induction coil reads signal and sends it to ECU or other computer device to authenticate the signal.
- If signal is recognized in the computer's memory, signal is accepted and electronic components of vehicle permit starting of the vehicle or the continuation of engine operation.
- Note: Some immobilizer systems tend to remember last key code for so long that they **may** accept a **"non-transponder key"** even after a few minutes of taking out the original key from ignition.

System Diagram



Remote Keyless Entry Fobs

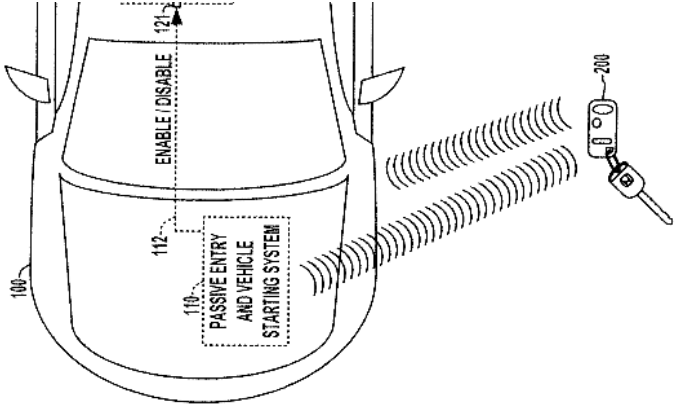
- Remote keyless entry fobs emit a radio frequency with a designated, distinct digital identity code.
- “Programming" fobs is a proprietary technical process, typically performed by the automobile manufacturer.
- Point of fact: It is the vehicle computer which is programmed in the process, not the fob itself.
- The general procedure is to put the car computer in 'programming mode'.
- Once in 'programming mode' one or more of the fob buttons is depressed to send the digital identity code to the car's onboard computer.
- The computer saves the code and the car is then taken out of 'programming mode‘.

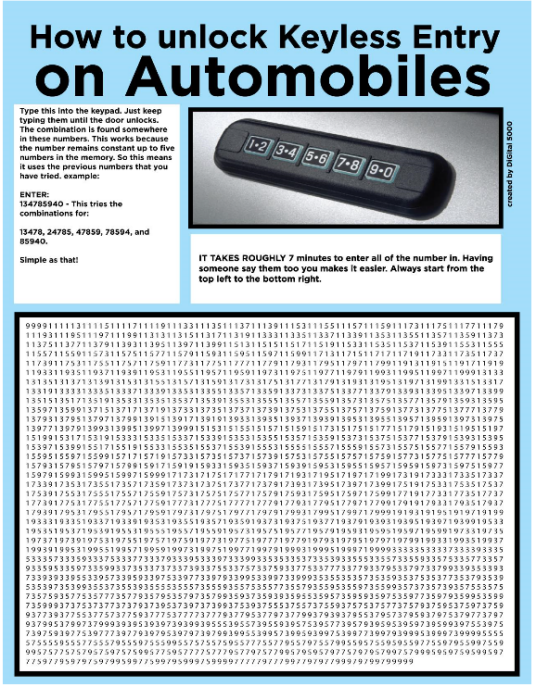
Keyless Entry Theft

- Researchers at ETH Zurich discovered encrypted signals easy to intercept and trick.
- The theft works by setting up two antennas, one near the targeted vehicle and one near the holder of the key fob.
- The person with the antenna aimed at the owner of the key fob needs to get within 26 feet of the target.
- Once the antenna is near the intended victim's key fob, the key transmits a low-power signal to the antenna, which is then relayed to the antenna near the vehicle.
- Once that occurs, the thief can unlock the doors to the vehicle.
- Swiss researchers hacked into eight car manufacturers' passive-entry systems using this method.
- No cryptology protocol could stop it.
- The "nasty aspect of high-tech car theft" is that it doesn't leave any sign of forced entry

Keyless Entry Theft

NATIONAL INSURANCE CRIME BUREAU





Transponder Key replacements

- After–market providers

http://www.youtube.com/watch?v=OkDqiZaZvBY

When in doubt?

