IACP

International Association of Chiefs of Police

IACP Vehicle Crimes Committee

Vehicle Crimes Reference & Resource Guide

2017-2019

Emerging Technologies Working Group

Research Conducted from September 2017 through April 2019

Christopher McDonold—Vehicle Crimes Committee Chair

Paul Steier—Working Group Chair

TABLE OF CONTENTS

IACP

History

Mission

Members

Goals

Summary

Recommendations

Executive Summary

HISTORY: The Emerging Technologies with Vehicle Crimes Working Group commenced in September 2017 at the request of the IACP Vehicle Crimes Committee.

MISSION: To research latest technologies impacting vehicle crimes and to educate IACP members of these findings in order to enhance efforts to deter, detect, and prosecute vehicle crime activity.

MEMBERS: Working group Members were selected from membership within the IACP Vehicle Crimes Committee.

GOALS: The working group had three goals: research current and emerging trends used to perpetuate vehicle crimes; research tools and technology available to prevent, detect, and investigate these crimes; and effectively communicate these findings to IACP members.

SUMMARY: This working group referred to a variety of private and governmental resources to determine current and future technology trends. The working group focused on two areas for research as they were shown to be an emerging threat with the use of technology to commit vehicle crimes. These two areas were vehicle cybercrime and vehicle odometer fraud. Research results included information from the following areas: vehicle relay attacks, unauthorized access to vehicle infotainment and security systems, and illegal tampering of on-board diagnostic computers.

RECOMMENDATIONS: Although no solutions or resolutions to these vehicle crime threats was immediately clear, the working group recommends the use of the information and contacts contained within this guide to better prepare agencies to encounter these threats. The working group recommends that it continue to research technology threats with vehicle crimes as these undoubtedly will continue to develop.

Auto-ISAC (Automotive Information Sharing and Analysis Center):

An industry–driven community to share and analyze intelligence about emerging cybersecurity risks to the vehicle, and to collectively enhance vehicle cybersecurity capabilities across the global automotive industry, including light-and heavy –duty vehicle OEMS, suppliers and commercial vehicle section.

NHTSA - National Highway Traffic Safety Administration:

The National Highway Traffic Safety Administration is an agency of the Executive Branch of the U.S. government, part of the Department of Transportation. It describes its mission as "Save lives, prevent injuries, reduce vehicle-related crashes".

Auto—ISAC (Automotive Information Sharing and Analysis Center) - http:www.automotiveisac.com

Faye Francy, Executive Director ***Presentation Reviewed: Auto-ISAC Executive Overview, March 2018***

This presentation covers the risks of vehicle connectivity, managing risk and sharing information learned about cyber risks, and gives an overview of Auto-ISAC's role. Charts depict the flow of communication from numerous sources through Auto-ISAC's communication channels to members who are better prepared to identify threats, detect vulnerabilities, and validate risks. Best practice guides make members better prepared and trained to mitigate risks, respond to possible attacks, and provide threat protection. Auto-ISAC conducts monthly community calls where members and other interested parties can collaborate on current trends and share contacts and resources.

Email: Faye Francy—Fayefrancy@automotiveisac.com / Phone: 703-861-5417
Kim Kalinyak—kimkalinya@automotiveisac.com / Phone: 240-422-9008 / Membership Lead

NHTSA—National Highway Traffic Safety Administration

Presentation Reviewed: Cybersecurity for modern vehicles, October 2016
Author: NHTSA

NHTSA's guidance to motor vehicle manufacturers for improving motor vehicle cybersecurity includes security controls, information sharing , vulnerability reporting, cybersecurity protections and vehicle communications. Monthly community calls where members and other interested parties can collaborate on current trends and share contacts and resources.

Publication/Research Reviewed: An Overview of NHTSA's Electronics Reliability and Cybersecurity Research Programs, (publish date unknown). Authors: Arthur Carter, David Freeman, and Cem Hatipoglu

