Auto Theft Today

A PROFESSIONAL E-NEWSLETTER BY THE INTERNATIONAL ASSOCIATION OF AUTO THEFT INVESTIGATORS

VOLUME 4 ◆ ISSUE 1 ◆ SEPTEMBER 2016

this issue

International Seminar - our Olympics

Well after years of hard work, and what seems like a blink of an eye, another International seminar has come and gone. This years seminar was another great event with around 325 delegates from all around the world meeting in Murfreesboro, Tennessee.

While in Murfreesboro I couldn't help but draw some parallels with the Olympics that were taking place in Rio. Firstly, both events involved a gather of highly trained individuals from all around the world. Secondly, while only a few would go home with a trophy, that didn't matter — we all gained something from being there and formed new friendships. It also struck me that just like the Olympics it doesn't matter where you come from or how many wins we score. We all contribute something and sometimes the most significant contribution can come from the places you least expect. For example, in the 2016 Rio Olympics the tiny Pacific Ocean country of Fiji, with a population of less than 900,000, won its first ever Olympic medal – a gold medal. This demonstrates we all have something to offer, no matter where we are from.

IAATI is a fantastic Association with members all around the world who are willing and able to assist with your investigations. Reach out and make the most of this incredible network of professionals.

As well as a solid program of classes, and networking opportunities this was also a productive time for the IAATI board, including:

- The release of a new policy about the use of IAATI's name and logo;
- The launch of a new fee structure for members in financially disadvantaged countries;
- Approval of a new one day auto theft investigation training to police officers in areas that are not currently represented by auto theft associations or areas where IAATI membership is limited at this time;
- Selection of the host branch for the 2019 International Seminar; and
- The approval, at our AGM, of amendments to our constitution.

(See more information about these initiatives on pages 3-7)

Thanks again to Rusty Russel and the Southeast Regional Chapter for a great seminar. Now I am excitedly counting down the days to our 65th International Seminar in Cape Town, South Africa, 28 August to 1st September 2017.

Chris McDonold, Editor

Auto Theft Today

Editor: Chris McDonold

Editor: Christopher T. McDonold

Email: enews@iaati.org

Auto Theft Today is an official e-newsletter of The International Association of Auto Theft Investigators (IAATI).

This newsletter is designed to provide the reader with links to the related information. Click on pictures or links to see more information. The inclusion of a link does not imply the endorsement of the site.

IAATI's Branch and Chapter Websites

Branches:

Australasian Branch
iaatiaus.org

European Branch
eb-iaati.org

Latin American Branch
iaatilatam.org

Southern African Branch
iaatisab.co.za

United Kingdom Branch
http://www.iaati.org.uk/

Chapters (North America/Canada)

North Central Regional Chapter
ncrc-iaati.org

North East Regional Chapter
neiaati.org

South Central Regional Chapter
tavti.org

South East Regional Chapter
seiaati.org

Western Regional Chapter
wrciaati.org

BOARD & COMMITTEE UPDATES

- **2016 Annual General Meeting—Outcomes**

  The Association held its 2016 Annual General Board meeting on Thursday 11th August during the 64th Annual Training Seminar in Murfreesboro, Tennessee. At that meeting the proposed changes to the constitution were passed thereby increasing the number of Directors on the International Board to 10, of which up to four may be Affiliate members.

  The Nomination Committee also announced their recommendations for the 2016/17 Board positions which were accepted and subsequently sworn in later that night during the Seminar Dinner. The 2016/17 Board comprises:

President:	Hans Kooijman (European Branch)
1st Vice-President :	JD Hough (Western Region)
2nd Vice-President :	Joey Canady (South Central)
3rd Vice-President:	William Johnson (Western Region)
4th Vice-President:	Tinus Odendal (Southern African Branch)

Directors :	Renato Schipani – European	Richard Spallinger – Western
	Paul Thomas – Australasian	Danny Sheppard – South Central
	Barb Rambo – North Central	William Biondo – North Central
	Reg Phillips – Northeast	Ana Laura Brizuela – Latin American
	Brad Anderson – Northeast	George Graham – Northeast

Associate Director's:	Arne Knippel – European	Philip Opperman – Southern African Branch
	Michelle Lanham – South Central	Anna Kotsovos – North Central
	Irene Molinari – Latin American	David Northey – U.K. Branch
	Walt Robinson – Southeast Chapter	Frank Cruz – Western Chapter
	Sheri Taynor - South East	Annette Jacobs Western Region
	Jorge Omar Nasrala – Latin American	

The following Administrative appointments were also made by the President: for the coming year:

John Abounader – Executive Director	Bob Hasbrouck - Treasurer
Carmen Swanson - Marketing Director	Stephen Gobby - Editor APB
Chris McDonold - Auto Theft Today	Philip Crepeau – Managing Editor of APB
Kevin McHugh - Legal adviser; Domestic USA	
John O'Byrne - Legal adviser; International	

The 2016/17 IAATI Board

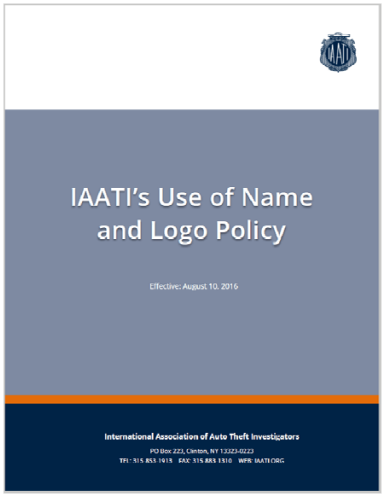
BOARD & COMMITTEE UPDATES

- **New policy released for the use of IAATI's name and logo**

  The IAATI Board have approved the release of a new policy that outlines the use its logo and name by members and sponsors. The new policy recognises the changes in today's society and outlines the circumstances IAATI members are able to use the IAATI logo on their own personal business card and the IAATI name on their own personal and business email signature, It also specifies how the logo and name can be used by sponsors or those corporate organizations that which to show their support of IAATI. This policy will provide more flexibility for members and corporate bodies to use the logo provided they follow the conditions outline in the policy.

  Copies of *IAATI's Use of Name and Logo Policy* can be downloaded by clicking on the image to the right or by via the link: http://www.iaati.org/download/efiles_all.asp?id=1346

  The Policy should also be read in conjunction with IAATI's Corporate Style Guide which can be access via: https://www.iaati.org/download/efiles.asp?id=1348



- **New incentive to support IAATI members in Latin America, Southern Africa and Europe**

  The recent board meeting in Murfreesboro also approved a recommendation from the Membership Committee for a new fee structure for members of some branches. An analysis of the after tax monthly incomes of almost 70 countries revealed that the financial impact of the Annual IAATI membership fee is four times higher for members in Latin American, African and some European countries. Thus the Board approved a new $US 10 fee for members in Latin American and Africa countries. This offer has also been extended to members in financially disadvantaged countries in Europe and the European Branch Board has been tasked with determine which countries within their region will qualify for the reduced membership fee. As part of the lower fee these members will receive only an electronic copy of APB, however, they may elect to receive a printed version of APB for an additional fee of $US 30 per year. The new fees will apply from 1st January 2017.

- **Updated versions of our Constitution and Standard Operating Procedures now available.**

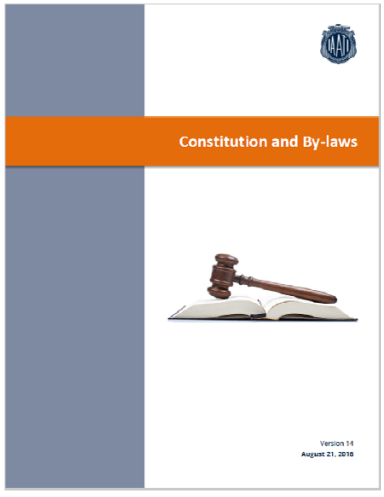
  As noted on the previous page our Constitution was recently amended at the 2016 Annual General Meeting. Updated copies of our Constitution and also our Standard Operating Procedures can be accessed from the following links:

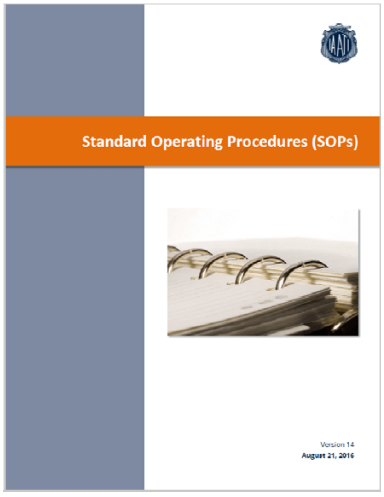
  Constitution and By-laws:

  https://www.iaati.org/download/efiles.asp?id=1342

  Standard Operating Procedures:

  https://www.iaati.org/download/efiles.asp?id=1344





BOARD & COMMITTEE UPDATES

- **Survey Committee - Thank you for your feedback**

  Over the past 12 months IAATI Survey Committee has been extremely active. In addition to our annual post seminar feedback surveys of delegates and sponsors/exhibitors and an Exit Survey of non-renewing members, the Committee also undertook a feedback survey about Auto Theft Today and a major study of other Successful Association to determine what lessons IAATI can learn from them.

  The Committee appreciates the time and effort given by it survey respondents to provide their feedback and we will be using the information provide to improved our services over the coming year.

  Below are some of the key findings from some of our recent surveys:

  Auto Theft Today—Member feedback

  Overall the feedback about Auto Theft Today is very positive:

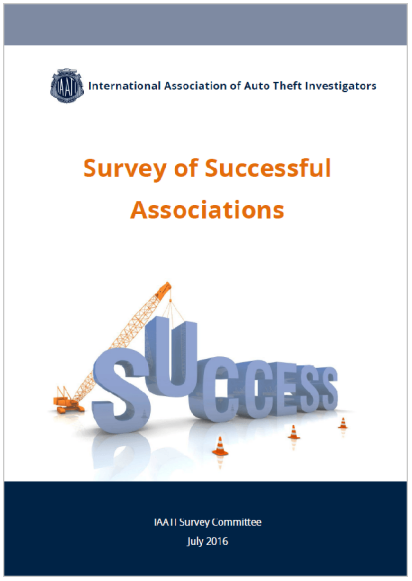
  - The vast majority of respondents (88%) reported downloading and Auto Theft Today.
  - Respondents are generally satisfied with the current mix of content of each issue although would appreciate more original articles authored by members and more articles about current and emerging trends.
  - The growing size of the recent issues of Auto Theft Today does not appear to be a major impediment to most members with 79% of respondents either happy with it current size or don't care about its size. Furthermore, only 7% of respondents reported experiencing any difficulty downloading each issue. (While this number is relatively small it is still important that the Auto Theft Today Committee does not disadvantage members from regions that suffer from slow or unreliable internet connections and should look at alternative options that enable members to download smaller versions of Auto Theft Today)
  - Three quarters of respondents were happy with the bi monthly release schedule of Auto Theft Today, although one in seven respondents (14%) would like it be published monthly.

  Suggestions the Auto Theft Today Committee are considering in the future include:

  - More 'calls for articles' to the membership as opposed to just the Board members.
  - Directly targeting specific members to write articles.
  - Establishing a representative within each Branch/Chapter (possibly a Vice President or committee member) who is responsible for soliciting and providing local news items, Branch/Chapter news and original articles from their local members.
  - Providing members with a choice of formats of Auto Theft Today to download, i.e. a quick access format v's the current full content format.
  - Use HTML formatted emails to advise members of the latest release.
  - Encourage members to follow IAATI's Facebook page and make greater use of Facebook to convey selected Auto Theft Today content.

BOARD & COMMITTEE UPDATES

Survey of Successful Associations



Based on the findings from this study the Survey Committee makes the following recommendations:

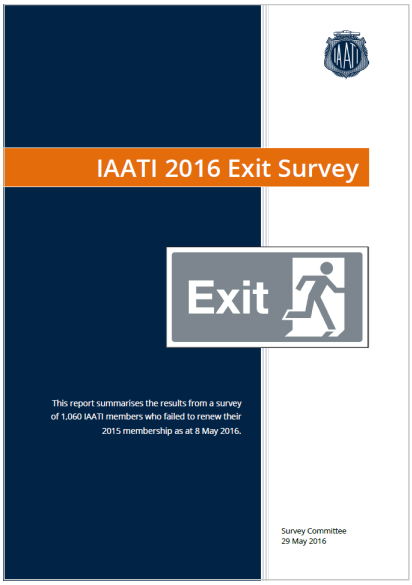
1. IAATI should ensure it maintains regular communication. This should be at least monthly, but preferably more frequently.
2. IAATI utilize social media, other related conferences, partnerships with other organizations and the media to create a public profile so people are aware of IAATI, particularly amongst younger potential members.
3. I AATI regularly promote it's achievements, as members and sponsors like to feel they are part of a growing and successful organization.
4. That the 2016/17 Membership committee work with the local branches and chapters to develop a New Member Integration Program. Included in this are ideas such:
   - Developing a welcome kit for new members,
   - Initiate follow up contact with new members at 3, 6 and/or 12 months
   - Introduce colour coded badges to identify new members at training seminars
   - Initiate a range of activities to integrate new member at networking or training events, including having board members take responsibility for introducing new members to existing members.
5. The 2016/17 Membership committee has a major focus on member retention, including
   - Working with the Executive Director to develop a "Report Card" that will accompany membership renewal invitations.
   - Developing recognition for long term members (i.e. 10 year/ 20 year/ 30 year members) – possibly via our publications and/or the website.
   - Implement a "We want you back" program that targets lapsed members.
   - Encouraging members to be more involved in the Association as research demonstrates members who are more involved not only get more from an Association, but also more rapidly enhance their professional networks and are more likely to remain as members. Involvement can range from sourcing or writing article for a newsletter, offering to provide a training session, chairing a session, assisting with packing satchels or assisting with the organisation of a seminar, distribution information about the Association to work colleague, serving on a board/committee, etc.
6. To address the issue of employers being unable to fund staff to travel to attend training seminars IAATI:
   - Consider forming partnerships with other related Associations to run a number of smaller joint regional events and thus 'take the training to the members' rather than expecting the members to come to us.
   - Implement a webinar program asap so members unable to attend seminar are still able to access some training throughout the year.
7. The Awards Committee consider increasing member involvement in the awards program by following the IACA and the ACFE approach of designating one award to be judged and voted upon by the members.
8. The Board consider developing a more rigorous reporting program from the committees to ensure that any issues relating to tasks not being completed on time are readily identified and the Committee chairs are offered any additional support they may require.

BOARD & COMMITTEE UPDATES

Exit Survey

Key findings from our 2016 Exit survey included:

- The most frequent reason respondents gave for not renewing their membership in 2016 was that "they had retired or no longer work in the area of auto crime" (36% of respondents). This was marginally higher than the 30% recorded in the 2015 exit survey.
- One in seven (14%) had "simply forgotten or haven't renewed yet but I intend doing so" (compared to 22% in 2015).
- A similar proportion (14%) " haven't been able to attend a chapter/ branch training seminar or are unlikely to be able to attend a training seminar due to cost or no support from Agency/ Company", up from 9% in 2015.
- There were also a small number of respondents (8%) who reported having renewed their memberships. In these cases their Branch or Chapter may have failed to have notified the International Executive Director of their renewal prior to the survey being sent out to the members.
- The percentage of respondents who cited negative experiences with IAATI as the reason for not renewing their membership was 9%.



The Membership Committee will be analysing the findings from these surveys to develop new strategies and incentives to attracted new members and retain existing members.

- **Education and Training Committees**

The Education & Training Committees has received $5,000 from the IAATI Board to establish a new one day *Basic Motor Vehicle Crime and Identification* training program in 2017. The pilot program will be offered in geographical areas that are not currently represented by auto theft associations or areas where IAATI membership is limited at this time. This new one day Basic Training will cover:

- IAATI background and information
- Nader Labels
- Counterfeit VIN/Nader labels
- Vehicle Identification Numbers (VIN)
- Secondary vehicle identification methods
- Search warrant preparation

This will be free training by IAATI instructors who will also provide information about IAATI.

Did you know?

That as a financial member you can always access past issues of Auto Theft Today or APB in our f the IAATI **File Library**.

The File Library also contains a range of other important documents including our Constitution and By-laws, SOPs, our 2015-20 Strategic Plan, Legislation Update, Corporate Partner Program plus training material from past seminars and Certification reading materials.

Just log into the member only section of the website and search the file library.

BRANCH & CHAPTER NEWS

Southern African Branch:

- 2016 Annual Seminar: Planning and preparation is well underway for the annual SAB training seminar which will again be held **26th—28th October 2016** at the usual venue, the South African Police Resort & Conference Centre Weesgerus in the Limpopo Province. For more information contact Daan Nel, via email: dnel@tracker.co.za

- 2017 International Seminar: The countdown to the first ever International IAATI Training Seminar in Africa has began. The event will be held in Cape Town **28 August to 1 September 2017.** Please note the revised dates which have changed by one week from those previously advertised. This change in dates was made to move the seminar venue to a neighbouring conference facility which is substantially bigger and just been built. The 65th Annual Seminar Committee is keen to ensure that this will not only be a great educational and networking opportunity for all attendees but also an exceptional opportunity for delegates and their families to experience the many wonderful highlights of Southern Africa, pre and post the seminar. More details about this major event will be included in the coming issues of Auto Theft Today and APB, but in the meantime you are encouraged to register your interest in attending at http://iaati2017.co.za/

- If you have any questions about the 2017 Seminar, or wish enquire about sponsorship or exhibiting at the seminar please contact either:
    - Phillip Opperman - philip@iaati.org
    - Marthinus Odendal - todendal@iaati.org
    - Daan Nel - dnel@iaati.org

Australasian Branch:

- The Branch Committee are currently seeking speakers for its 2017 Annual training Seminar which will be held in Brisbane, 20-22 March at the Pullman Brisbane. If you would like to nominate to give a presentation or host a workshop, or wish to suggest someone we should consider as a presenter then please contact Branch President, Mark Pollard, on mpolllard@iaatiaus.org The Pullman Brisbane is a five star hotel conveniently located on the corner of Ann and Roma Streets in the heart of Brisbane, a short stroll from both the Queensland Police headquarters and the head office of Suncorp Insurance. Conference Direct have secured a number of cost savings for the Branch including a lower accommodation rate than delegates paid at our 2016 Seminar.