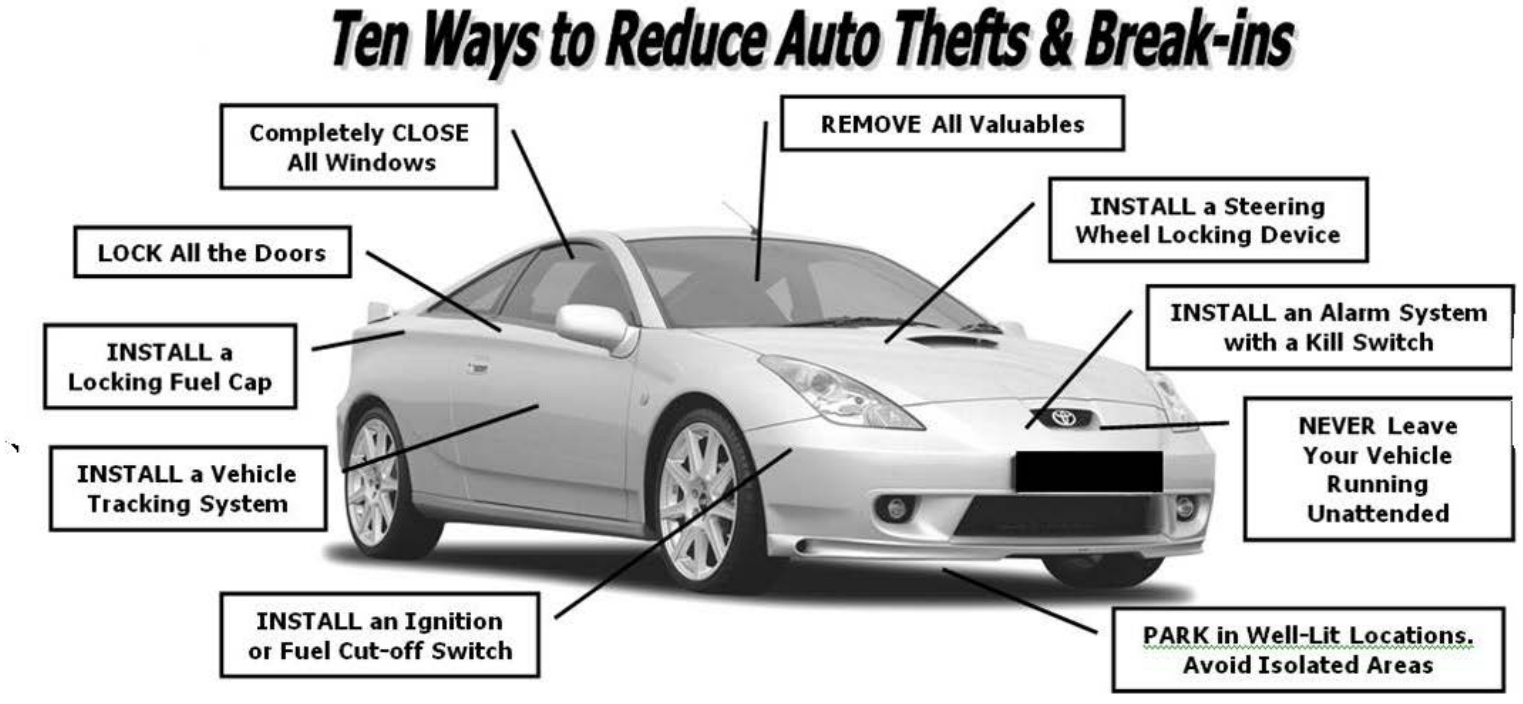
NICB
NATIONAL INSURANCE CRIME BUREAU

- Consider services of forensic locksmith
- Qualified interpreting and evaluating the effectiveness of transponder-based systems
- Insurance companies and police held out as the bad guys
- Misplaced trust in the integrity of transponder-based immobilizer systems
- Methods of theft evolve directly behind changes in technology
- While many forensic examiners, law enforcement officers, and insurance SIU personnel are familiar with the class characteristics of transponder systems, most are not familiar with the intricacies of the individual characteristics
- A qualified forensic locksmith/examiner, armed with the correct tools and experience, can retrieve data from the vehicle that provides clues as to the status of the vehicle at the time of last operation