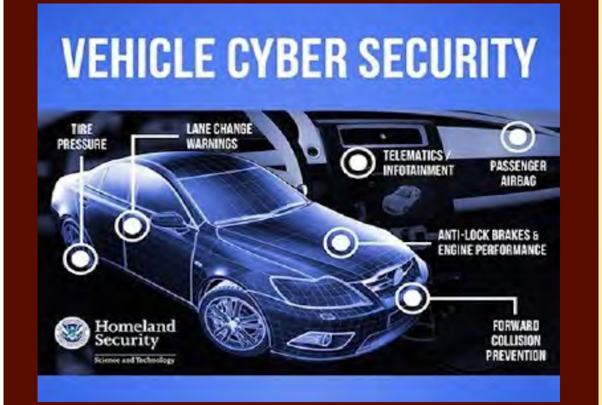
In this summary of NHTSA's research programs related to electronic vehicle control systems and automotive cybersecurity, the cybersecurity focus is on: protection of vehicular electronic systems, communication networks, software, users, data from malicious attacks, unauthorized access, and manipulation. Primary goals of NHTSA's electronics reliability and automotive cybersecurity programs are to establish an automotive cybersecurity knowledge-base, develop voluntary industry standards and best practices, foster the development of new system solutions, and identify performance standards or principles for electronics reliability / cybersecurity.

Presentation Participated in: Modern Vehicles & Cybersecurity Research— October 2017 Author: Cem Hatipoglu

This presentation was an overview of vehicle technology innovations, cybersecurity risks, vulnerabilities, research, resources, best practices, and industry efforts.

Cybersecurity vulnerability, as depicted by a modern vehicle's attack surface, increases as the vehicle's technology becomes more sophisticated.

Heidi King, Deputy Administrator of the National Highway Traffic Safety Administration, speaking at the 2018 Billington Automotive Summit in Detroit, Michigan.



Vehicle Hacking has become a major problem across the globe. Hackers have the ability to threaten not just lock systems, but dozens of electronic systems which are becoming more and more common.

Cem Hatipoglu, NHTSA Director of Vehicle Crash Avoidance and Electronic Controls Research.

November 7, 2017

Cem discussed the presentation *"Modern Vehicles & Cybersecurity Research".* Cem explained cyber security concerns have been in existence since software has been on vehicles. Today there is more of a concern for cyber security since technology is more prevalent, easier to replicate, and knowledge is shared more readily. The primary focus of this NHTSA research team: cyber risks that affect highway safety and critical systems (safety critical systems). Other topics discussed but not immediately addressed by this team include: data, privacy, and vehicle unlocking and starting. Cem further identified that cybersecurity is looked at for possibly crash causation but he was not aware today of cybersecurity leading to critical outcomes in the real world. In 2015 there was a recall related to Fiat Chrysler that presented an unreasonable risk to safety. There are some reports of cybersecurity hacking and potential risks that NHTSA analyzes to see if an unreasonable risk to safety exists. FBI cybercrime and U.S. Homeland Security are looking at other areas of criminal cybercrimes.

Email: cem.hatipoglu@got.gov

Rob Heilman—NHTSA Division Chief, Electronic Systems Safety Research

Dan Kenney—NHTSA Special Agent, Office of Odometer Fraud Investigation

Paul Steier held a conference call with Rob Heilman and Dan Kenney. Rob's office is researching three areas: automated vehicle policy, crash worthiness, and crash avoidance. They are studying a vehicle with respect to the areas of : USB connectivity, Bluetooth, phone connectivity, event data recorders, virus attacks, and how quickly a virus can spread to other vehicles. Rob encouraged connections with the National Domestic Communication Assistance Center (NDCAC) for law enforcement sharing of technology information.

Rob is leading development of a NHTSA white paper to educate the public on what to do if their vehicle is cyber attacked but no law enforcement educational information has been published yet. They would like to see how IACP can be utilized to educate law enforcement and agree there needs to be a common forum for law enforcement to report vehicle cybercrime incidents. A large scale vehicle cyberattack is a possibility and the quicker information is passed along to proper authorities and experts the sooner countermeasures can be put in place.

Email: Robert.heilman@dot.gov / Phone: 202-366-2730
Email: Daniel.kenney@dot.gov / Phone: 202-366-0821

Also mentioned as a source: The National Cyber-Forensics and Training Alliance *https://www.ncfta.net*

The NICB (The National Insurance Crime Bureau) is a North American non-profit membership organization located in Des Plaines, Illinois. It was created by the insurance industry to address insurance-related crime and works closely with law enforcement.

MOS Devices and Vehicle Crime as vehicles become more and more digitally connected, new avenues for criminal activity are opened. German researchers used handheld radio devices to unlock vehicles by makers such as Audi, BMW, Volkswagen, Mitsubishi, and Toyota. The way these devices work is by imitating the radio signals which ignite the a vehicle's wireless entry system. The hackers are then able to gain access to vehicles from as far as 300 feet away.