- The Australasian Branch is also keen to hear from any potential sponsors or exhibitors for the 2017 seminar. This is a great opportunity to provide you business to our members and to show your support for auto-theft investigators, so get in early to secure you preferred package. The 2017 Sponsorship and Exhibitor prospectus can be download y clicking on the image to the right or following the link: https://www.iaatiaus.org/images/uploads/documents/Seminars/2017_Seminar_Brisbane/2017_Sponsorship_Brochure.pdf

- In October nominations will open for the 2017 Australasian Branch Awards. It is expected we will again have five categories of awards, namely:
    - Investigation of the Year
    - Insurance Industry Investigation of the Year
    - Forensic and Supporting Services Award
    - President's Award
    - Member of the Year

  So start thinking about and your nominations any work you or your colleagues have been involved in.

BOARD & COMMITTEE UPDATES

- ## UK Branch

UK wins the right to host the 2019 International Seminar

The UK Branch has been confirmed by the International Board as the hosts for the 2019 International Seminar following a successful bit to the Site Selection Committee. This will mark the first time the international IAATI seminar has been held in the UK and only the sixth time the seminar will have been hosted outside of North America. The exact location of the seminar is yet to be determined but the UK Branch Committee now have 3 years to plan this major event.

Reflecting IAATI's expansion around the world the International Seminar continues to be rotated between the North America Chapters and the International Branches in alternating years. The 2017 Seminar will be held in Cape Town, South Africa (28 August to 1 September 2017) and the 2018 International Seminar will be held in Pittsburgh, Pennsylvania (August 2-11, 2018).

2016 Training seminar

The UK Branch held it 's National Vehicle Crime Conference 2016 at Loughborough University, 8-9th June 2016, where there were stakeholders from over 30 organisations present with up to 132 delegates attending. To view photos from this successful event visit: http://www.iaati.org.uk/conference-2017/conference-2016/

Trade Vehicle Locks (TVL)
TVL's team were pleased with the amount of engagement we received through the delegates. A really good cross sector of law enforcement and industry were engaged to see some of the solutions we have on offer to some of the current threats posed by vehicle crime. The subjects discussed really highlighted how we all need to work together to curb the current threats and sharing knowledge and good networking to this is key. IAATI certainly proved it can pull together the right stakeholders and this has led to further engagement with TVL after the conference. With the success of this one we are certainly looking forward to next year!

Vehicle Provenance Limited
Really impressed with this years conference. The new location was excellent as was the quality and calibre of speakers and exhibitors who attended. It was also great to see the diversity of candidates from all sectors of the industry which clearly highlights the current problems being faced. The knowledge and contacts gained have already lead to further business opportunities and partnership approaches to tackle the current problems. It is clear to see why the IAATI UK conference has become the UK's leading conference discussing vehicle theft and vehicle 'enabled' issues. Certainly looking forward to next years event.

Vodafone Automotive
Great conference and really gave us a platform to demonstrate how our technologies can help in the fight against vehicle crime. Being able to present also helped us highlight what we have learned along the way. With vehicle crime on the increase technologies will also play a large factor in curb the threat of vehicle theft.

DATATAG
Datatag's whole team was very impressed with this year conference and the new location, in Loughborough, was convenient and an excellent venue for the event. It was nice to hear from a wide range of speakers, all of a high calibre, from diverse backgrounds. All sectors of the industry were well represented which helped to highlight all the current problems being faced in tackling the many different types of criminal activity.

The new contacts that we made have already led to further business opportunities. We like the partnership approach taken, which we believe to be essential, to tackle all the current problems.

It's clear to see why the IAATI UK conference has become one of the leading conferences discussing vehicle theft and we look forward to supporting and participating in next year's event.

Continued on the next page

- ## UK Branch (continued)

Chronos Technology Limited
Excellent event in Loughborough. Some good new contacts as well as the opportunity to keep up with existing contacts. Since the event we have had some positive feedback and are now working in wider parts of the industry. Look forward to next year and will be bringing latest news on our GPS Jammer Detection technology, where it is deployed and success stories.

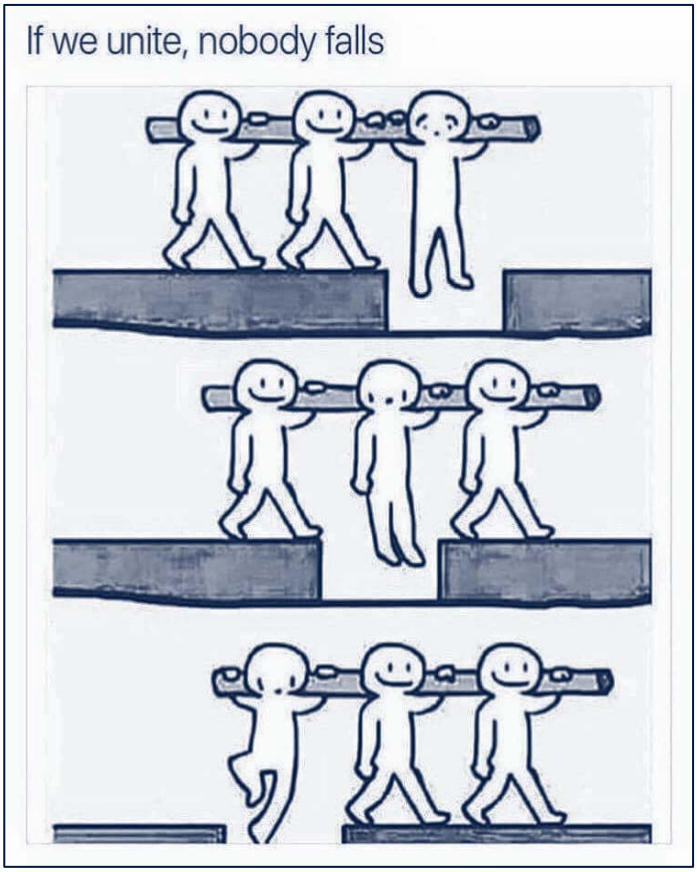
Hafren Fasteners
Matthew Lynes Managing Director of Hafren Fastener explains, "Hafren Fasteners have always been happy to support the IAATI conference, which plays an important role in reducing the theft of and from vehicles. There's an incredibly strong alignment between our two organizations, both are committed to preventing crime and theft through innovative approaches, and collaborations with parallel organisations/professionals."

We have always had a great experience at the IAATI conference, with a lot of attendees, inspirational speakers, interactive workshops, fantastic networking opportunities and breakout discussions we have found it an invaluable resource and a mainstay of our calendar.

Claims Management and Adjusting (CMA)
It was pleasing to see a good mix of police, security experts, vehicle manufacturers, insurers and others with an interest in the subject of vehicle theft. That we are seeing an increase in reports of theft likely results from some complacency over the past years following the introduction of immobilisers and engine management units shortly before 2000. It was pleasing to see so many dedicated to the issue and to be able to meet and discuss the matters at a dedicated location – to have all parties brought together. I doubt we could have accomplished so much in a month of meetings! The environment was well suited to the presentations and I would welcome future use of the venue.

CDL Vehicle Information Services
My first visit to the conference was an eye-opener to the issues facing the industry and was very insightful. With some experienced and knowledgeable speakers and attendees, I definitely gained some interesting, useful and actionable information for our business.

BikeTrac
BikeTrac have been supporters of IAATI for a number of years but this years conference was really special. Lots of engagement with everyone and events such as this really do help the industry realise there are cost effective solutions in the marketplace to tackle the current issues. We will never completely stop all vehicle crime but any barriers we can put in the criminals way or tools we can provide police with their investigations has always got to be a step in the right direction.



'A PARTNERSHIP APPROACH' – GET INVOLVED.
#IAATIGLOBAL

Proudly hosted by the Palm Beach County Sheriff's Office

SE INTERNATIONAL ASSOCIATION OF AUTO THEFT INVESTIGATORS IAATI RC

*You are invited to join us **6/11/17- 6/15/17**, in beautiful Delray Beach, FL. This symposium will include 4 days of intensive training in all aspects of fraud and theft, especially those cases involving vehicles, cargo haulers, and marine vessels.*

Register ONLINE today!

SEIAATI 43rd Annual Training Symposium

Delray Beach Marriott
10 N. Ocean Boulevard
Delray Beach, FL 33483
Reservations: 877-433-5729 or reserve your room online at www.seiaati.org
June 11-15, 2017
(rates are good pre and post event)

Rates: $139.00 per night, plus $8.00 p/day parking

Reservation Deadline: May 15, 2017

Local Airports: Palm Beach International & Fort Lauderdale International. Check website for shuttle information.

Register online at www.seiaati.org

FEES (Prior to May 15, 2017)
$200.00- Members $245.00 Non Member (includes membership)

Late Registration- After May 15, 2017:
$250.00- Members $295.00-Non Member (includes membership)

Training Topics

- ***Surveillance & Bait Systems***
- ***Vehicle Identification***
- ***Fraud Investigations***
- ***Marine ID & Investigations***
- ***Cargo Theft Crimes***
- ***Identity Theft***
- ***Insurance Fraud Investigations***

And many more! 3 breakout classrooms each day with multiple classes available!

Check the website for updated training!

For questions on the conference, please contact Onsite Coordinator Nathan McGanty at: nmcganty@gmail.com

SEIAATI
PO Box 274
Edgewater, FL 32132
secretary@seiaati.org
(386) 846-3965- Sheri Taynor

Includes:

***Welcome Reception**-Business Casual*

***Offsite Picnic** –Casual (transportation will be provided!)*

***Annual Banquet**-Business Dress*

***Networking Suite Nightly**- Casual*

64th INTERNATIONAL SEMINAR

After years of planning this year's International Seminar in Murfressboro is now over. It was a great success thanks to the hard work of Rusty Russell and his seminar committee. A full wrap up of the seminar including a range of photographs from the event will be included in the next issue of APB. However if you can't wait below are a small selection of photos. If you would like to view a more photos visit the IAATI Facebook page.

In Murfreesboro we had interesting presentations and established new friends from around the world.

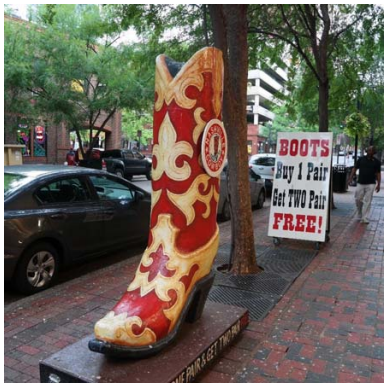
64th INTERNATIONAL SEMINAR

We also enjoyed good food and, on the Monday night , the hospitality of Willis J. Johnson (Copart), at the Speed and Feed BBQ.

Some delegates even managed a pre-seminar visit to the Jack Daniel's Distillery,

a photo with Miss Tennessee,

or a visit to Nashville to buy some new boots.



But the 'Best footware' prize went to ....

Turn to page 54 to find out who is the owner of these high fashion shoes.

64th INTERNATIONAL SEMINAR

2016 Sponsors/Exhibitors

IAATI would like to thank the following Sponsors and Exhibitors who supported the 2016 IAATI/SEIAATI Annual Training Conference in Murfreesboro, Tennessee. Your support to IAATI and our members is greatly appreciated.

Diamond Sponsors:

MANHEIM

Observint TECHNOLOGIES

Silver Sponsors:

Do-It-Yourself Pull-A-Part USED AUTO PARTS

Copart

OnStar by GM

PassKey Premium Products

Selex ES A Finmeccanica Company

Regula forensic science systems

Conference Sponsors:

LOJACK

Hampton Wildlife Fund

Exhibitors:

LAW ENFORCEMENT FBI LEEP ENTERPRISE PORTAL

INSTA etch MARKING SYSTEMS

TRACERSINFO.com

VIGILANT SOLUTIONS

LOCATOR TECHNOLOGIES

Liberty TIRE RECYCLING

SPONSOR SPOTLIGHT

How deep can one go when analyzing obliterated VINs

By Arif Mamedov, Ph.D.i and Yuriy Agalidi, Ph.D.ii

In the process of recovery of obliterated VINs there is always a question on how deep technology can go beyond the depth of the original stamp. This question is valid for any restoration method. While many investigators are familiar with limitation of chemical and electrochemical methods, method of magneto-optical imaging (MOI) often considered as a new method, despite of its 15+ years use in the filed worldwide.

To address some of these questions we have designed and carried out a simple experiment using 2 mm thick steel coupons with stamped numbers at the distance of 10 mm from each other (Figure 1A). The several specimens then were 1:100 cone tapered. 1:100 ratio means, that at the end of 100 mm coupon 1 mm of material was removed from the surface of the sample (Figure 1B). With such arrangement around character 4 it was removed 0.4 mm of material (average VIN stamp depth) and we no longer can see the number with optical tools. The place of the character 8 will correspond to the double depth of the stamp and the second character 2 – to the triple depth of the stamp.

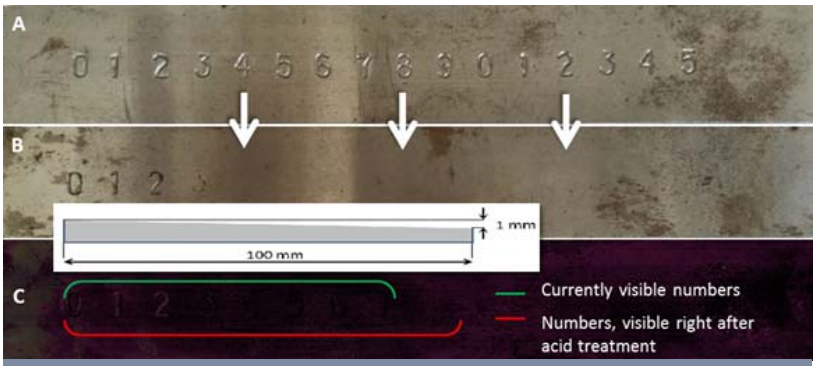


Figure 1. Original (A), 1:100 cone tapered (B) and acid treated steel specimens, used for experiment

The chemical (acid) examination has been done by Special Agent Todd Blair (NICB) using the standard acid kit he had in stock. At the time of experiment we were able to see numbers all the way to the character 9. Characters 8 and 9 later have faded and no longer visible by optical tools (Figure 1C).

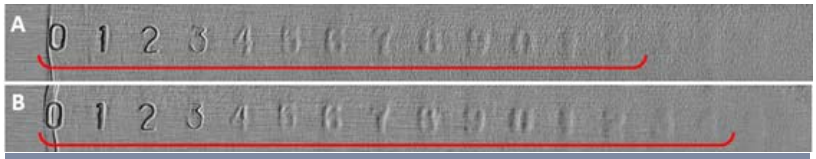


Figure 2. Eddy-current scan of the acid-treated (A), and non-acid treated (B) 1:100 cone tapered specimens. The red bracket indicates area of definitive character recognition area. Being destructive method, acid based examination removes portions of the information layer. Such removal results in shorter area of definitive character recognition for acid treated sample.

We have examined both acid treated and non -treated test coupons, using Eddy-current examination method. This method of MOI is sensitive to the internal stress of metal, rather than to its physical deformation. The results are shown on Figure 2. We clearly can see second characters 1 and 2 and traces of 3 and 4 on the specimen, previously treated with acid (Figure 2A) and clear characters all the way to second character 4 on the non-treated sample. In some experiments we were able to recover all 15 digits from the specimen. These results enable us to make a statement that non-destructive MOI methods under certain examination conditions can reach up to the depth of 3-4 times of the original stamping.

For any technical, sales and support questions feel free to contact any Regula office or local Regula representative in your country. You can find information about Regula offices and worldwide partners on our web: www.regulaforensics.com.

i Regula Forensics, Inc., Reston, VA, USA, arif.mamedov@regula.us, +1.703.234.2355
ii LAD Laboratory of National Technical University of Ukraine, Kiev, Ukraine

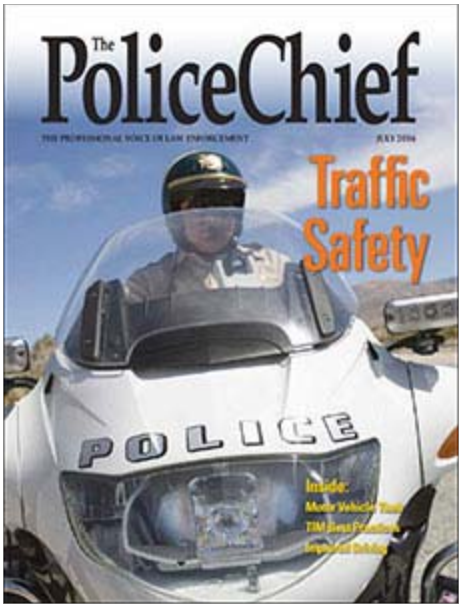
IN THE NEWS

Motor Vehicle Theft: A Relationship to Other Crimes

By Robert D. Force, "Motor Vehicle Theft: A Relationship to Other Crimes," The Police Chief 83 (July 2016): 32–38

The July issue of *The Police Chief* magazine has included an interesting article by Robert D. Force on the relationship of motor vehicle theft to other crimes.