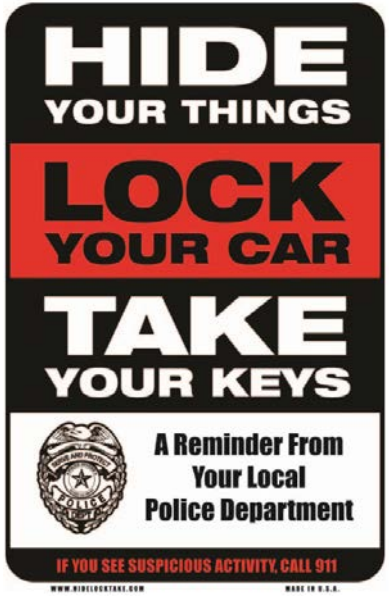
Transponder vehicles can be stolen

- **Ivan Blackman**, the manager of the Vehicle Information and Identification Program for the NICB, says that:
- “Insiders are gradually getting over their dogmatic belief in the invincibility of transponder systems”.
- “Companies are slowly realizing that the cars can be stolen,”
- “Most of the dogmatic belief in the invincibility of transponder systems, came from a lack of knowledge of these systems and how they operated”.

Strategies



Strategies – Public Awareness



Theft Prevention

1) Remove valuables from your vehicles and lock your doors.

2) Park in a well lit area.

4) Keep an eye and ear out for suspicious or unusual activity.

5) Call the police immediately (911 or 614-889-1112) if you witness a crime or if you witness something suspicious.

Support LATIFPA Bait Vehicle Operations

- Vehicles needed for participating LE agencies
- Deployed through NICB Vehicle Use Agreements, (VUA)
- Quarterly Reports – Performance Accomplishments
- Proven Results – Reduction in BMV Offenses
- Reduction in claims handling and claim losses
- Salvage items needed as "bait"

National Automotive Service Task Force

- **What is the VSP Registry**?
- Professional (VSP) Registry is a service created from the NASTF Secure Data Release Model (SDRM)
- Project of the NASTF Vehicle Security Committee.
- SDRM is a data exchange system conceived and designed cooperatively by automakers, the independent repair, insurance and law enforcement communities.
- Allows the aftermarket to access security sensitive information related to automobiles, i.e. key codes, PIN numbers, immobilizer reset information, and similar types of information.
- The NASTF VSP Registry program allows access to security-related information while protecting the safety and security of consumers and the integrity of automobile security systems.

Who should use the NASTF VSP Registry and why?

- USA-resident* locksmiths and service technicians qualified in vehicle security system repairs need a subscription to the NASTF VSP Registry in order to purchase security codes and VIN-specific computer files directly from the OEM/automaker.

- Most automakers/OEMs make this information available instantly from their websites

Parties Responsible for SDRM and the VSP Registry

- Committee (VSC), NASTF is responsible for bringing the parties together to identify and prioritize security information gaps and to help the Industry build and modify the systems necessary to close the gaps.
- The NASTF VSC has a standing Security Review Committee to manage disputes regarding enrollment in the Registry and access to security-related service information.
- Automakers: responsible to host service information websites and/or call centers that serve as the portal to security-related service information. A complete list of automaker website URLs is available on the NASTF website at the OEM Service Websites link.
- **NICB:** responsible to log transactions with automakers that involve security-related information. The National Insurance Crime Bureau protects consumers and automakers and also represents the insurance and law enforcement communities. NICB maintains transaction logs for all security-related information and provides forensic evidence to law enforcement to investigate automotive related crimes.

NASTF VSP Registry provides:

- Consumer choice by ensuring that vehicle owners can choose aftermarket service providers who have access to security-related information, tools and components.
- Control of security-related information and tools by the owners of these resources - the automaker and the consumer. No outside entity has access to or control of the manufacturer's/consumer's data without strict security protocol and oversight.
- Improved indemnity (compared to many current practices) for automakers from legal actions resulting from the unauthorized use, misuse, or illegal use of any security-related information.
- The NASTF VSP Registry ensures that responsibility for governance of independent repairers falls on the independent aftermarket service industry, not automakers.
- The NASTF VSP Registry also meets **insurance industry** expectations for security with respect to release of security-related information.

How it works:

- The NASTF VSP Registry provides safeguards to automakers and their customers to allow a change in the historic/customary practice of strict limitation of access to security-related service information, tools, and components to the aftermarket.
- Ability to identify stolen vehicles through NICB data analytics, ISO, NCIC, SDRM
- Investigative leads sent to NICB Special Agents & Law Enforcement Partners
- NICB - Vehicle Interest Notice – ISO Query – Contact Special Agent