Cyber crime is a global problem that is emerging for police globally as criminals adapt to new technology. During 2017, damages in Europe amounted to over a billion Euro as a consequence of vehicle hacking. In May 2019, a ring of car thieves were implicated in over 14 million Euro robberies involving 261 stolen vehicles. There is also a growing problem in South Africa with criminals hacking luxury vehicles and employing them in high stakes heists.

Paul Burnley—Director, Adrow Ltd.
On-line presentation conducted September 13, 2018 (Continued)

Paul discussed replicating hard keys, replicating key chips, key transponder cloning, key emulation and use of OBD port, immobilizer override, and relay attacks. Key emulation is the newest emerging technology. Paul explained how wireless vehicle attacks will soon be the method of choice as it's the fastest and most efficient. These newest attacks allow the criminal to steal items from inside the car or just car parts more efficiently. Also, criminals don't need to be as close to the vehicle and can start the vehicle at a later date. Europe has seen a high spike in the past three to six months in the use of relay attack tools. Key programming is the most prevalent method of relay attack used in Europe and they are not only used for passenger vehicles but for stealing commercial vehicles as well.

Email: paul@adrow.co.uk / Phone: +44-7958-215618

General Motors (GM)
George Baker—GM Global Vehicle Security Lead
General Motors Vehicle Security Reference Card

George and his global vehicle security team have designed a reference card to educate law enforcement on many areas of vehicle security while providing resources and contacts. Areas covered on the resource document include: vehicle identification, odometer fraud investigations, counterfeit parts investigations, stolen vehicle assistance, cybersecurity, and outside GM investigative resources. George is GM's primary liaison to law enforcement.

Email: George.baker@gm.com / Phone: 248-515-0673

National Insurance Crime Bureau (NICB)
Rusty Russell—NICB Director, Vehicle Operations

Rusty has expertise in vehicle relay attacks and devices used to perform such attacks. He is a leader of NICB investigative efforts involving vehicle crime prevention, investigation, and education.

Email: drussell@nicb.org / Phone: 847-544-7042

American Association of Motor Vehicle Administrators (AAMVA)
Cathie Curtis – AAMVA Director of Vehicle Programs
Autonomous Vehicle Reference Library

AAMVA has an extensive library of autonomous vehicle information based on research developed by the Autonomous Vehicle Best Practices Working Group and the Autonomous Vehicle Information Sharing Group. This library includes information related to the development, design, testing, use, and regulation of autonomous vehicles and other related emerging technologies.

Email: ccurtis@aamva.org / Phone: 207-395-4100
https://www.aamva.org/Autonomous-Vehicle-Information-Library/

The United States Department of Justice (DOJ) also known as the Justice Department is a federal executive department of the U.S. government, responsible for the enforcement of the law and administration of justice in the United States. The department was formed in 1870.

The Federal Bureau of Investigation is the domestic intelligence and security service of the United States, and its principal federal law enforcement agency. The FBI has jurisdiction over violations of more than 200 categories of federal crimes.

Adrow works with vehicle manufacturers, security system suppliers, insurers, semi conductor manufacturers and others to help them understand the latest theft techniques and advise them how to design-out some of the weaknesses exploited in contemporary vehicle security systems.

U.S. Department of Justice and FBI

NDCAC National Domestic Communication Assistance Center

https://ndcac.fbi.gov/ (See brochure)

NDCAC provides a central hub to law enforcement for technical knowledge management that facilitates solutions with the communication industry. Areas for law enforcement to collaborate on include technology information sharing regarding vehicle cybersecurity. NDCAC also provides training to law enforcement on vehicle intelligence data recovery and analysis.

Supervisory Special Agent Paul Mueller
Email: psmueller@fbi.gov / Phone: 540-361-2450
Supervisory Special Agent Evan Nicholas, Operational Technology Division
Email: emnicholas@fbi.gov / Phone: 540-361-2460

FBI Cyber Division
Edward Parmelee, Supervisory Special Agent

Ed is the law enforcement point of contact for Auto-ISAC. Paul Steier visited with Ed about the working group and vehicle cyber security law enforcement outreach. Ed recommended NDCAC for law enforcement liaison and technology sharing information related to vehicle cybercrimes. Ed is aware of the need to educate law enforcement on the topic of vehicle cybersecurity and will keep IACP in mind in the future as an avenue of outreach.