Robert D. Force is a member of the IACP Vehicle Crimes Committee and the director of the Colorado Auto Theft Prevention Authority, a business unit assigned to the Colorado State Patrol. Mr. Force retired in 2003 as an assistant chief of police from the Rio Rancho, New Mexico, Police Department and has worked in the law enforcement field for the past 36 years. He is a graduate from the FBI National Academy (202nd class) and the NW School of Police Staff and Command (63rd class) and holds bachelor's degrees in criminal justice and law & society from New Mexico State University.



In his article Robert concludes:

"States and agencies deploying auto theft task forces have a strong documented history demonstrating that auto theft is a transformational crime associated with a wide array of criminal activities, as discussed herein. Those in the field of auto theft prevention understand this issue, such as the International Association of Auto Theft Investigators, auto theft prevention authorities, and the IACP Vehicle Crimes Committee. However, there are law enforcement administrators and prosecutors who still consider auto theft as a victimless, nonviolent property crime.

The Colorado Auto Theft Prevention Authority's study determined that motor vehicle theft is not an isolated property crime, but rather a crime incurring numerous victims and motivated by the furtherance of other "higher-priority" crimes. As pointed out in The Colorado Auto Theft Annual Report–2012, "In many cases, the crime of auto theft is considered a transitional crime as offenders use the crime of auto theft to pre-empt, complete, or otherwise conduct organized white collar crime and/or other crimes against persons (e.g., bank robberies, burglaries, drug trafficking, and human trafficking)."

Law enforcement executives should be encouraged to elevate the prioritization of vehicle theft events (report incident to the recovery incident) in order to:

- increase forensic evidence collection (e.g. DNA, fingerprints and hair) that can be used to identify and substantiate individuals who may be involved with other crimes:
- increase the ability of law enforcement and prosecutors to establish the criminal predicates of offenders engaged in a pattern or series of criminal behavior beyond property crime; and
- elevate intelligence and information gathering to associate criminal enterprises engaged in pattern or organized crimes such as home invasions, burglaries, robberies, drug cartels, identity theft, homicide, and arson. "

The article is excellent and well worth a read. I encourage everyone to read this article which can be viewed by following the link:
http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=4205&issue_id=72016

This same issue of *The Police Chief* also has an interesting article by Kevin Davis, California Highway Patrol entitled 'Preparing for a Future with Autonomous Vehicles' - see:
http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=4200&issue_id=72016

IN THE NEWS

USA: Police nab car thief who posted crime on Snapchat

By WMAR Staff, 18 July 2016

OCEAN CITY, Md. - Ocean City Police arrested a New York man after he posted videos of himself stealing a car on social media.

Police said 24-year-old Brian Engelmann of Mystic Beach, NY posted a series of videos on Snapchat showing him stealing a Jeep Wrangler from the parking lot of Seacrets Bar and Grille around 2 a.m. Saturday morning.

The videos posted around 8 p.m. Saturday night helped police identify and locate Engelmann. They showed him stealing the car and driving erratically to 37th Street, where he abandoned the car in a condominium parking lot.

Police tracked Engelmann down back at Seacrets later that night where he was arrested with the help of security staff.

Ocean City police charged him with vehicle theft in addition to multiple traffic violations including using a handheld phone while driving, negligent driving, and driving while on a suspended license.

Englemann was seen by a Maryland District Court Commissioner and was transferred to the Worcester County Jail on $20,000 bond.

Source: http://www.abc2news.com/news/crime-checker/eastern-shore-crime/oc-police-nab-car-thief-who-posted-crime-on-snapchat

---

European Branch Annual Seminar

The next IAATI European Branch training seminar will be held in Torremolinos, Spain. The Seminar will take place from 5th—7th of October at Hotel: Sol Principe - Paseo Colorado 26 - 29620 Torremolinos (Malaga), Spain.

To view the seminar program: *http://eb-iaati.org/auto_investigators/documents/uploads/Program_Torremolinos_2016_-_updated_19.08.pdf*

The **last date for registration** for this seminar **is Wednesday September 21st**, please use registration form: *http://eb-iaati.org/auto_investigators/documents/uploads/Registration_form_Torremolinos_2016_ENGL_%281%29.doc*

For details about this, not to be missed event contact **Arnie Knippel**, 1st Vice President, at akn@forsikringogpension.dk

2016 European Branch Annual Seminar

5th - 7th October, 2016

Hotel Sol Principe,
Paseo Colorado 26 - 29620
Torremolinos, Spain

Register by 21st September

BOARD & COMMITTEE UPDATES

Did you attend the 2016 International Seminar in Mursfreesboro?

If so, then please help us **look back** and see what we did well and where we can improve.

Please check your emails for a link to a short feedback survey which will help us tailor future training seminars to your needs.

The survey closes: **September 15, 2016**

If you attended the 2016 International Seminar but did not receive an email link to complete the survey please visit:

www.surveymonkey.com/r/IAATI2016Seminar

Your wireless footprint can help police catch a thief

By Maxim Chernyshev, Cyber Security Researcher, Edith Cowan University,1 July 2016

With billions of wireless devices shipped across the globe every year, it is safe to assume that most of us carry at least one wireless gadget with us much of the time.

The number of wearables to be shipped this year alone is expected to exceed 100 million. Interestingly, one-third of wearables next year will be rather inconspicuous, with smart contact lenses and connected jewellery also hitting the market.

The growing demand for more traditional gadgets such as smartphones and tablets is also set to continue. The increasing popularity of wireless home automation products and smart appliances means there will be more wireless gadgets around your home.

Our cars are getting smarter too, with built-in wireless technologies delivering the latest connected driving and infotainment experience.

All in the signals

Wireless communications including the omnipresent Wi-Fi and Bluetooth technologies are underpinned by radio transmissions. These seemingly invisible radio waves travel in the open air – a medium that is easily accessible by anyone.

What cannot be seen with a naked eye can be revealed using special sensors and technology components that are getting cheaper, smaller and more capable.

Even when not actively used, a good portion of wireless devices leak radio signals that can be collected, processed and possibly even matched to a specific device.

These signals can also be labelled as digital fingerprints or wireless traces or footprints. Most wireless devices have a unique identifier such as the MAC address for Wi-Fi and BD_ADDR address for Bluetooth and these identifiers can be captured using commodity technology.

While a number of protocol improvements add privacy preservation mechanisms, research suggests that characteristics of wireless radio signals transmitted by individual devices can also be used to obtain highly unique traces.

A single wireless trace may not be very useful, but a collection of traces over time and multiple locations can be quite revealing.

There is an obvious privacy concern here, as tracking wireless devices based on their fingerprints naturally leads to tracking people. Yet, the potential benefits may outweigh these risks.

The concept of visitor analytics, for example, has gained popularity in the retail sector to provide businesses with greater visibility into the visiting habits of their stores. These analytics solutions are able to detect repeat visitors and gauge their visit duration with impressive location accuracy.

Fortunately, these solutions usually aim to incorporate privacy preservation measures and are more likely to be interested in a summary view rather than tracking of specific devices.

Similarly, a better understanding of city environments based on wireless footprints can result in more informed urban planning decisions aimed at making our cities smarter, safer and more liveable.

For example, traffic analyses based on wireless signals could be used to tackle congestion.

Continued on the next page

Your wireless footprint can help police catch a thief (continued)

Theft of devices

But more importantly, wireless devices and cars are also an attractive target for burglars and car thieves.

Burglaries and theft are a growing issue in Australia. In particular, Western Australia was earlier this year labelled as the "home invasion and car theft capital" of all Australian states and territories.

Fortunately, a solution might be in sight if we consider the use of wireless traces to track and locate stolen items, provided that device fingerprints are known to the police. While voluntary MAC and BD_ADDR registrations can easily be facilitated, maintaining a database of radio signal-based fingerprints will be tricky.

But finding a stolen device could be as simple as scanning the air for its presence using a known digital fingerprint. These traces can usually be recognised from up to a 100 metres and even further away using specialised equipment.

Despite the apparent logistical and possible legal challenges, the concept has significant potential.

The idea is to disrupt the criminal network by making the use and circulation of stolen property less viable. Knowing that an unlawfully obtained laptop or a smart TV can be found could discourage people from buying or selling these items.

The solution could also reduce the claim stress faced by the insurance companies in the wake of these types of crime.

To stop the traces from being discovered, the wireless on the device would need to be turned off and in many cases this would make it useless.

With cars that have an in-dash entertainment unit with wireless technology, the unit would need to be removed or replaced and that represents additional and likely undesirable effort.

Practical attempts to leverage wireless traces for law enforcement are already taking place. A proof-of-concept solution called L8NT ("latent") that uses Wi-Fi has been on trial in the US state of Iowa late last year.

Video: https://youtu.be/4Fr6ceUrxAk

While the concept is simple and the underlying technology is readily accessible, there will be significant challenges to overcome. To be effective, the solution will require a widespread sensor network and integration of additional technology into the police cars, public transport and city infrastructure. Drones can also be used to fly sensors up in the air for increased coverage.

Certain types of wireless footprints can also be easily spoofed on some devices and techie criminals will likely learn and use tricks to effectively hide these devices. But, it is unlikely that an average home burglar will have the necessary technical skills to use these techniques

Source: *http://theconversation.com/your-wireless-footprint-can-help-police-catch-a-thief-60117*

UK: The car that locks out cyber criminals: Hack-proof black cab to be unveiled in London could be the future of transport

By Ryan O'Hare, MailOnLine, 27 June 2016

- A British firm claims to have made the first hack-proof security system
- It uses a series of firewalls and unique data keys which can't be cloned
- Experts have warned vulnerability of car computers is a major concern
- The system is fitted in the next generation of London taxi, the Metrocab

Cybercriminals on the lookout for a vehicle to hack may soon face stiff opposition, as experts claim to have made the first hack-proof car.

Would-be hackers have turned to targeting cars as on-board computers become increasingly common to control locking and safety systems – such as auto braking and power steering.

The system relies on a series of firewalls and unique data keys which can't be cloned to keep vehicles from being hacked. It will be fitted in electric Metrocabs, set to hit London's streets (pictured).

Experts say that bolstering security and making vehicles impervious to cyber criminals is a crucial step as autonomous vehicles roll out in coming years.

According toThe Times, the 'banking-style' security system will make it close to impossible for hackers to gain access from outside the vehicle.

The system, developed by Camberley-based firm Frazer-Nash Research, will be unveiled tomorrow at Connected Cars '16 at Olympia in London and will be fitted in Ecotive's Metrocab, which began trials on London's streets last year.

Greg Starns, executive director software at Frazer-Nash, said: 'These additional safety measures will help protect drivers and their passengers from the increase in malicious hacking we are seeing on the roads today.'

The Times reports a series of firewalls and unique data keys which can't be cloned are at the heart of the security system, which leave the vehicles closed to would-be cyber-attacks.

Despite car makers' efforts to thwart hackers, a number of high profile attacks have made the headlines in recent years.

In 2014, security experts compiling a list of most vulnerable makes and models of car listed the Jeep Cherokee as the most hackable car, followed by Cadillac's Escalade.

Demonstrating the vulnerabilities of the Cherokee last year, security experts hacked into the vehicle's computer via its Wi-Fi connection. Using just a phone and a laptop, the hackers were able to gain control over critical safety systems to apply the brakes and steer the car into a ditch as it drove.

With self-driving cars already hitting the road for tests, security experts have warned of the potential to hack the connected systems.

Most recently, a security expert revealed how easy it is to fool the remote sensing technology on self-driving vehicles by proving it can be done using basic, off-the-shelf equipment.

Continued on the next page

UK: The car that locks out cyber criminals: Hack-proof black cab to be unveiled in London could be the future of transport (Continued)

During tests, researcher Jonathan Petit at the University of Cork said he was able to trick the sensors into seeing 'echoes' of cars or pedestrians from a distance of 330ft (100 metres) using a simple laser pointer.

In an effort to block such security blunders, the new 'hack-proof' security system is based on three factors, The Times reports.

Initially, drivers will need to connect their keys to the car's software to get a unique code.

The car's computer systems are separated by firewalls, meaning hackers have to penetrate multiple levels of security rather than gain a single entry.

Finally, data sent to the car is verified by a triple-check system similar to that used by banks to protect people banking online.

Tomorrow will see the system demonstrated in the next generation London cabs.

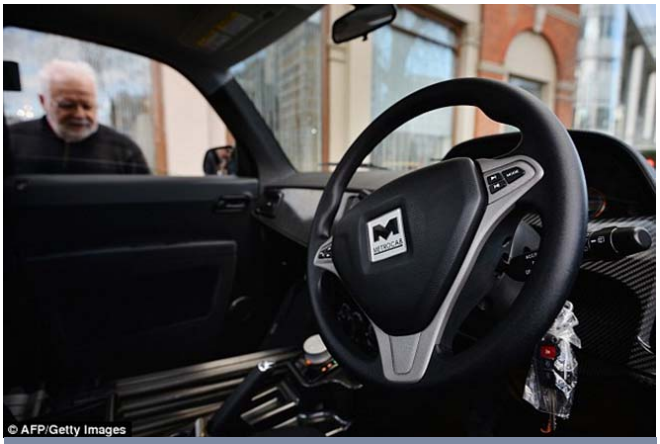
Designed and built in Britain, the zero-emission electric Metrocab runs on a powerful, near-silent electric motor.

Inside there is seating for up to seven passengers, complete
with a USB charging socket, panoramic glass roof and colour TV displays.

Noamaan Siddiqi, general manager at Frazer-Nash, said: “This pioneering technology is a game-changer for passenger experience. It will also help passengers travel in comfort and put those lost hours stuck in traffic to good use.”

He added: “We are redefining the way people travel. With the connectivity we are offering in the cab, passengers will be able to check emails, watch videos, travel in comfort and have an overall more productive journey.”

The vehicle's computer systems are separated by firewalls, meaning hackers have to penetrate multiple levels of security rather than gain a single entry, making any cyber-attack much more difficult.



Locked out: Car security experts claim to have made Britain's first 'hack-proof' car. The system will be fitted in electric Metrocabs (pictured), which began trials on London's streets last year

Source: *http://www.dailymail.co.uk/sciencetech/article-3662011/The-car-locks-cyber-criminals-Hack-proof-black-cab-unveiled-London-future-transport.html*

IN THE NEWS

USA: Thieves Go High-Tech to Steal Cars

By Jeff Bennett, 5 July 2016

Police say vehicle electronics co-opted to bypass ignition controls in late-model vehicles

Police and car insurers say thieves are using laptop computers to hack into late-model cars' electronic ignitions to steal the vehicles, raising alarms about the auto industry's greater use of computer controls.

The discovery follows a recent incident in Houston in which a pair of car thieves were caught on camera using a laptop to start a 2010 Jeep Wrangler and steal it from the owner's driveway. Police say the same method may have been used in the theft of four other late-model Wranglers and Cherokees in the city. None of the vehicles has been recovered.

"If you are going to hot-wire a car, you don't bring along a laptop," said Senior Officer James Woods, who has spent 23 years in the Houston Police Department's auto antitheft unit. "We don't know what he is exactly doing with the laptop, but my guess is he is tapping into the car's computer and marrying it with a key he may already have with him so he can start the car."

The National Insurance Crime Bureau, an insurance-industry group that tracks car thefts across the U.S., said it recently has begun to see police reports that tie thefts of newer-model cars to what it calls "mystery" electronic devices.

"We think it is becoming the new way of stealing cars," said NICB Vice President Roger Morris. "The public, law enforcement and the manufacturers need to be aware."

Fiat Chrysler Automobiles NV said it "takes the safety and security of its customers seriously and incorporates security features in its vehicles that help to reduce the risk of unauthorized and unlawful access to vehicle systems and wireless communications."

A homeowner's security-camera video shows thieves in Houston using a laptop to thwart electronic-ignition control and start a 2010 Jeep Wrangler and drive away. Video Link: https://youtu.be/drCZTjvW0Ag

On Wednesday, a Fiat Chrysler official said he believes the Houston thieves "are using dealer tools to marry another key fob to the car."

Titus Melnyk, the auto maker's senior manager of security architecture for North America, said an individual with access to a dealer website may have sold the information to a thief. The thief will enter the vehicle identification number on the site and receive a code. The code is entered into the car's computer triggering the acceptance of the new key.

The recent reports highlight the vulnerabilities created as cars become more computerized and advanced technology finds its way into more vehicles. Fiat Chrysler, General Motors Co. and Tesla Motors Inc. have had to alter their car electronics over the last two years after learning their vehicles could be hacked.

Continued on the next page

USA: Thieves Go High-Tech to Steal Cars (continued)

Fiat Chrysler last year recalled 1.4 million vehicles to close a software loophole that allowed two hackers to remotely access a 2014 Jeep Cherokee and take control of the vehicle's engine, air conditioning, radio and windshield wipers.

Startups and auto-parts makers also are getting involved in cyber protections for cars. "In an era where we call our cars computers on wheels, it becomes more and more difficult to stop hacking," said Yoni Heilbronn, vice president of marketing for Israel-based Argus Cyber Security Ltd., a company developing technologies to stop or detect hackers. "What we now need is multiple layers of protection to make the efforts of carrying out a cyberattack very costly and deter hackers from spending the time and effort."

San Francisco-based Voyomotive LLC is developing a mobile application that when used with a relay switch installed on the car's engine can prevent hackers with their own electronic key from starting a vehicle. Its technology also will repeatedly relock a car's doors if they are accessed by a hacker.

This month, U.S. Secretary of Transportation Anthony Foxx is slated to attend an inaugural global automotive cybersecurity summit in Detroit. General Motors Co. Chief Executive Mary Barra and other industry executives are scheduled to speak.

Automotive industry trade groups are working on a blueprint of best practices for safely introducing new technologies. The Auto-Information Sharing and Analysis Center, created by the Alliance of Automobile Manufacturers and the Global Automakers Association, provides a way to share information on cyberthreats and incorporate cybercrime prevention technologies.

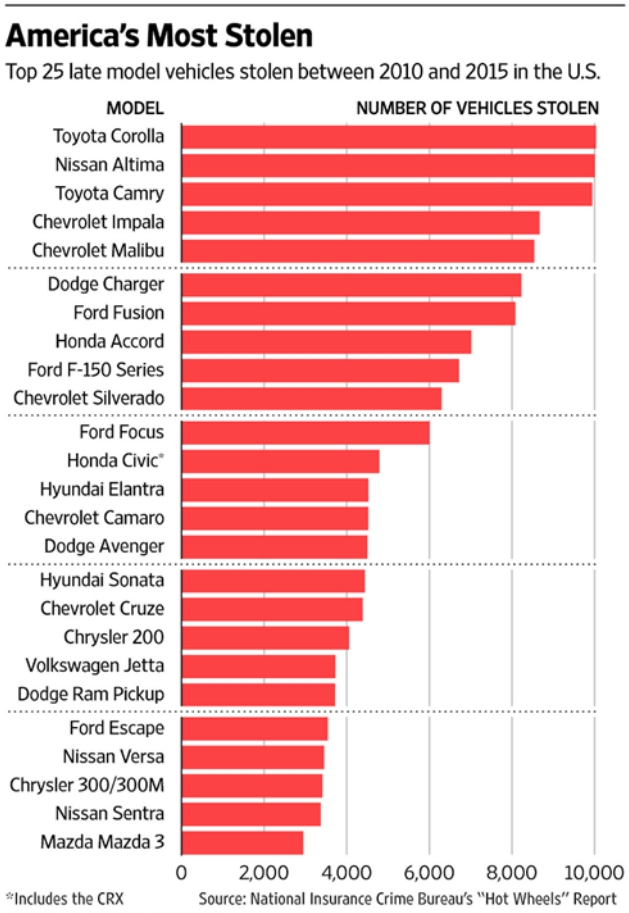
In the Houston car theft, a home-security camera captures a man walking to the Jeep and opening the hood. Officer Woods said he suspects the man is cutting the alarm. About 10 minutes later, after a car door is jimmied open, another man enters the Jeep, works on the laptop and then backs the car out of the driveway.

"We still haven't received any tips," the officer said.

The thief, says the NICB's Mr. Morris, likely used the laptop to manipulate the car's computer to recognize a signal sent from an electronic key the thief then used to turn on the ignition. The computer reads the signal and allows the key to turn.

"We have no idea how many cars have been broken into using this method," Mr. Morris said. "We think it is minuscule in the overall car thefts but it does show these hackers will do anything to stay one step ahead."

Source: *http://www.wsj.com/articles/thieves-go-high-tech-to-steal-cars-1467744606*



LoJack Announces a New Era in Vehicle Theft

By Ali Raza, HackRead, 3 May 2016

CANTON, Mass., July 1, 2015 -- As vehicle theft continues to evolve and expand beyond traditional methods, LoJack Corporation (NASDAQ: LOJN), a leader in vehicle theft recovery, today introduced 'The Connected Vehicle Thief' Era to open National Vehicle Theft Protection Month. According to a survey conducted by Gallup, 42 percent of Americans frequently or occasionally fear that their vehicle will be stolen or broken into.LoJack cautions that the nature of vehicle theft has changed and one of the vehicle owner's adversaries is a smarter, connected and more targeted network of thieves.

"The FBI reports in its 2013 Uniform Crime Report that a vehicle is stolen every 45.1 seconds in the United States, which amounts to more than $4.1 billion in lost assets each year," saidPatrick Clancy, Vice President of Law Enforcement, LoJack Corporation.

"With only 54.8 percent* of stolen vehicles being recovered, auto theft is still a serious problem and we are now dealing with a more advanced, sophisticated thief. These individuals are increasingly creative, connected and dangerous in their approaches to steal your valuable assets."

"In recent years, the traditional methods, techniques and mindset towards auto theft has evolved," Clancy continues.

"Although numbers show a decline in theft, the impact that today's Connected Vehicle Thief has on the individuals and businesses that fall victim to them is much greater. We rely on our vehicles for much more than just transportation. Today, our vehicles hold critical information such as our phone contacts, registration and insurance details, even the address and directions to our home - making entry, theft and further damage even more of a possibility. Vehicles are truly an extension of our connected self and without it, we are less productive and informed and risk becoming exposed to the outside world."

With the emergence of new technology, LoJack cautions vehicle owners against 'The Connected Vehicle Thief.' These thieves have adapted techniques and methods to steal expensive, critical assets, such as cars, fleet vehicles and commercial equipment by adhering to key trends:

- **Smart cars = Smarter thieves**: Thieves have become more advanced in their techniques, which includes: illegally acquiring and copying smart keys, using GPS and manufactured keys to target rental vehicles, using stolen credit reports and creating false identities to finance vehicles at dealerships and VIN cloning.

- **Go big, Go home, or Go overseas**: Thieves have placed a great emphasis on expensive vehicles. Whether it be a brand new 2015 BMW X3 or a 1965 Ford Mustang, 'The Connected Vehicle Thief' is targeting cars that are valuable on the open market. Many of these thieves are taking and filling orders based on black market demands. Thieves know they can get the most value by targeting new, or rare, vehicles that are worth a substantial amount of money when they are exported and shipped overseas. Often times, new cars are stolen and placed in shipping containers or are part of an elaborate, large international crime operation.

- **The Connected Vehicle Thief Can Cost You Money and Your Identity**: In an increasingly connected-era, cars are more important than ever before. According to LoJack's latest recovery data, the average value of vehicles stolen and recovered is more than $10,000**. In addition, vehicle theft has a glaring impact on rising insurance rates - an added cost to the vehicle owner. There's also a troubling link between car theft and identity theft, as thieves not only take a person's vehicle, but their identity when documents containing personal information such as a vehicle registration or even bills are left in a vehicle.

Continued on the next page

LoJack Announces a New Era in Vehicle Theft (continued)

- **The Impact on Commercial and Fleet Businesses**: The average value of vehicles stolen does not take into account the significant costs associated with theft, including loss in job productivity, critical data, transportation and overall professional impact. For example:
    - A small business owner has a generator stolen from a job site and costs them time off a job and a substantial amount of money to replace the equipment.
    - The construction business owner who has a piece of heavy equipment stolen, such as a front loader, can't complete a job on time.
    - The fleet owner who has a dump truck stolen can't complete a job, or take on new work, without the vehicle.

"Auto theft is having a tremendous impact on our day-to-day lives and these smarter, more advanced thieves can be extremely dangerous," said Chris McDonald, former president of the International Association of Auto Theft Investigators and executive director with the Maryland Vehicle Theft Prevention Council.

"With advancements in technology, it is much more difficult for thieves to gain access to the vehicle without a smart key or key fob. As such, we are seeing an uptick in home burglaries and violent crimes in order to gain access to the vehicle. Although the numbers might say auto theft is declining, we need to be more vigilant than ever before in order to protect our assets, and more importantly ourselves, from this new breed of smart and dangerous criminals."

Educational resources available to vehicle owners this July and beyond include:

- **'LoDown With LoJack' - Auto Theft Trends video** highlighting auto theft trends from around the country and the importance of vehicle security systems in combating today's sophisticated thief.
- **Tips from IAATI and LoJack** for consumers to help protect and keep their vehicle assets safe. By adhering to a multi-layered theft prevention approach - which includes common sense approaches, theft prevention and immobilization devices, and tracking/recovery systems - consumers can better protect their vehicles from theft.
- **LoJack's Sixth Annual Vehicle Theft Recovery Report, infographic and slideshow** reviewing auto theft trends over the past year specific to vehicles equipped with the LoJack® Stolen Vehicle Recovery System.

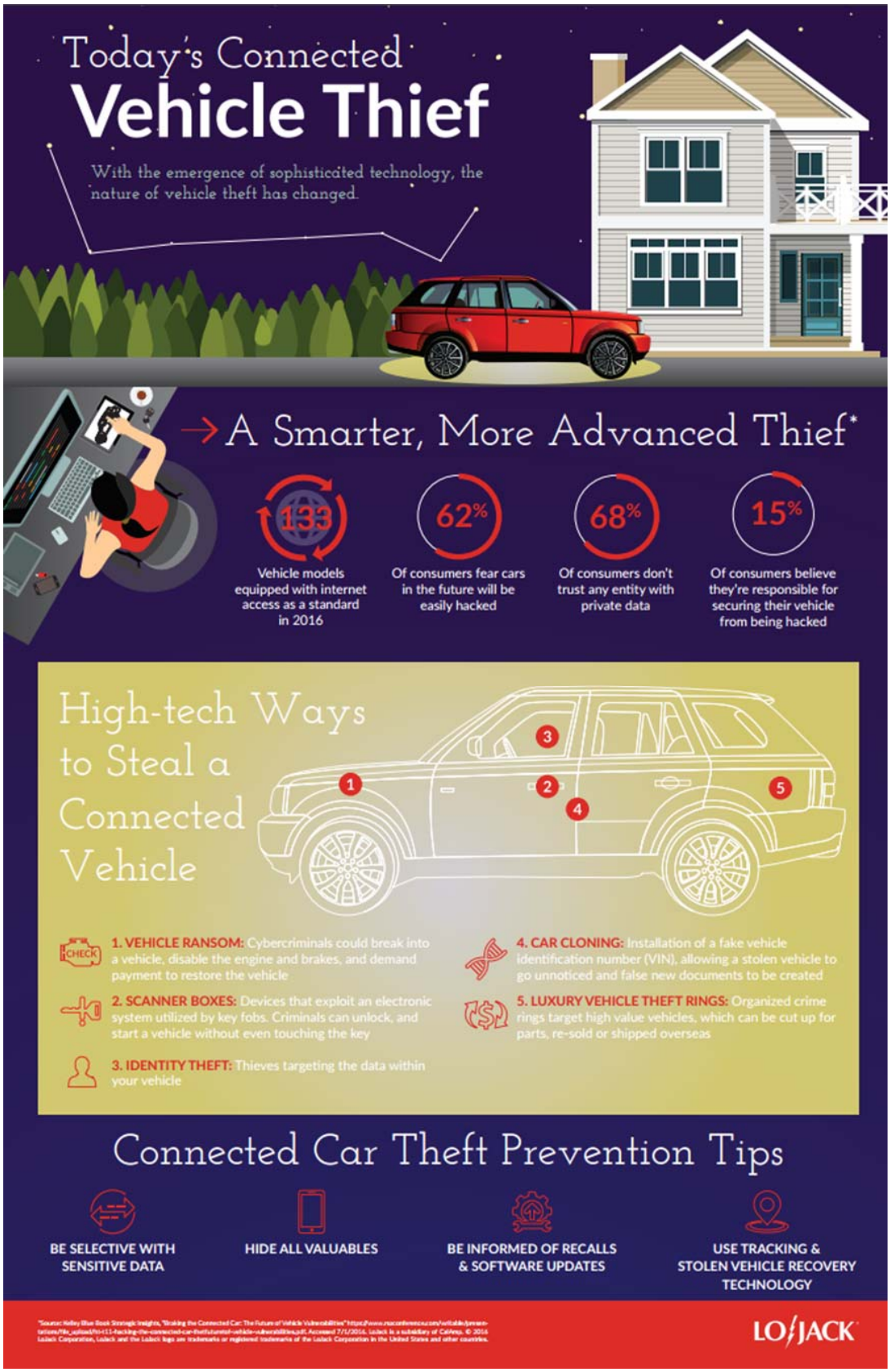
For more information from LoJack and tips for how to keep your valuable assets safe during National Vehicle Theft Protection Month, please visit www.lojack.com.

*Source: 2013 FBI Uniform Crime Report
**Source: Used Car values are best estimates derived from: NADA Guide web services values and clean retail value fromNADAGuides.com for the make, model and year of the vehicle in the month that it was recovered.

Source: *https://www.lojack.com/About-LoJack/News-and-Media/Press-Releases/2015/LoJack-Announces-a-New-Era-in-Vehicle-Theft*

See Lojack's infographic on the next page. To download this infographic either click on the image or use the following link: *http://www.autotheftblog.com/wp-content/uploads/2016/07/FINAL_2016_LoJack_Vehicle_Thief_Infographic_as-of-7.7.16.pdf*

IN THE NEWS


Today's Connected
Vehicle Thief
With the emergence of sophisticated technology, the nature of vehicle theft has changed.
A Smarter, More Advanced Thief*
133
Vehicle models equipped with internet access as a standard in 2016
62%
Of consumers fear cars in the future will be easily hacked
68%
Of consumers don't trust any entity with private data
15%
Of consumers believe they're responsible for securing their vehicle from being hacked
High-tech Ways to Steal a Connected Vehicle
1
2
3
4
5
1. VEHICLE RANSOM: Cybercriminals could break into a vehicle, disable the engine and brakes, and demand payment to restore the vehicle
2. SCANNER BOXES: Devices that exploit an electronic system utilized by key fobs. Criminals can unlock, and start a vehicle without even touching the key
3. IDENTITY THEFT: Thieves targeting the data within your vehicle
4. CAR CLONING: Installation of a fake vehicle identification number (VIN), allowing a stolen vehicle to go unnoticed and false new documents to be created
5. LUXURY VEHICLE THEFT RINGS: Organized crime rings target high value vehicles, which can be cut up for parts, re-sold or shipped overseas
Connected Car Theft Prevention Tips
BE SELECTIVE WITH SENSITIVE DATA
HIDE ALL VALUABLES
BE INFORMED OF RECALLS & SOFTWARE UPDATES
USE TRACKING & STOLEN VEHICLE RECOVERY TECHNOLOGY
LOJACK

IN THE NEWS

Indian Man Rents Car, Sells it Online, Then Steals it Back on the Same Night

By Nextshark.com, 7 July 2016

A 28-year-old man is in police custody after stealing back the same car he sold online with a duplicate key.

The New Delhi man resorted to the con because his spa business is struggling to stay afloat. According to Hindustan Times, the BCA graduate rented a car and sold it on an ecommerce site. Of course, since he wasn't the owner, Kumar had to steal the car back the same night from the person he sold it to.

Police eventually got word of the theft. Last week, authorities at the Dwarka Sector 23 station examined the vehicle's record, but found that the details corresponded to another Mahindra XUV that was owned by a Delhi resident.

An officer explained what seemed to be going on. He said: "The owner was not lying. He had bought the car through the site. It was stolen the same night. Initially we thought he was sold a stolen vehicle but later we suspected the seller may have stolen the same car from the new owner. We registered a case and began probe."

As the investigation went on, police received a tip regarding a man planning to sell a Mahindra XUV and that's how Kumar's golden days of sale came to an end.

Kumar, the son of a retired captain of the Indian Army, revealed that he rented the car two months back when his massage parlour and spa in Faridabad was faltering. He then looked for a similar automobile and took note of its details to provide false information to his buyers.

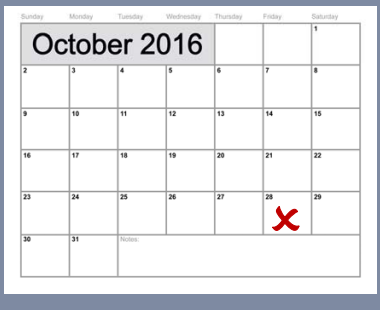
Following his first sale, Kumar stole the car back from its new owner within seven hours of the transaction. Using GPS and a duplicate key, Kumar was able to track down the vehicle and retrieve the rental car. The person responsible for renting the auto to Kumar had no knowledge of the scheme.

Car theft is rampant in India. In the first quarter of 2016, 9,714 vehicles were stolen in Delhi, Times of India reported. This number is a huge leap from last year's 6,724. During the period, a vehicle was stolen every 13 minutes and only 4% were recovered, the outlet said.

Source: *http://nextshark.com/india-man-steals-car-he-sold/*

September Issue of Auto Theft Today — Publication deadline

The next issue of Auto Theft Today will be released in November 2016. If you have any articles, photographs, member news, or anything else you would like included in the next issue please email it to: **PThomas@iaati.org** by **Friday 28th October 2016**



Super Natwarlal: 77-year-old thief who can't stop stealing

By Prawesh Lama, Hindustan Times, New Delhi, 8 July 2016

Old habits die hard and Dhani Ram Mittal can't stop stealing a car or two even at 77.

The man — known in police records as Super Natwarlal, Indian Charles Sobhraj, and simply as Super Thief — was arrested for the 25th time on Tuesday since he first landed in prison in 1964.

The septuagenarian kleptomaniac was released on bail only in June after his arrest early this year for a car theft. He allegedly stole at least four cars in the past month.

In his 52-year career in crime, he has amassed at least 128 FIRs; posed as a cop, a judge, a police inspector and government officer, among others.

In the late 1960s, he was a clerk in a Rohtak court. When the judge went on a vacation, he took his chair for over two months and gave bail to many criminals.