Email: emparmelee@fbi.gov/ Phone: 703-633-4388

Other Contacts

U.S. Government Accountability Office (GAO)
Publication Reviewed: Vehicle Cybersecurity—DOT Industry Have Effort Underway, but DOT Needs to Define Its Role In Responding to a Real-World Attack

This research looked at vehicle cybersecurity threats and vulnerabilities to determine impact and capabilities of vehicle cyberattacks. This was directed at the preparedness of the U.S. DOT in regulating how the vehicle manufacturing industry is deterring and preventing such attacks. This publication does mention the value of the Auto-ISAC but points out that the DOT needs to determine what its role will be in addressing vehicle cyberattacks.

Paul Burnley—Director, Adrow Ltd.
On-line presentation conducted September 13, 2018

Paul has conducted extensive research in vehicle relay attacks and advanced methods in Europe. His presentation started with the history of vehicle attacks to gain entrance to/break into vehicles. He discussed mechanical devices and manual manipulation and tools to prevent cars with remote locks from locking. Devices to jam vehicle GPS programs was discussed which can cut use of telematics systems from reporting GPS locations. He also discussed the cloning of key fob signals and key code grabbing. These tools are difficult to detect and can cause law enforcement to believe the key fob was left in the vehicle upon theft. Paul discussed several examples of seized relay attack devices that law enforcement in Europe have confiscated. These devices continually are smarter and more effective in infiltrating a vehicle. However, the most common vehicle entry method by criminals today is to manipulate the door lock or break the window. As technology improves, becomes more readily available and affordable, there will be continued movement to using more sophisticated tools to gain vehicle entrance and control. Paul also discussed how engine start methods have evolved and provided examples of confiscated tools.

THE LEAD *is* an e-newsletter delivered to IACP members daily and is a collection of law enforcement related news stories published by news outlets around the globe. The lead is a members only benefit for IACP members. Through The Lead you can gain critical awareness of global news and issues relevant to law enforcement, view online resources including model policies, training keys, reports and other tools to assist you in your daily operations.

In 2019, OVER 143,000 STOLEN CARS WERE IDENTIFIED BY INTERPOL

THROUGH THE USE OF THE SMV DATABASE 130 COUNTRIES SHARED THEIR VEHICLE THEFT DATA, CREATING A DATABASE WHICH HAS ALREADY GARNERED 256 MILLION SEARCHES BY LAWENFORCEMENT GLOBALLY

OTHER ACTIVITES

IACP—The Lead Article

Published by IACP: January 29, 2018

Virginia Man Causes $550,000 in Losses Through Odometer Scam

The Hampton Roads (VA) Virginian-Pilot (1/25) reported a Virginia man pleaded guilty on Thursday to conspiring to "roll back the odometers of more than 50 vehicles before selling them to used-car dealerships and others, according to court documents." According to court documents, the scheme ran from September 2010 through October 2016. To conceal the scheme, the suspect "would sometimes pose as a used-car dealer while buying the vehicles and give an alias, documents said." He would then "direct the sellers not to write their vehicle's mileage on the title," and would then "roll back the odometer and fill out the document with the false reading" before applying for and securing a new title. The article mentioned that the suspect's fraud resulted in "$250,000 to $550,000 in losses." In the United States alone, 1.5 million vehicles have tampered odometers, and crimes such as that discussed in the article total a billion dollars in damages annually according to the NHTSA.

Conference: 2nd Billington Automotive Cybersecurity Summit, Detroit, MI
August 3, 2018
https://www.billingtoncybersecurity.com/2nd-billington-automotive-cybersecurity-summit/

This conference was attended by working group members Holly Merz, George Baker, and Paul Steier. The following bullet points highlight key points of the summit. For a list of presenters visit the link above.

- A quarter billion connected cars estimated by 2020; *Gartner*. The human factor is still the biggest threat in the cyber chain.

Constant cyber software updates and patching are critical but will consumers perform them and at what cost?

- Tier 1 and 2 suppliers need to have their products cyber protected but who pays for it and monitors it? Who will be responsible for solving problems as they arise?

Do state and federal laws address cyber hacking of vehicles?