A graduate in law and a student of calligraphy, Mittal posed as regional transport officers too and forged car papers. He argues his own case in court.

He had even landed the job of the Rohtak railway station master in 1968, producing fake documents. But was sacked a year later after his bluff was called.

Dhani Ram Mittal, 77, has been arrested 25 times and has 128 FIRs against his name.

He was arrested this Tuesday after a police team found him driving a Maruti Esteem, which he had allegedly stolen in June.

CCTV footage shows it takes less than a minute for Mittal to break into a car. "That man is a pro. My car was an old Maruti 800 and the CCTV outside my house caught him in the act. It took him less than a minute. I am surprised how a 77-year -old could do that," a Rohini resident said.

He is old but refuses to change his ways, an investigator explained.

"He says he cannot do without stealing. He steals old cars such as Esteems, Maruti 800s, Hyundai Santros, which do not have security alarms and digital keys. He pretends to be on the phone and uses a master key to break into old cars."

Police said he must have stolen around 500 cars so far. Mittal allegedly sold his loot to used-car dealers in west Delhi for Rs 30,000 to Rs 50,000 apiece, depending on the vehicle's condition.

"He does not need the money. But he has always been a con man. He cannot do anything else, though he is old," the officer said.

Prison officials know the old, familiar jailbird too, who refuses to be lodged in the separate ward where elderly prisoners are kept. He prefers to hang around with the younger lot, which gives the opportunity to form a new gang each time he goes to prison.

"Every time he goes inside, he makes different associates. He wins the confidence of other prisoners with his legal advice. He has argued their cases too in Delhi courts," said a police officer.

Outside the high walls of jail, Mittal is a family man, living with his wife and a daughter-in-law in outer Delhi's Narela. Frustrated over his refusal to reform, his two sons left him and live separately.

Source: *http://www.hindustantimes.com/delhi/super-natwarlal-77-year-old-thief-who-can-t-stop-stealing/story-hwNIe0Wa1nFVkYd6DT6YaO.html*

Phillippines: Car thieves face longer terms under new law

By News Philippines , 19 July 2016

A new Anti-Carnapping Act imposes jail terms up to life imprisonment, a measure that its proponent, Sen. Grace Poe, hopes would deter a crime that has long been rampant across the country.

Poe said President Duterte had "allowed the measure to lapse into law" 30 days after it was forwarded to Malacañang on June 16 and then President Benigno Aquino III took no action on it.

"It is our hope that this new and comprehensive Anti-Carnapping Act imposing much stiffer penalties, alongside strict implementation by our law enforcers, will hinder the commission of this crime and give vehicle owners peace of mind," Poe said, who sponsored the bill in the 16th Congress.

Amendments

The new measure supplants the law against car theft enacted in 1972 and amendments to car theft penalties imposed by Republic Act No. 7659, or the law laying down penalties for heinous crimes.

In pushing for the measure in May last year, Poe noted car thefts had totaled more than 44,000 from 2009 to 2013. In the first half of 2015 alone, car theft cases reached 10,039, nearly twice the 5,599 recorded during the same period in 2014.

Under the new law, convicted car thieves face a jail term of 20-30 years, roughly double the 14 years and eight months to 17 years and four months under the old law.

Higher penalty

The penalty is higher if the crime involves "violence, intimidation and force," with the jail term raised to 30 years and one day to up to 40 years, from the previous 17 to 30 years.

If the crime results in murder or rape, the penalty is life imprisonment.

A person who has knowledge of the crime but keeps quiet about it—regarded as "concealment of the crime of carnapping"—faces a prison term of 6-12 years and a fine corresponding to the cost of the motor vehicle, engine or any other part involved in the violation.

The law requires those seeking original registration for any vehicle to get clearance from the Philippine National Police and the Land Transportation Office (LTO), a step that would determine if an applicant is clear of any criminal involvement.

Permanent database

The law also reiterates the need for the LTO to maintain a permanent database of all motor vehicles in the country and their present and previous owners, plus details on the vehicles such as "motor vehicle engines, engine blocks and chassis of all motor vehicles stating the type, make, and serial numbers."

The law considers a crime the tampering with serial numbers and transfer of license plates without LTO approval and the sale of secondhand spare parts from stolen vehicles.

Source: *http://newsphilippines.net/car-thieves-face-longer-terms-under-new-law*

Brake pedal data can fingerprint drivers with 87% accuracy in 15 minutes

By Kiki der Gerko, Network World, 20 July, 2016

Have you opted for lower car insurance premiums via installing an insurance-supplied dongle? If so, then did you realize that dongle could narc you out when brake pedal usage is used as a biometric identifier?

If you are thinking surely not, then think again, as researchers had nearly a 90% accuracy in identifying drivers via brake pedal sensor data after only 15 minutes of driving.

Yesterday, researchers from the University of Washington and of California presented "Automobile Driver Fingerprinting" (pdf) at PETS 2016, short for Privacy Enhancing Technologies Symposium.

The abstract states: "While we do not know of attempts by automotive manufacturers or makers of after-market components (like insurance dongles) to violate privacy, a key question we ask is: could they (or their collection and later accidental leaks of data) violate a driver's privacy?"

They used 15 drivers for their study and logged data from 16 in-vehicle sensors collected by a car's CAN (controller area-network) bus. For the study, they had the drivers perform maneuvers in an isolated parking lot, as well as drive in traffic along a 50-mile loop in Seattle.

The researchers determined that "drivers are indeed distinguishable using only in-car sensors." The top sensor to fingerprint drivers was the brake pedal.

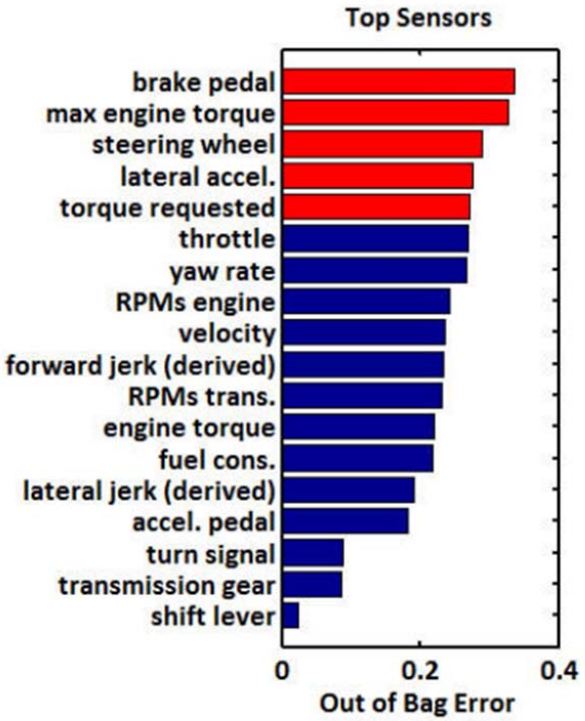


Fig. 3. Top sensors shown in sorted order of their ability to differentiate between drivers (top 5 sensors are shown in red). The brake pedal position is the most telling indicator of a driver's style. The next most relevant sensor is the max engine torque.

Automobile Driver Fingerprinting by Miro Enev, Alex Takahuwa, Karl Koscher, and Tadayoshi Kohno

Brake pedal data can fingerprint drivers with 87% accuracy in 15 minutes (continued)

Some of the researchers' key findings included:

- 100% driver ID among 15 drivers is possible using 15 sensors and the entire database of driving data.
- 100% driver ID among 15 drivers is possible using just the brake pedal and the entire database for training.
- 100% ID among 15 drivers is possible given short training datasets (8 mins, 15 mins, 1 hour) and multiple sensors.
- 87% accuracy is achievable using a single sensor (brake pedal) and only the first 15 minutes of open-road driving as a training database; the 15 minutes was broken down as 13.5 minutes training and only 1.5 minutes of test data.

They aren't saying it's all bad, as driver fingerprinting could be used for vehicle theft detection, but there are plenty of privacy risks. There is also a growing data-sharing aftermarket, such as insurance companies offering dongles for rate reductions, dongles that offer diagnostics and even some that offer concierge services.

Potential driver fingerprinting privacy violations

It's not a new idea that companies can tell a great deal about you, good and bad, via the data collected from modern vehicles. For example, Jim Farley, executive vice president for Ford Motor Co., said in 2014, "We know everyone who breaks the law. We know where and when you are doing it. We have GPS and other technologies in your car, so we know what you are doing."

After Farley's statements caused an uproar, he retracted his statements.

Since drivers can be "fingerprinted" by the data, the researchers proposed potential privacy risks. They wrote:

While we anticipated some level of de-anonymization success, our results are surprising given the apparent potential of vehicle sensor data present in stock vehicles to distinguish between individuals given limited time and restricted access to sensors. We view this as a significant result since it implies that even simple devices—such as insurance dongles attached to a car's internal computer network—have the potential to violate privacy.

Good ole Alice and Bob were featured in numerous scenarios about potential privacy problems. If a red-light camera snaps a shot of a car running a light, and Alice says she wasn't driving because she loaned her car to Bob, then police could obtain data from the insurance dongle connected to the car. Then it's bad news for Alice when the data indicates she was driving, not Bob.

If Alice and Bob rented a car together, but Alice was the only "authorized driver" and Bob also drives, then the rental company could tap into the dongle data to detect Alice was not driving. Say hello to fines and added fees from the rental agency after the rental agreement was broken.

In another scenario, Alice bought only daytime insurance coverage for her son, Bob. But the insurance company uses the data from its dongle to detect that Bob is driving at night and then cancel Alice's insurance.

Alice could install a monitoring dongle in Bob's car if she wanted to know if his "significant other" was driving, and then receive a real-time text message if the dongle detects a driver other than Bob.

The dongle in Alice and Bob's car could detect which one was driving and then push targeted ad text messages, such as for a favorite restaurant, depending upon who was driving.

The researchers advised drivers to be wary about sharing their vehicle data "without substantial guarantees for superior service." The companies collecting that data have a responsibility to offer privacy controls for users and "develop safeguards for data processing and retention that keep up with the evolving threat model landscape."

Source: *http://www.networkworld.com/article/3097579/security/brake-pedal-data-can-fingerprint-drivers-with-87-accuracy-in-15-minutes.html*

UK: Car theft gang convicted

By Metroplitan Police, 19 July 2016

Four men who stole at least nine high-value vehicles worth approximately £680,000 were convicted yesterday, Monday 18 July, at Snaresbrook Crown Court.

- Adeel Arshad, 29 (31.5.87) of Church Road, Waltham Forest pleaded guilty to conspiracy to steal and conspiracy to handle stolen goods.
- Hassan Iqbal, 26 (18.7.90) of Helena Road, Waltham Forest pleaded not guilty to conspiracy to steal and conspiracy to handle stolen goods. He entered a guilty plea at the start of the trial.
- Ban Cooper, 21 (14.1.95) of Beavon Close, Huntingdon pleaded guilty to conspiracy to steal.

- Farasat Bhamjee, 28 (25.8.87) of Northumberland Road, Waltham Forest was found guilty of conspiracy to steal and conspiracy to handle stolen goods.

All four will be sentenced on 9 September. The gang stole the vehicles - the majority of which were Range Rovers - using sophisticated car security technology. They carried out their offences in areas likely to be frequented by drivers of high-value vehicles, such as wealthy areas of London and shopping centres.

Once a suitable vehicle was identified, the gang would tail-gate the vehicle, to enable them to park nearby. They would then wait for the driver to leave the vehicle and attempt to lock it. At this point, the gang member would activate a jamming device, preventing the vehicle from being locked. In the majority of cases the victims believed their cars were secure and walked away.

At this point entry was gained to the unsecure vehicle and an onboard diagnostic device [OBD] would be connected to the vehicle's computer, enabling a new key code to be issued to one of the Range Rover fobs in their possession.

Although the thieves at this point had a working key, they did not steal the vehicle at that time. Instead, they installed a tracking device that would enable the gang to track and locate the vehicle in order to steal it at a later date, usually in the early hours of the morning. It is believed this was to minimise the risk to the criminal network of being caught while stealing or driving a stolen vehicle. The vehicle was then driven away from the owner's address to a location where any legitimate tracking device on the vehicle was removed.

Police launched an investigation after establishing a link between a number of the crimes, and subsequently arrested Arshad, Iqbal and Bhamjee in a stolen Range Rover. A garage controlled by Arshad and Bhamjee was found to contain tracking devices, Range Rover fobs, jammers and GPS 'cloaking' devices.

Four vehicles have now been recovered by police in containers ready for export at both Felixstowe and Southampton docks and returned to their owners.

Detective Constable Julian Thompson of Waltham Forest police said: "These offences caused distress and huge inconvenience to a number of victims across London and I'm pleased that these men have now been convicted.

"Whilst this type of crime is sophisticated in nature, there are certain things car owners can do to reduce the risk of becoming a victim. I would urge high-value car owners to always double check that their car is locked before leaving it, and consider using a steering-wheel lock device."

Source: *http://news.met.police.uk/news/car-theft-gang-convicted-175281*

Canada: Police-reported crime statistics in Canada, 2015: Motor vehicle theft increases 6%

Excerpts from a report by Mary Allen, Statistics Canada, 20 July 2016 2016

- In 2015, police-reported crime in Canada, as measured by both the crime rate and the Crime Severity Index (CSI), increased for the first time since 2003. The CSI measures the volume and severity of police-reported crime in Canada, and has a base index value of 100 for 2006. The CSI increased 5% from 66.7 in 2014 to 69.7 in 2015. The 2015 CSI was 1% higher than the CSI reported in 2013 (68.8), but 31% lower than a decade earlier in 2005.
- The change in the CSI in 2015 was driven primarily by increases in fraud, breaking and entering, robbery, and homicide. The upward movement of the national CSI was fuelled by a notable growth in crime reported by Alberta.
- The police-reported crime rate, which measures the volume of police-reported crime, also increased in 2015, rising 3% from the previous year to 5,198 incidents per 100,000 population. This was about the same rate as reported in 2013 (5,195 per 100,000 population) and 29% lower than a decade earlier in 2005.
- Among the violent violations to increase in rate were homicide (+15%), attempted murder (+22%), major assaults (+3%), sexual assaults (+3%), robbery (+5%) and Criminal Code violations specific to the use of, discharge, and pointing of firearms (+22%) (referred to as violent firearms offences).
- The overall volume and severity of violent crime, as measured by the violent CSI, increased 6% between 2014 and 2015 to 74.5. This increase was largely the result of increases in robbery, homicide, attempted murder, and violent firearms offences.
- Police-reported crime rates for all types of property crimes increased in 2015, including fraud (+15%), possession of stolen property (+13%), theft over $5,000 (excluding motor vehicles) (+8%), identity fraud (+9%), motor vehicle theft (+6%) and breaking and entering (+4%).
- The overall volume and severity of non-violent crime, as measured by the non-violent CSI rose to 67.8 in 2015, marking a 4% increase from the previous year. The increase was largely the result of more reported incidents of fraud and breaking and entering.

Motor vehicle theft up due to increases in Alberta

There were nearly 79,000 incidents of motor vehicle theft reported by police in 2015, resulting in a rate of 220 per 100,000 population. Between 2014 and 2015, the rate of motor vehicle theft in Canada increased 6%. This was the second consecutive increase in the rate following ten years of declines (Chart 13). However, the rate of motor vehicle theft in 2015 was 56% lower than ten years earlier, marking the largest ten-year decline among all types of property crime (Table 5).

Table 5. Police-reported crime for selected offences, Canada, 2014 and 2015

Type of offence	2014		2015		Percent change in rate 2014 to 2015	Percent change in rate 2005 to 2015
	number	rate	number	rate	percent	
Theft of motor vehicle	74,010	208	78,849	220	6	-56

As with many other property offences, much of the increase in the rate of motor vehicle theft in 2015 can be attributed increased levels in Alberta (+32% increase in rate). Large increases in rates of motor vehicle theft were also reported in Yukon (+25%), Prince Edward Island (+19%), and the Northwest Territories (+18%), but with little impact on the change at the national level due to small numbers of incidents. However, a 14% decline in rates of motor vehicle theft in Quebec somewhat mitigated the impact of the increase in Alberta on the national rate.

Continued on the next page

Canada: Police-reported crime statistics in Canada, 2015 (continued)

The highest rates of motor vehicle theft in 2015 were reported in Alberta (532 per 100,000 population), the Northwest Territories (528 per 100,000 population) and Saskatchewan (427 per 100,000 population). Despite the large increase in rate reported in Prince Edward Island in 2015, it still had the lowest rate of motor vehicle theft (65 per 100,000 population) among all provinces and territories, followed by the other Atlantic provinces and Ontario (Table 6).

Increases in rates of motor vehicle theft in Alberta's two CMAs, Calgary (+67%) and Edmonton (+16%), accounted for most of the increased number of incidents at the national level in 2015. Windsor and Kitchener-Cambridge-Waterloo also had notably large increases in rates of motor vehicle theft in 2015 (+39% and +30% respectively). In contrast, Sherbrooke (-41%) and Saint John (-26%) reported relatively large declines (Table 7) .