- There is a substantial security threat when mechanics connect to vehicles for diagnosis and repair. This may leave a vehicle vulnerable for cyber-attack. Ransomware attacks are also a threat to vehicles.
- Safety, trust, and privacy are the three main elements in cyber protection. Laws need to address this and the public must be more aware of these threats.
- Lack of knowledge and training among corporate leaders in cybersecurity threats is a concern. Many may not see value in spending money/resources on cyber protection.
- Real time operations management for vehicle cyber threats is important for good cyber hygiene. When a threat is uncovered it must be stopped immediately. Who is responsible? What is the law enforcement response?

Billington Automotive Cybersecurity Summit,

Detroit, Michigan, 2018 discussion about autonomous vehicle security and technology.

Odometer fraud is the disconnection, resetting, or alteration of a vehicle's odometer with the intent to change the number of miles indicated. NHTSA estimates that more than 450,000 vehicles are sold each year with false odometer readings. This crime costs American consumers more that $1 billion annually according to the NHTSA.

Conference: 2nd Billington Automotive Cybersecurity Summit, Detroit, MI August 3, 2018 (Continued)

- Autonomous Vehicle technology is substantial lifesaving technology but is designed by humans. The driving danger will move from operator error to programming error. We still have human involvement which makes technology vulnerable. Highly Autonomous Vehicles (HAV) concerns are the use of them as mass weapons.
- Substantial effort in cyber security is needed with constant, timely updates and patches.
- Auto-ISAC does table topic exercises and vulnerability testing for vehicle cyber threats. This is a good resource for law enforcement to learn more about vehicle cyber threats.
- Is there value to include five star ratings for cyber security? Public may not care and it's difficult to measure as it is fluid: good protection today, not tomorrow.

Webinar September 6, 2018: Odometer Fraud Investigations.
Presenters: Holly Merz, Investigator - Iowa Attorney General's Office. Dan Kenney and Kevin Porter, Special Agents, NHTSA Office of Odometer Fraud Investigation.
Host: American Association of Motor Vehicle Administrators (AAMVA) – 89 attendees

This webinar provided training and information on the scope of odometer fraud, latest technology used to commit odometer fraud, and provided investigative tools and resources to investigate odometer fraud. Case examples were reviewed and participants gained knowledge and insight into how this growing vehicle crime impacts their communities. The use of On-board Diagnostic tools to change vehicle mileage was discussed as the reason that has caused this crime to grow.

Holly Merz: Email: Holly.Merz@ag.iowa.gov / Phone: 515-281-7686
Dan Kenney: Email: Daniel.kenney@dot.gov / Phone: 202-366-0821
Kevin Porter: Email: kevin.porter@dot.gov / Phone: 816-329-3911

IACP—The Lead Article
Published by IACP: February 21, 2019
Jackson Mississippi father and son sentenced for odometer fraud

FWJTV-TV Jackson, MS (2/19, Christopher) reports from Jackson, Mississippi, "A Jackson father and son were sentenced to prison in a large scale vehicle odometer roll back scheme." Mark Longgrear, 54, "was sentenced to almost five years in prison, while his son, 29-year-old Zachary Longgrear, was given almost two and a half years in prison by United States District Judge Carlton W. Reeves." According to WJTV-TV, "The two men committed securities fraud and conspired to reset and change the odometers of motor vehicles, leading to customers being given false statements relating to odometers." From 2014 "through at least February 2018, the Longgrears, both individually and under their company Southern Auto Buyers LLC, bought late model, high mileage vehicles from numerous sources, and then illegally changed the odometers to show lower mileage," and "some of these rolled-back vehicles were later sold to consumers in the Mississippi area and elsewhere."

OTHER RESOURCES:

- ***Kraig Palmer—Graylane, LLC. Current California Highway Patrol Officer***

  Officer Palmer works in the San Diego Regional Auto Theft Task Force (RATT). He has experience and conducted research in vehicle key code (relay) attacks. He is knowledgeable in areas of radio transmissions and use of RFID technology to infiltrate vehicle entrance lock systems. He conducts training to law enforcement on related topics.

- ***Kellyn Wagner – Intelligence Analyst – Northern California Region Intelligence Center (NCRIC)***

  Kellyn works cyber intelligence and cybercrime. She is developing a training course of cyber enabled crime and is collecting reports of cyberattack events including vehicle cyber-crimes. Email: kwagner@ncric.ca.gov / Phone: 415-918-0981

  Cyber Security Team Email: Cyber@ncric.ca.gov

- ***Andre Weimerskirch – Vice President, Lear Corporation***

  Presentation Reviewed: Vehicle 2 Vehicle Security, Automotive Cybersecurity, 2017 This presentation provides an overview of connected vehicle security, communication and privacy, server security, and vehicle cybersecurity concerns. This includes discussion of Lear's product development in cybersecurity countermeasures.