Source: *http://www.statcan.gc.ca/pub/85-002-x/2016001/article/14642-eng.htm?fpv=2693*

Data table for Chart 13

Year	Breaking and entering	Motor vehicle theft
	rate per 100,000 population	
1984	1,394	299
1985	1,380	318
1986	1,399	328
1987	1,377	329
1988	1,341	334
1989	1,277	367
1990	1,370	412
1991	1,550	497
1992	1,506	518
1993	1,417	546
1994	1,338	550
1995	1,334	552
1996	1,341	608
1997	1,248	592
1998	1,163	550
1999	1,046	531
2000	956	522
2001	901	544
2002	879	516
2003	901	551
2004	864	532
2005	811	496
2006	772	487
2007	704	443
2008	635	378
2009	613	321
2010	579	272
2011	528	240
2012	507	225
2013	445	206
2014	428	208
2015	444	220

Note: Additional data are available on CANSIM (Table 252-0051). Populations are based upon July 1st estimates from Statistics Canada, Demography Division.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

Australia: Parts market regulation 'key to cutting car crime'

Insurancenews.com.au, 4 July 2016

Profit-motivated car crime is best stopped through regulatory reform, according to the National Motor Vehicle Theft Reduction Council (NMVTRC).

It says about 10,500 cars "appear to simply vanish altogether from our roads each year", indicating the extent to which organised crime is converting stolen vehicles into cash.

In the year to March 31, 9838 cars were stolen for profit, and the council believes illegal activity in the second-hand goods and scrap market accounts for at least half these crimes.

Task Force Discover, an NMVTRC and Victoria Police initiative, has found "a staggering level of regulatory non-compliance" across the market facilitates the laundering of stolen vehicles.

Now the council is calling for regulatory reforms in the vehicle scrap and parts industry.

It wants "consolidation of related laws to address critical omissions and anomalies", and "performance-based business standards set with peak industry bodies including environmental and occupational health and safety compliance".

It also calls for the adoption of "chain-of-responsibility principles to ensure stolen vehicles or parts are not traded" and a range of "search, seizure and other tools to assure compliance, including the application of court-enforced commercial penalties to neutralise illegal profits".

A recent Victorian Law Reform Commission report on regulatory regimes that prevent the infiltration of organised crime into lawful industries backs up the NMVTRC's position.

The report set out four strategies: assessment of the current regulatory regime; restricting entry to industry through licensing schemes; regulating post-entry behaviour; and addressing the use of professional facilitators.

The commission says "collaboration between government agencies and industry is key" and regulators need to engage with industry on identifying risks and developing a regulatory response.

Source: http://www.insurancenews.com.au/local/parts-market-regulation-key-to-cutting-car-crime

---

Netherlands: Annual car theft rate on course to drop below 10,000

DutchNews.nl, 11 July 2016

The number of car thefts fell by 7 per cent in the first half of 2016, continuing the steady downward trend of the last 20 years. The six-month figure of 4,776 means the annual figure is on course to dip below 10,000 for the first time since records began. Last year 5,180 privately owned vehicles were stolen, itself a 6 per cent drop on the same period in 2014, according to figures compiled by anti-vehicle crime group Stichting Avc. The group attributed the drop in part to better security and information exchanges between government vehicle agencies, making it harder for criminals to sell stolen cars over the border. Thefts of container lorries fell even more sharply by 27 per cent, while motorbike theft was down by 15 per cent and moped theft was 7 per cent lower.

Source: *http://www.dutchnews.nl/news/archives/2016/07/car-theft-figure-drops-by-6-per-cent/*

IN THE NEWS

Interpol: Stolen cars recovered in Spanish operation targeting vehicle trafficking

By Interpol, 5 August 2016 - http://www.interpol.int/News-and-media/News/2016/N2016-101

ALGECIRAS, Spain - An operation targeting the trafficking of stolen vehicles in Spain has led to the recovery of nearly 20 cars in nine days.

Led by the Spanish National Police and supported by INTERPOL's Task Force on Stolen Motor Vehicles (SMV), Operation Paso del Estrecho (which means 'crossing the straits') was carried out from 28 July to 5 August.

Identified as a key route used by organized criminal networks smuggling cars from Europe into Northern Africa, some 3,000 vehicles were screened against INTERPOL's Stolen Motor Vehicle database at the ports of Algeciras and Tarifa in southern Spain.

Experts from the INTERPOL Task Force on Stolen Motor Vehicles took part in the Spanish-led Operation Paso del Estrecho which targeted the trafficking of stolen vehicles

A range of brands were among the cars recovered, including Audi, BMW, Citroen, Mercedes, Renault and Volkswagen, which had been reported stolen from Belgium, France, Italy, Spain and the Netherlands.

With the Vehicle Identification Numbers (VIN) removed from the cars, on the ground assistance from 20 experts belonging to the INTERPOL Task Force from Austria, Finland, France, Germany, Italy and Sweden enabled direct checks to be made with the manufacturers to identify their origin. In addition to the stolen vehicles, three cars were also impounded after the accompanying documentation was found to be false.

Operation Paso del Estrecho is an annual initiative conducted by Spanish police and supported by INTERPOL to prevent stolen vehicles from leaving the country and to help identify the criminal networks behind the illicit trafficking. Follow-up investigations initiated in connection with the arrests are now underway, with continued support from INTERPOL's SMV Task Force.

The INTERPOL SMV database contains some 7.2 million records from 127 countries. In 2015 the SMV database was searched nearly 150 million times, resulting in more than 120,000 positive hits.

Identified as a key route used by organized criminal networks smuggling cars from Europe into Northern Africa, some 3,000 vehicles were screened against INTERPOL's Stolen Motor Vehicle database at the ports of Algeciras and Tarifa in southern Spain

With the Vehicle Identification Numbers (VIN) removed from the cars, on the ground assistance from 20 experts belonging to the INTERPOL Task Force from Austria, Finland, France, Germany, Italy and Sweden enabled direct checks to be made with the manufacturers to identify their origin.

Prestige cars stolen to order in carjackings, home invasion flooding into Malaysia

By Mark Buttler, HeraldSun, 14 August 2016

Prestige cars stolen to order in car-jackings, home invasions and other thefts are flooding out of Victoria and into Malaysia.

Organised crime networks with international links are cashing in on a supply chain stretching from Melbourne's suburbs to Asia and the Middle-East.

Other vehicles, stolen by youth gangs like Apex, are suspected of having been used in major insurance rip-offs or for fake smash rorts.

Audis, BMWs and Mercedes-Benzes, some valued at over $100,000, are being exchanged for between $1000 and $3000 cash in the outlaw trade.

Rogue operators are then disassembling them, mostly for engines and gearboxes, and cramming them into shipping containers for which they can expect to be paid tens of thousands of dollars per load.

The rest of the shell is crushed and sold to metal merchants for further profit.

One industry observer said the risks of exporting stolen vehicles or parts, usually packed alongside legitimate vehicle elements, were minimal.

He said Malaysia had emerged as a particularly attractive option because of an inexhaustible appetite for vehicles.

"We (Australians) are not that concerned about what's out-going (in containers). We're more worried about drugs and weapons coming in," the source said.

The Herald Sun has found:

- A LOOSELY regulated cash economy is helping keep payments to teenage thieves off the books.
- LINKS have been found between some of those involved and the Comanchero motorcycle gang.
- CARS bought from youth gangs are being used in orchestrated smashes to rip off insurance companies.
- CARS are being insured with multiple firms to maximise the profits from faked smashes.
- PROFITS are being invested in other criminal activity like drug trafficking.

Victorian Automobile Chamber of Commerce executive director Geoff Gwilym said a number of "major king-pins" had large networks of youths ready to do their bidding.

"They'll say, `I need an S-Class Mercedes by Sunday and off they (the thieves) go," Mr Gwilym said.

The Herald Sun has been told there are dozens of buyers prepared to unquestioningly pay cash for cars.

National Motor Vehicle Theft Reduction Council executive director Ray Carroll said demand for vehicles in Malaysia was such that buyers had come to Melbourne trying to purchase cars legitimately. He said community alarm at the escalating rate of car theft in Victoria was being compounded by its, at times, violent nature.

Continued on the next page

Prestige cars stolen to order in carjackings, home invasion flooding into Malaysia (continued)

"It changes the game when there's a threat to your safety," Mr Carroll said.

A Victoria Police spokeswoman said: "Vehicle crime squad continues to investigate serious organised crime relating to disposal points of stolen high end vehicles."

Mr Gwilym said police often toiled hard on complex car theft investigations only to find the offenders got off lightly. He said the case of a north suburban father-and-son team who did no jail time after chopping up almost $1 million in stolen cars was a case in point.

"The penalties dished out to these guys is nine hours community service for every vehicle stolen. We're highly complimentary of the police and highly critical of the sentence," Mr Gwilym said.

How it works
1: Thief steals car from street, by aggravated burglary or by car-jacking.
2: It is sold to crime figure with wrecking industry contacts for about $2000.
3: Vehicle is disassembled and shipped to staging post in Malaysia.
4: Crime networks then move it on to Europe, the Middle-East or other Asian country.

Source: *http://www.heraldsun.com.au/news/law-order/prestige-cars-stolen-to-order-in-carjackings-home-invasion-flooding-into-malaysia/news-story/d3f9fbb234ae8958a9d4d4a1db197678*

Boat heist thwarted as thief forgets to untie vessel from dock

By Will Greenlee, 7 July 2016

When swiping a boat, make sure it's not tied to the dock as you drive it away.

It's an oversight that Jimmie Shuman, 42, appears to have made June 24 that sank his alleged boat heist outside Sailor's Return, a waterfront restaurant in Stuart, according to an arrest affidavit.

Shuman is accused of trying to abscond with the 23-foot vessel shortly before 10 p.m.

"The victim stated he saw the defendant on his boat trying to drive it away, but the boat was still tied to the dock at Sailor's Return," an affidavit states.

The victim, a retired law enforcement officer, detained Shuman until Stuart police arrived, torpedoing Shuman's waterborne caper.

Shuman wound up not in Davy Jones' locker, but in the back of a patrol car.

The victim told police he wished to prosecute Shuman, but it's not clear whether he wished Shuman, "Bon voyage," before police took him to jail.

Shuman, of Southeast Hawthorne Street in Stuart, was arrested on charges including grand theft of a boat and battery on a law enforcement officer.

Source: *http://offthebeat.blogs.tcpalm.com/2016/07/07/boat-heist-thwarted-as-thief-forgets-to-untie-vessel-from-dock/*

USA: Laptop used to reprogram, steal more than 100 cars

By Michael Graczyk and Tom Krisher, Associated Press 7 August, 2016

HOUSTON — Two men jailed in Houston and accused of using pirated computer software to steal more than 100 vehicles may have exploited an electronic vulnerability to advance auto theft into high-tech crime.

Michael Arce, 24, and Jesse Zelaya, 22, focused on new Jeep and Dodge vehicles, which attract big money on the black market in Mexico, authorities said. The men allegedly used a laptop computer to reprogram the targeted vehicles' electronic security so their own key worked.

Jesse Irvin Zelaya (left) and Michael Armando Arce. (Houston Police Department via AP)

The stolen vehicles had a common software that's used by auto technicians and dealers, Houston police officer Jim Woods said.

"As you get more and more computers installed in vehicles — if somebody has that knowledge and that ability, they can turn around and figure out a way to manipulate the system," he said.

Fiat Chrysler, which makes Jeeps and Dodges, and police are investigating how the thieves got access to a computerized database of codes used by dealers, locksmiths and independent auto repair shops to replace lost key fobs, said Berj Alexanian, a spokesman at the company's U.S. headquarters in Auburn Hills, Michigan. He said the code database is national and includes vehicles in areas outside of Houston, although he wasn't aware of similar thefts elsewhere.

"We're looking at every and all solutions to make sure our customers can safely and without thinking park their vehicles," Alexanian said Friday.

With more automotive tasks becoming computerized and more cars being linked to the internet, such thefts are likely to increase across the globe, said Yoni Heilbronn, a computer security expert.

The auto industry has worked hard in the past year to develop protections, but hackers with multiple motivations will always be looking for ways to get in, said Heilbronn, vice president of marketing for Argus Cyber Security, an Israeli company that works with automakers.

While increased computerization brings safety benefits, Heilbronn foresees more thefts, malicious software being installed that shuts down cars until a ransom is paid, and even attacks that disable many cars at a time. The industry, he said, has to install multiple layers of defense.

Automakers have been working together to develop best practices and to share information on cybersecurity threats. Companies, including Fiat Chrysler, have their own hacking teams and have offered bounties to outside hackers if they find vulnerabilities.

The Houston investigation began in late May with the theft of a Jeep Wrangler near downtown. Leads in that case had been exhausted when investigators received information from federal Homeland Security and Immigration and Customs Enforcement officers about vehicles being stolen using a laptop. Arce and Zelaya then were identified as suspects.

The two men, who each have criminal records, were arrested last weekend driving a stolen Jeep Grand Cherokee after police had been concentrating on an area of Houston that had been hit previously by auto thieves. They also recovered electronic devices, keys and other tools believed used in the thefts, along with drugs, firearms and body armor.

In the Jeep Wrangler case caught on a surveillance video, the suspect got under the hood, cut wires to the horn to disable an alarm and then got inside the SUV. Once inside, he used the database and the vehicle identification number to program a new key fob for the Jeep.

Arce remained in jail without bond on charges of unauthorized use of a vehicle, felony possession of a weapon, and possession with intent to deliver a controlled substance. He was set for a court appearance Aug. 26. Zelaya is being held on $500,000 bond on a charge of unauthorized use of a vehicle and was due in court Wednesday.

Source: *http://www.policeone.com/investigations/articles/207552006-Police-Laptop-used-to-reprogram-steal-more-than-100-cars/?nlid=207227044&utm_source=iContact&utm_medium=email&utm_content=TopNewsRight5Title&utm_campaign=P1Member&cub_id=usr_kk6WJsut4x7X84qe?utm_source=email-to-friend&utm_medium=email*

Fiat Chrysler Cracks Down on Data Violators After Ram/Jeep Theft Ring Bust

By Steph Willems on August 27, 2016

A Houston-area vehicle-theft ring that used laptops to enter, then steal, over 100 Jeep and Ram vehicles exposed a serious internal security breach at Fiat Chrysler Automobiles.

Now that two arrests have been made in the case, FCA is talking tough and threatening criminal proceedings against anyone who provides outsiders with key vehicle data, Automotive News reports.

Earlier this year, Houston police noticed a trend in vehicle thefts. Certain Ram and Jeep models disappeared from driveways and garages more than any other model, and a private security camera eventually captured one thief using a laptop to enter a Jeep Wrangler, disable its security system, then drive off.

Suspicion fell on hackers, but FCA's security head told us last month that the thefts aren't the result of a purpose-built gadget or device.

"Not just anyone can do that — you need to have access to our systems in order to get the information necessary from each vehicle to marry a key fob," Titus Melnyk, FCA's senior manager of security architecture, told TTAC, adding that the thefts were the result of someone "abusing their privileges."

On Thursday, the automaker updated the terms of use for its internal DealerCONNECT software. FCA now threatens "civil and criminal proceedings" against those who provide outsiders with "key codes, radio codes and other anti-theft or security measures."

Houston police say the thieves used a laptop, OBD-II plug and software to make off with the vehicles, most of which had crossed the Mexican border by the time their owners noticed them missing.

A FCA spokesperson told the Houston Chronicle that thieves entered the vehicle identification number of a target vehicle into a FCA database to access the code for that vehicle's key fob. After programming the vehicle's security system to accept a generic key fob, the Jeep or Ram was theirs for the taking.

The vehicle-theft ring is still active in the Houston area, according to police, and more arrests are likely. Neither the police nor FCA have stated exactly how thieves accessed the automaker's VIN database.

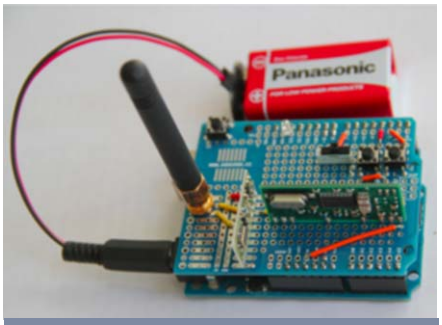
Source: *http://www.thetruthaboutcars.com/2016/08/fiat-chrysler-cracks-data-violators-ramjeep-theft-ring-busted/*

A New Wireless Hack Can Unlock 100 Million Volkswagens

By Andy Greenberg, Wired, 10 August 2016

In 2013, when University of Birmingham computer scientist Flavio Garcia and a team of researchers were preparing to reveal a vulnerability that allowed them to start the ignition of millions of Volkswagen cars and drive them off without a key, they were hit with a lawsuit that delayed the publication of their research for two years. But that experience doesn't seem to have deterred Garcia and his colleagues from probing more of VW's flaws: Now, a year after that hack was finally publicized, Garcia and a new team of researchers are back with another paper that shows how Volkswagen left not only its ignition vulnerable but the keyless entry system that unlocks the vehicle's doors, too. And this time, they say, the flaw applies to practically every car Volkswagen has sold since 1995.

Later this week at the Usenix security conference in Austin, a team of researchers from the University of Birmingham and the German engineering firm Kasper & Oswald plan to reveal two distinct vulnerabilities they say affect the keyless entry systems of an estimated nearly 100 million cars. One of the attacks would allow resourceful thieves to wirelessly unlock practically every vehicle the Volkswagen group has sold for the last two decades, including makes like Audi and Škoda. The second attack affects millions more vehicles, including Alfa Romeo, Citroen, Fiat, Ford, Mitsubishi, Nissan, Opel, and Peugeot.



The $40 Arduino radio device the researchers used to intercept codes from vehicles' key fobs.

Both attacks use a cheap, easily available piece of radio hardware to intercept signals from a victim's key fob, then employ those signals to clone the key. The attacks, the researchers say, can be performed with a software defined radio connected to a laptop, or in a cheaper and stealthier package, an Arduino board with an attached radio receiver that can be purchased for $40. "The cost of the hardware is small, and the design is trivial," says Garcia. "You can really build something that functions exactly like the original remote."