  Email: aweimerskirch@lear.com / Phone: 248-447-4512

- **Publication/Research Reviewed: University of Michigan Research; Identifying and Analyzing Cybersecurity**

  Threats to Automated Vehicles, January 2018

  Authors: Andre Weimerskirch and Derrick Dominic

  This research discusses the vulnerabilities and threats to autonomous vehicles and research conducted on such. A threat matrix is included for automated parking features that may be vulnerable for attack and an overall summary explains areas needing further research and development.

- **Presentation Reviewed: Connected and Automated Vehicles and the Cybersecurity Threat, Industry Responding – February 2015**

  Author: Andrew Brown, Delphi

  This is an overview of the volume of active safety technology and increasing levels of infotainment integrated into vehicles. This includes an overview of vehicle cybersecurity and areas needing to be addressed. Delphi's response to cybersecurity needs is also discussed.

- ***Publication/Research Reviewed: The Autonomous Vehicle Revolution, March 2017*** Author: Center for the Study of the Presidency & Congress

  This publication discusses the concern of autonomous vehicle cybersecurity measures and importance of government and private sector relationships to find solutions to risks and threats. Discussions focused on security of vehicles electronic control units (ECU), and how vulnerable they may also be to attack. This area is a concern for all connected vehicles.

M UMTRI

Andre Weimerskirch joined University of Michigan Research Transportation Research Institute (UMTRI) on January 1, 2014, as an associate research scientist. He is an internationally known expert in the area of vehicle-to-vehicle (V2V) communication security and privacy mechanisms, both in the United States and Europe. He says that…

"Cybersecurity is an overlooked area of research in the development of autonomous vehicles."

UMTRI's researchers cover topics as diverse as the automation of transportation, to senior mobility, to a broad range of security specific research interests that have relevance to public safety.

Reference Materials

1. Interpol, Fighting Vehicle Crime and Stolen Motor Vehicle Database (https://www.interpol.int/en/Crimes/Vehicle-crime/Fighting-vehicle-crime)

2. NHTSA Cybersecurity Best Practices for Modern Vehicles—U.S. Department of Transportation

3. NHTSA Electronic Reliability and Cybersecurity Research Programs

4. NHTSA Cybersecurity Modern Vehicles and Cybersecurity Research—Cem Hatipoglu, PhD

5. NHTSA Odontometer Fraud Overview (https://www.nhtsa.gov/equipment/odometer-fraud)

6. V2X Security and Privacy, Andre Weimerskirch—Sans Automotive Cybersecurity 2017

7. Connected and Automated Vehicles the Cybersecurity Threat—How the Industry is Responding Auto-ISAC Executive Overview—March 2018

8. The Autonomous Vehicle Revolution Fostering Innovation with Smart Regulation—March 2017

9. Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles—University of Michigan NDCAC Tri-Fold— March 8, 2018

10. GM Vehicle Security Reference Card

11. GAO Report on Vehicle Cybersecurity & U.S. DOT Response

Working Group Members

Christopher McDonold—Vehicle Crimes Committee Chair

Paul Steier—Chair, Law Enforcement Program Manager, AAMVA

George Baker— Global Vehicle Security Lead, General Motors

Robert Force— Director, Colorado Theft Prevention Authority

Sherry LeVeque— Emergency Services Outreach, OnStar

Holly Merz—Investigator, Iowa Attorney General's Office

David Scaff— Security Manager, Copart

Sgt. Blake Schnabel— California Highway Patrol

David Sparks— Director, NHTSA Office of Odometer Fraud Investigation

Joann Tierney—Daniels, Program Manager, New York State Division of Criminal Justice Services, Law Enforcement & Legal Services

Jason Tillou— Program Representative, New York Division of Criminal Justice Services

DJ Thompson— Senior Director of Law Enforcement, LoJack Corporation

Julio Valcarcel— Vice President of Sales, Selex ES Inc.

Special Thanks to Kevin Wiggins—Intern, Iowa Attorney General's Office / Editor

IACP
International Association of Chiefs of Police