100 Million Vehicles, 4 Secret Keys

Of the two attacks, the one that affects Volkswagen is arguably more troubling, if only because it offers drivers no warning at all that their security has been compromised, and requires intercepting only a single button press. The researchers found that with some "tedious reverse engineering" of one component inside a Volkswagen's internal network, they were able to extract a single cryptographic key value shared among millions of Volkswagen vehicles. By then using their radio hardware to intercept another value that's unique to the target vehicle and included in the signal sent every time a driver presses the key fob's buttons, they can combine the two supposedly secret numbers to clone the key fob and access to the car. "You only need to eavesdrop once," says Birmingham researcher David Oswald. "From that point on you can make a clone of the original remote control that locks and unlocks a vehicle as many times as you want."

The attack isn't exactly simple to pull off: Radio eavesdropping, the researchers say, requires that the thief's interception equipment be located within about 300 feet of the target vehicle. And while the shared key that's also necessary for the theft can be extracted from one of a Volkswagen's internal components, that shared key value isn't quite universal; there are several different keys for different years and models of Volkswagen vehicles, and they're stored in different internal components.

The researchers aren't revealing which components they extracted the keys from to avoid tipping off potential car hackers. But they warn that if sophisticated reverse engineers are able to find and publicize those shared keys, each one could leave tens of millions of vehicles vulnerable. Just the four most common ones are used in close to all the 100 million Volkswagen vehicles sold in the past twenty years. They say that only the most recent VW Golf 7 model and others that share its locking system have been designed to use unique keys and are thus immune to the attack.

Continued on the next page

A New Wireless Hack Can Unlock 100 Million Volkswagens (continued)

Cracked in 60 Seconds

The second technique that the researchers plan to reveal at Usenix attacks a cryptographic scheme called HiTag2, which is decades old but still used in millions of vehicles. For that attack they didn't need to extract any keys from a car's internal components. Instead, a hacker would have to use a radio setup similar to the one used in the Volkswagen hack to intercept eight of the codes from the driver's key fob, which in modern vehicles includes one rolling code number that changes unpredictably with every button press. (To speed up the process, they suggest that their radio equipment could be programmed to jam the driver's key fob repeatedly, so that he or she would repeatedly press the button, allowing the attacker to quickly record multiple codes.)

With that collection of rolling codes as a starting point, the researchers found that flaws in the HiTag2 scheme would allow them to break the code in as little as one minute. "No good cryptographer today would propose such a scheme," Garcia says.

Volkswagen didn't immediately respond to WIRED's request for comment, but the researchers write in their paper that VW acknowledged the vulnerabilities they found. NXP, the semiconductor company that sells chips using the vulnerable HiTag2 crypto system to carmakers, says that it's been recommending customers upgrade to newer schemes for years. "[HiTag2] is a legacy security algorithm, introduced 18 years ago," writes NXP spokesperson Joon Knapen. "Since 2009 it has been gradually replaced by more advanced algorithms. Our customers are aware, as NXP has been recommending not to use HT2 for new projects and design-ins for years."

While the researchers' two attacks both focus on merely unlocking cars rather than stealing them, Garcia points out that they might be combined with techniques like the one he and different teams revealed at the Usenix conferences in 2012 and last year. That research exposed vulnerabilities in the HiTag2 and Megamos "immobilizer" systems that prevent cars from being driven without a key, and would allow millions of Volkswagens and other vehicles ranging from Audis to Cadillacs to Porsches to be driven by thieves, provided they could get access to the inside of the vehicle.

Black Boxes and Mysterious Thefts

Plenty of evidence suggests that sort of digitally enabled car theft is already occurring. Police have been stumped by videos of cars being stolen with little more than a mystery electronic device. In one case earlier this month thieves in Texas stole more than 30 Jeeps using a laptop, seemingly connected to the vehicle's internal network via a port on its dashboard. "I've personally received inquiries from police officers," says Garcia, who added they had footage of thieves using a "black box" to break into cars and drive them away. "This was partly our motivation to look into it."

For car companies, a fix for the problem they've uncovered won't be easy, Garcia and Oswald contend. "These vehicles have a very slow software development cycle," says Garcia. "They're not able to respond very quickly with new designs."

Until then, they suggest that car owners with affected vehicles—the full list is included in the researchers' paper (see below)—simply avoid leaving any valuables in their car. "A vehicle is not a safebox," says Oswald. Careful drivers, they add, should even consider giving up on their wireless key fobs altogether and instead open and lock their car doors the old-fashioned, mechanical way.

But really, they point out, their research should signal to automakers that all of their systems need more security scrutiny, lest the same sort of vulnerabilities apply to more critical driving systems. "It's a bit worrying to see security techniques from the 1990s used in new vehicles," says Garcia. "If we want to have secure, autonomous, interconnected vehicles, that has to change."

To see the researchers' full paper and the source of this article: *https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/*

IN THE NEWS

Mexico: 225,000 Cars Stolen in Mexico Since 2015: Report

By Mike LaSusa, Insight Crime, 29 July 2016

A new report sheds light on the scale of auto theft in Mexico, which often intersects with other illicit activities commonly carried out by criminal groups.

More than 150,000 cars were stolen in Mexico last year and over 78,000 have been stolen so far this year, according to Reporte Indigo. The news outlet writes that stolen cars are often sent abroad to the United States or Central America, and that vehicles stolen in Mexico have been tracked down as far away as Europe, Asia and Africa.

By some estimates, auto theft in Mexico is a multi-billion dollar industry.

The stolen cars exported abroad sometimes leave from Mexico's ports. Data fromMexico's Tax Administration Service (Servicio de Administración Tributaria - SAT), obtained by Reporte Indigo, shows that between 2007 and 2015 authorities stopped more than 2,000 vehicles from transiting the country's ports due to lack of proper documentation.

Reporte Indigo notes, however, that "given the immense quantity of vehicles that are moved through the country's ports, and the low inspection capacity on the part of national authorities, it is very probable that the more than 2,000 vehicles embargoed by the SAT are just a small sign of the real size of the problem."

Mexico is one of the largest producers and exporters of automobiles in the world. The country exported a total of more than 2.75 million vehicles last year alone. According to Reporte Indigo, some 6.1 million vehicles were exported through Mexican ports between 1996 and 2013.

InSight Crime Analysis

The Reporte Indigo article illustrates several ways in which the stolen car trade intersects with other illicit businesses. For example, Guillermo Prieto, the president of the Mexican Automobile Distributors Association (Asociación Mexicana de Distribuidores de Automotores - AMDA), told the news outlet that stolen cars could be used as payment for drug shipments or as a means of laundering money.

Beyond their mere financial value, criminal organizations have other reasons to seek out stolen automobiles. One of the main attractions of a stolen vehicle is the challenge of tracing it to the person who is actually using it. The difficulty of determining actual ownership makes such vehicles ideal for smuggling contraband, or for use in the commission of other crimes such as robberies and murders.

Source: *http://www.insightcrime.org/*

USA: 15 People From 8 New Jersey Towns Busted In Car-Theft Ring: AG

By Tom Davis (Patch Staff), August 25, 2016

Fifteen New Jersey residents from eight towns were indicted this week in connection with an auto-theft network that preyed on people selling their vehicles on Craigslist, according to authorities.

In an indictment handed up by a state grand jury on Wednesday, Luther Lewis, 38, of Piscataway, Tyisha Brantley, 36, of Scotch Plains, and Justinas Vaitoska, 39, of Palm Beach Gardens, Florida, were indicted on charges of first-degree promotion of organized street crime and second-degree charges of leader of an auto theft network and other offenses in connection with the alleged car theft network.

Others were indicted for their alleged roles in the criminal scheme that was brought down by a multi-jurisdictional investigation dubbed “Operation Title Flip,” according to a news release from Attorney General Christopher S. Porrino.

The case involves the theft of 10 vehicles, valued in total at $248,650, between May and November of 2015. The cars were sold to dealerships for a $107,250 profit, according to the release.

According to prosecutors, Lewis, Vaitoska, and Brantley enlisted the aid of intermediaries to use fake bank checks to “purchase” cars from private sellers then sell them to various car dealerships in New Jersey.

“These alleged con artists trolled the Internet in a quest for cars they could steal through their fraudulent scheme,” said Porrino. “We will not let their predatory conduct go unpunished.”

“Car thefts drive up insurance claims, which lead to higher premiums for everyone,” said Acting Insurance Fraud Prosecutor Christopher Iu. “By breaking up this alleged crime ring we are protecting honest citizens from having to pay the price for the misdeeds of others.”

Lewis, Brantley, and Vaitoska were also indicted on charges of second-degree conspiracy and theft by deception. Also indicted on those charges were:

- Milagros Jimenez, 54, of Haines City, Florida
- Heather Cater, 20, of Woodbridge
- Saint Hardy, 32, of Elizabeth
- Deborah Rodgers, 32, of Carteret

Lewis, Brantley, Jimenez and Rodgers were also charged with second-degree impersonation. Lewis, Brantley and Jimenez were charged with third-degree attempted theft by deception.

Under the direction of Lewis, Brantley, and Vaitoska, intermediaries posed as buyers interested in vehicles advertised for sale on Craigslist, according to authorities. After arranging to see the cars, the intermediaries allegedly “purchased” them by presenting the unsuspecting sellers with fake and/or stolen identification and a counterfeit Bank of America cashier’s check. The sellers, in turn, handed over the vehicles’ keys and title to the intermediaries, according to the release.

The “buyers” typically arranged to purchase the vehicles in the late afternoon so the private seller could not bring the checks to the bank that day. In the days after the "sale," the private sellers attempted to deposit the checks and discovered they were counterfeit, prosecutors said. The bogus sales could not be traced to the intermediaries because they had used fake identification, according to the release.

Meanwhile, before the private sellers could discover the check was counterfeit, other intermediaries would take the vehicle titles to the NJ Motor Vehicle Commission office to transfer the title to their names.

IN THE NEWS

After successfully flipping the title to the new names, the intermediaries would sell the vehicle to a car dealership for cash. After the transactions were complete, Lewis would pick up the intermediaries, take the sale proceeds, and pay the intermediaries for their role in the scheme, prosecutors said. Intermediaries were paid between $300 and $1,000 each, according to the release.

The alleged intermediaries were indicted on charges of fourth-degree falsifying records. They are:

- Nikisha Goodman, 20, of the Avenel section of Woodbridge
- Stephen Hester, 48, of Orange
- Chester Kinder, 62, of Newark
- Tassan Howard, 32, of Newark
- Kamilla Bunn, 20, of Elizabeth
- Tanika Arrington, 30, of Newark
- Javairia Jihad, 29, of East Orange
- Yvonne McBride,38, of Newark
- Marixa Medina, 31, of Newark

Another alleged intermediary, Nakita Savage, 28, of Newark, was previously indicted on charges of third-degree conspiracy, receiving stolen property and fencing by the Middlesex County Prosecutor's Office.

The indictment is merely an accusation, and the defendants are presumed innocent until proven guilty. First crimes carry a sentence of 10 to 20 years in state prison and a fine of up to $500,000.

Source: *http://patch.com/new-jersey/oceancity/15-people-8-new-jersey-towns-busted-car-theft-ring-ag*

65th International Seminar

Malaysia: VTREC— Car manufacturers apathetic about vehicle security seconds

By Blake Chen, 26 August 2016

Vehicle Theft Reduction Council of Malaysia says that just as vehicles have four-star ratings on safety, they should have four-star ratings on security as well.

PETALING JAYA: The general attitude of car manufacturers in Malaysia is that as long as it is not made the law, they are unwilling to use a globally known security standard for products that prevent car thefts.

This apathetic attitude towards vehicle security was revealed by the Vehicle Theft Reduction Council of Malaysia (Vtrec).

It was reported yesterday that Malaysia ranked sixth in the world for car theft. According to Alex Lye, a spokesperson of Vtrec, Malaysia's poor ranking was due to the apathy car manufacturers had towards vehicle security.

Elaborating, Lye explained that for years he tried to propose the use of Thatcham security, a globally known security standard for products that prevent car thefts.

"However, it (the proposal) has been falling on deaf ears," he said.

"UK produced a car immobiliser and an installation system (via Thatcham). It then introduced it to all original equipment manufacturers (OEM) and within two years there was a drastic and fantastic 50 per cent reduction in vehicle theft in the country.

"In Malaysia, all we need to do is incorporate a Thatcham-certified product and Thatcham-certified installation system in all vehicles and our car-theft problem will go away. It is not even expensive to do so," Lye told FMT.

He said, however, that auto manufacturers "do not bother" to implement the Thatcham standards here simply because it was not the law in Malaysia, unlike in England.

"I have spoken to many OEMs and they said that as long as it was not mandatory by law, they would not comply."

Deploring the loss that car owners faced when their cars got stolen, he said, "It is a pity that there is no safety net for car owners or consumers. Once their vehicles are stolen, they are faced with loss of transport, having to spend extra money on transport while still servicing the vehicle loan.

"If the government is serious, then we should adopt a globally-accepted system. When our local cars are exported, they will be recognised in Europe, Australia and South Africa. A four-star rating on safety should be accompanied by a four-star rating in security."

Yesterday, it was reported that an average of 60 vehicles were stolen every day across the country, ranking Malaysia as one of the top 10 countries in the world for vehicle thefts.

General Insurance Association of Malaysia (PIAM) Chief Executive Officer Mark Lim was quoted in a report in The Star Online as saying that for the first half of 2016, the insurance industry incurred claims amounting to RM2.41 billion that equalled to a RM13.2 million payout per day in motor claims for property damage, bodily injury and vehicle theft.

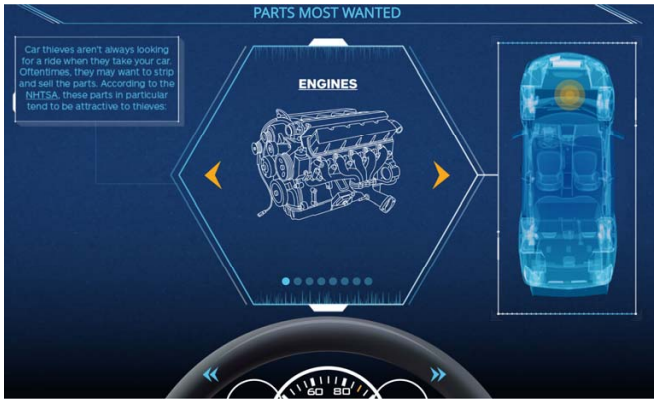
And car crime in Britain has jumped by eight per cent in just a year as 81,000 vehicles were stolen from their owners last year.

Source: *http://www.freemalaysiatoday.com/category/nation/2016/08/26/vtrec-car-manufacturers-apathetic-about-vehicle-security/*

IN THE NEWS

USA: An interactive infographic about Auto Theft

The following interactive infographic about auto theft in the USA has been produced by Allstate Insurance. On each screen there are multiple items to click on for more information. To access the infographic click on the first image below or visit https://blog.allstate.com/auto-theft-in-the-u-s-a-drivers-manual/

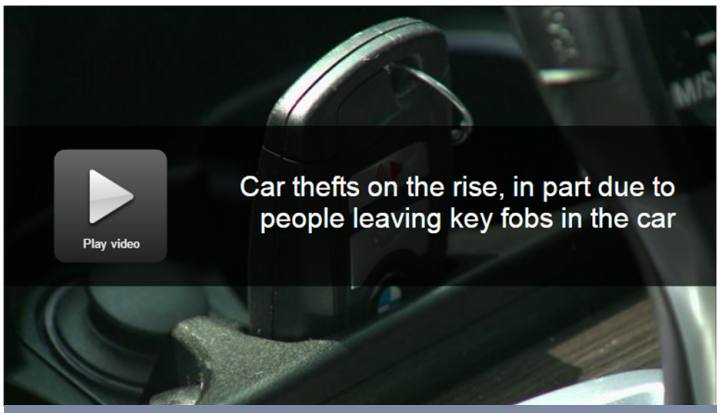


USA: Police issue warning about key fobs after increase in stolencars

By Katie Harris and Katie Corrado, 1 August 2016

HARTFORD -- Police in Hartford have noticed a new pattern of car thefts and are issuing an important warning for car owners across the state.

"Our investigators have noticed a specific similarity in car theft cases from out of town," said Deputy Chief Brian Foley. "Newer model cars with key fobs left in the vehicle."



To view the video: http://fox61.com/2016/08/01/police-issue-warning-about-key-fobs-after-increase-in-stolen-cars/

In 2014, the Hartford Police Department recovered 226 stolen cars in the city, which were stolen from out of town. In 2015, the department recovered 313.

If 2016 continues at it's current pace, Foley predicts that more than 425 stolen cars from out of town will have been recovered in Hartford.

"We are actively recovering vehicles daily from all over the state," Foley said. "One of our own HPD officers had a personal vehicle stolen in South Windsor last week. The vehicle was recovered in Hartford and it was a key fob theft."

Police believe car thieves are aware people leave their key fobs in the cars and are canvassing suburban neighborhoods in the greater Hartford area.

"Suspects walk the streets and driveways neighborhoods and pull on car door handles," Foley said. "In the newer model vehicles, if the fob is left in the vehicle, it will be unlocked. Once in the car, they will simply press the ignition button. If a key fob is within the vehicle, (or sometimes within several feet proximity, such as in a neighboring parked vehicle), the vehicle will start and the suspects will drive off with the car. The key fob does not always need to remain in the car for the vehicle to remain on."

Police warn drivers to leave key fobs in pockets or pocketbooks, not in cars.

"If you notice somebody walking the streets or driveways checking door handles on cars, please report this to your local police department immediately," Foley said.

In just the last four weeks in Hartford, 99 stolen vehicles recovered, 75 of those were thefts from out of town.

Source: *http://fox61.com/2016/08/01/police-issue-warning-about-key-fobs-after-increase-in-stolen-cars/*

A similar story from Hillsborough County, FLA titled:

Car thieves targeting unlocked cars looking for key fobs left behind

Can be seen at: *http://www.abcactionnews.com/news/region-tampa/car-thieves-targeting-unlocked-cars-looking-for-key-fobs-left-behind*

USA: Philly D.A. charges 32 in massive auto-theft and insurance-fraud ring

By Chris Palmer, Philly News Staff Writer, 11 August 2016

Bogus insurance. Fraudulent registrations. Stolen cars disguised and resold to unsuspecting customers.

Those were some of the tactics prosecutors say were used by dozens of people and three corporations in what they described as an auto-theft and insurance-fraud ring that operated in Philadelphia for years.

"This was a massive criminal enterprise," District Attorney Seth Williams said Wednesday as he announced charges against 32 people

Assistant District Attorney Linda Montag, who oversaw the investigation, described the ring as "a detailed, intricate criminal organization with many moving parts," allowing coconspirators to generate tens of thousands of dollars in profits.

Jihad Miller, 26, of Yeadon, and Preston Thomas, 37, of Philadelphia, were accused of heading the enterprise and faced dozens of counts each, including conspiracy, theft, and belonging to a corrupt organization. Their attorneys declined to comment Wednesday.

The others face a variety of related counts, and Montag said about half were expected to plead guilty. Some accused of lesser crimes may be accepted into a probationary program, she said.

Authorities said Miller and Thomas ran a company called Cheap Auto, buying inexpensive salvaged vehicles from online auctions.

The men would then strip the vehicle identification numbers from the salvaged cars, prosecutors said, and slap them onto other vehicles that they recruited people to steal.

The men and their co-conspirators also created or fraudulently obtained documentation, such as titles and registrations, prosecutors said. Part of the scheme involved mechanics who illegally passed cars through "enhanced inspections," allowing the vehicles to hit the road despite carrying a mismatched VIN, said Philadelphia Police Detective Jack Logan of the Major Crimes Auto Squad.

Designated sellers - including Miller and Thomas - would then market the seemingly legitimate cars to unknowing buyers, authorities said. While the salvaged VINs were typically purchased for less than $2,000, the stolen cars often sold for up to $20,000, prosecutors said.

In total, according to Williams, the organization resold 45 cars, most of them stolen from rental companies including Hertz, Enterprise, Avis, and Dollar/Thrifty. Authorities said the scheme cost the rental companies more than $500,000, and resulted in more than $60,000 in bogus insurance claims.

Some new owners of the stolen cars also had to surrender their vehicles to police, authorities said. Montag said she hoped restitution would eventually cover their costs.

All but one of the 32 people charged has been arrested, Williams said. The final conspirator, Karriem Upshur, fraudulently registered 17 vehicles with fake insurance policies, prosecutors say. Anyone with information on his whereabouts is asked to contact Logan at 215-685-9137 or Detective Patrick Gleason at 215-686-8737.

Source: *http://www.philly.com/philly/news/20160811_Philly_D_A__charges_32_in_massive_auto-theft_and_insurance_fraud_ring.html*

IN THE NEWS

Australia: Former Young Australian of the Year Brad Smith and his business partner charged over alleged motorcycle rebirthing syndicate

By Ben McCleelan and Patrick Billings, The Daily Telegraph, 29 July, 2016

A former Young Australian of the Year and his business partner have been charged over an alleged motorcycle rebirthing syndicate. Bradley Smith, 29, the 2010 Young Australian of the Year for Tasmania and Toby Wilkin, 33, were charged by the NSW Property Crime on Thursday. The pair head-up Tasmanian based motorcycle business Braaap which was raided by police on Wednesday. NSW detectives will allege the pair rebirthed 85 motorcycles, 35 of which were sold in NSW.

Wilkin, the Braaap general manager, was charged with four counts of fraud and deal in proceeds of crime knowingly conceal. He appeared at Launceston Magistrates Court where he was granted conditional bail to appear at Downing Centre Local Court on Thursday August 18.

Brad Smith (left) and Toby Wilkin

Smith, Braaap's owner and founder, was arrested in Melbourne after returning from a speaking engagement in Perth. He was charged with four counts of fraud and deal in proceeds of crime knowingly conceal.

He appeared at Melbourne Magistrates Court where he was granted conditional bail to appear at Downing Centre Local Court on August 18.

Mr Smith told the Daily Telegraph he would fight the charges in court. "We are denying the charges. We just have to trust in the system and let it clear our name and move forward. The true colours will shine," he said.

"We had a confirmative production audit three months ago which was passed. We didn't expect the drama of Wednesday. We are 100 per cent co-operative.

"When accusations are made the police have to do their job. We use this as motivation to get better. We always take the high road, our values don't change even when we are tested like today and yesterday. It only makes us stronger.

"We are a niche company. We are competing in an extremely competitive marketplace. We are underdogs."

Braaap motorcycle dealers at Launceston, Tasmania, and Frankston, Victoria, were raided on Wednesday by the NSW Police's property crime squad. Following the arrests, a further search warrant was executed at a business at Tullamarine, Victoria, where strike force detectives seized documentation. Police seized a punch stamp set, compliance labels, computers, and documentation.

The arrests follow an extensive investigation by the crime squad assisted by Tasmanian and Victorian Police, Australian Border Force, and the Department of Infrastructure and Regional Development.

NSW detectives established Strike Force Ologhlen to investigate alleged motorcycle rebirthing and their resale in NSW eight months ago. Property crime squad Commander Detective Superintendent Murray Chapman, alleged it was "a sophisticated and carefully-orchestrated" motorcycle rebirthing syndicate. "Vehicle rebirthing is a serious crime and potentially puts unsafe vehicles back on the road," he said. "This was an extensive and complex investigation, and all police involved have done an outstanding job.

"Their efforts have dismantled what we believe was a sophisticated and carefully-orchestrated motorcycle rebirthing syndicate, and we're confident it has now been stopped in its tracks."

Source: *http://www.dailytelegraph.com.au/news/nsw/former-young-australian-of-the-year-brad-smith-and-his-business-partner-charged-over-alleged-motorcycle-rebirthing-syndicate/news-story/33dd8c43d5e88e6b0b6b0989e081fc45*

Australian state proposes wide ranging anti-metals theft law

Recycling Today Global Edition, 29 August, 2016

A bill proposed in the Legislative Assembly of the Australian state of New South Wales is targeting the problem of metal theft by strictly regulating and scrutinizing the activities of scrap processors. The state of New South Wales includes the cities of Sydney and Newcastle. The "Scrap Metal Industry Bill 2016," sponsored by Assembly members Troy Grant and Duncan Gay, states as its object to "regulate the scrap metal industry" in seven specific ways with the potential for future regulation also.

The regulatory measures called for in the bill include:

- to require persons who carry on a business of dealing in scrap metal (scrap metal dealers) to register the business with the Commissioner of Police;
- to prohibit scrap metal dealers from paying cash for scrap metal;
- to require scrap metal dealers to keep and maintain records of transactions for buying scrap metal, including details of the person selling the scrap metal;
- to require scrap metal dealers to report suspicious transactions to the police;
- to prohibit scrap metal dealers from accepting a motor vehicle (or any motor vehicle body, engine or chassis) as scrap metal if it does not display its identification details;
- to provide for short-term and long-term closure orders in respect of premises at which a scrap metal business is being carried on if the business is not registered under the proposed Act or serious criminal offences have been committed on the premises;
- to authorise police officers without a warrant to enter premises at which a scrap metal
- business is being carried on to investigate contraventions of the proposed Act and to search, take photographs and recordings and seize and copy records; and
- to provide for other regulatory measures in respect of the scrap metal industry."

A scrap processor who operates in the Sydney area says the bill has come about as a response to increases in vehicle theft. "Our industry had no warning [on the proposed law], but there has been a recent increase in new entrants in the industry mainly focusing on cars—namely buying, breaking (pulling out engines and nonferrous parts) and exporting the shells overseas. As these yards have grown, it has come to the attention of the various authorities, particularly with statistics showing an increase in the number of stolen cars. Also there is no requirement to be licensed to operate a scrap yard so the industry was in need of some form of regulation."

He says eliminating cash will not be a problem with commercial customers, but will affect "the street trade." Says the processor, "Electronic funds transfer payment has been an easy and acceptable overnight payment system for medium and large customers, however it has remained unpopular with the street trade."

In a speech prepared to introduce the bill, the legislator Grant downplayed the burdens to scrap collectors. "I make it clear that the proposed legislation will not impact on anyone legitimately looking to offload scrap metal," he stated. "For instance, people who enjoy scavenging on council clean-up days with a view to making a few dollars or who find it necessary to move a rusted car chassis—I have one in my backyard—can still do so in the normal way but will no longer be paid in cash and will need to prove their identity. That is not too onerous."

He later represented the proposed switch away from cash payments as a benefit to processors, remarking, "More and more businesses are relying on [electronic and cheque] payments, so this is not considered onerous. It will also remove the need for scrap metal businesses to keep large volumes of cash on hand, which could also be a security risk for them."

Grant also cited laws in the United Kingdom as having served as a model, commenting, "We also know that a similar scheme in place in the United Kingdom has already proven to be successful, with the number of metal theft incidents falling significantly in the scheme's first year of operation."

Source: *http://www.recyclingtodayglobal.com/article/australia-sydney-scrap-metal-theft-law/*

IN THE NEWS

USA: More Than 300 Cars Stolen Across 13 Chicago Suburbs

NBC Chicago, 26 August, 2016

High-end, luxury cars parked in residential driveways are generally the vehicles targeted, police said

Police are warning residents in Chicago's suburbs after a rash of car thefts.

At least 300 cars have been reported stolen across 13 Chicago-area suburbs, according to police, including several on the North Shore.

The thieves are generally targeting high-end, luxury cars parked overnight in residential driveways, police said. Many of the cars were unlocked when stolen with the keys left inside, authorities said.

One woman, says her new car was stolen right from outside her new home. She told NBC 5 she had just moved to Elmhurst to get away from the crime in the city.

"When I woke up in the morning to leave at about 9 a.m. the car was missing," she said. "It was just gone."

Hundreds of cars have been reported missing from homeowners spanning 13 Chicago suburbs, according to police, including: Lake Bluff, Lake Forest, Highland Park, Glencoe, Einnetka, Wilmette, Deerfield, Northbrook, Glenview, Elmhurst, Hinsdale, Naperville and Boilingbrook.

Police are stepping up patrols and urge residents to lock their cars and garages and to invest in security cameras.

Source: *http://www.nbcchicago.com/news/local/More-Than-300-Cars-Stolen-in-Chicagos-Suburbs-Police-391400311.html*

From page 13

No you won't see this fashion statement on the streets of Paris, Milan, London, Tokyo, New York or Sydney.

Instead you are more likely to se them on the streets of Rotterdam and on the feet of our 2017 International President, Hans Kooijam.

TRAINING & TOOLS

Training is one of the most important areas that we as auto theft investigators need to continually seek out. With the trends in auto theft changing on a daily basis, we need to stay on top of these new developments that can assist us with prevention, identification, investigation, and prosecution. If you know of any other auto theft courses that are being offered, please contact Denny Roske at: iaatidenny@aol.com

2016/17 Conferences and Training Seminars

2016 Seminars

National Insurance Crime Bureau	Continuous	on line training web site, click on: courses	www.NICBTraining.org
Florida Auto Theft Intelligence Unit	Sep 8th – 9th	Ft. Myers, Florida	Sheri Taynor staynor@cfl.rr.com
NICB Auto Theft School	Sept 13th – 15th	Greenville, Texas	Daniel Looney dlooney@huntcounty.net
Miami Dade Auto Theft Symposium	Oct 3rd – 7th	Miami, Florida	Rosa Holtz rholtz@mdpd.com
European Branch Annual Seminar	Oct 5th – 7th	Torremolinos, Spain	Arne Knippel akn@forsikringogpension.dk
Western Regional Chapter & Western State Auto Theft Inv.	Oct 16th – 20th	San Diego, California	www.wsati.org/2016conference.html
South Central Regional Chapt. & Texas Auto Theft Invest.	Oct. 25th – 28th	San Antonio, Texas	Bill Skinner bskinner4309@gmail.com
South African Branch Seminar	Oct. 26th – 28th	Weesgerus Police Resort Modimole, Limpopo	Daan Nel dnel@tracker.co.za

2017 Seminars

Australasian Branch Annual Training Seminar	March 20th - 22nd	Brisbane, Australia	Mark Pollard mpollard@iaatiaus.org
North Central Regional Chapter	May 1st –4th	Indianapolis, Indiana	Cheryl Zofkie czofkie@nicb.org
North East Regional Chapter	May 15th – 18th	Portland, Maine	Dave Potter dpotter@PlymouthRock.com
National Odometer & Title Fraud Enforcement Assoc	June 4th – 8th	Charlotte, North Carolina	Jason Shrader 704-331-4506
Latin American Branch Seminar	June 8th - 9th	Buenos Aires, Argentina	Laura Brizuela analaurabrizuela@iaati.org
Southeast Regional Chapter Seminar	June 11th - 15th	Delray Beach, Florida	Nathan McGanty nmcganty@gmail.com
65th Annual International Seminar	Aug. 28th - 1st Sept	Cape Town, South Africa	Daan Nel dnel@tracker.co.za

The International Association of Auto Theft Investigators

EUROPEAN BRANCH

2016 IAATI EB SEMINAR
TORREMOLINOS - SPAIN

Hotel: SOL PRINCIPE - Paseo Colorado 26 - 29620 TORREMOLINOS (Malaga)

The region lends itself to extended stay for visits to Malaga, Cordoba, Ronda and Granada.

MALAGA:

RONDA

GRANADA

As the hotel lies straight to the beach it also invites to enjoy the sun (normal from 25 to 30° C begin October)

TRAVEL INFORMATION:

Nearby Airport: MALAGA (Malaga - Torremolinos = 8 km)
From Airport to hotel best take a taxi (costs: 12 to 15 €)

or

Rental car: several traditional rental companies rent you a car for good prices. For the moment it seems that Malagacar.com gives good price and conditions (full insurance) with very quick shuttle-service at airport (3min)(own experience). Also other companies give similar conditions.

Registration form

IAATI - EB TRAINING SEMINAR

October 05 - 07, 2016

TORREMOLINOS - PLAYAMAR - SPAIN

PLEASE FILL IN WITH COMPUTER - FOR EACH SEMINAR VISITOR 1 FORM

WE DO NOT ACCEPT REGISTRATIONS LATER THAN ON 21th SEPTEMBER

Step 1: Your personal information

Name : ……

Address : ……

City : ……

Country : ……

E-mail address : ……

Phone number : ……

IAATI membership number: ……

Profession : ……

Law enforcement : yes / no

T-shirt size : S M L XL XXL (please circle).

Companion (non attendee of the seminar)

Name : ……

Address : ……

Place : ……

Country : ……

Phone number : ……

EXTRA INFORMATION FOR THE ORGANISERS?

……

……

PRIVACY

Do you want your name and information to be mentioned on the participants list which will be spread during the seminar?

☐ Yes ☐ No (When not filled in = yes)

Step 2: Your hotel and seminar fees

ROOMS ARE TO BE RESERVED VIA IAATI EB SECRETARIAT. WE BOOK ONLY ON BASE OF ROOM+BREAKFAST.

a. Standard room - single use 85€ / night
Check-in date:..... Check-out date..... Total nights:.....

b. Standard room - double use 95€ / night
Check-in date:..... Check-out date..... Total nights:.....

c. Standard room - triple use 135,40 € / night
Check-in date:..... Check-out date..... Total nights:.....

d. Junior suite *** Pool view 1pax 105€ / night
Check-in date:..... Check-out date..... Total nights:.....

e.Junior suite *** Pool view 2pax115€ / night
Check-in date:..... Check-out date..... Total nights:.....

f. Junior suite *** Pool view 3pax155,40€ / night
Check-in date:..... Check-out date..... Total nights:.....

g. Junior suite *** Pool view 4pax 195€ / night
Check-in date:..... Check-out date..... Total nights:.....

NET RATES PER ROOM PER NIGHT. VAT 10% INCLUDED
BASIS: B&B: Bed & Breakfast (buffet style)
WI-FI CODE: Included

REDUCTIONS POLICY
1 Child 0-2 years (baby cot) -100% (GRATIS)
1 Child 3-11 years sharing twin room or Junior suite Pool View -50% over 95€/2=47.50€

To pay: .....x.....=.....€ (**Quantity X price)**

Seminar fee

		MEMBERS / POLICE	NON MEMBERS	COMPANIONS
Early Bird	15/05-30/06/16	225	275	120
Second Bird	01/07-15/08/16	250	300	120
Final registration	15/08-21/09/16	275	325	120

(Price includes: Presidents Reception at Wednesday and Banquet on Thursday (both with drinks), lunch on Thursday, all coffee breaks (more extensive on Friday)

TOTAL PRICE: **ROOM** **.....€**

SEMINARFEE **.....€**

TOTAL **.....€**

If two registered attendees stay in a double room (non-companion), please provide the name of the attendee with whom you are sharing the room with (also enclose second registration-form= on his/her name

Name second attendee in the double room: ……

SPECIAL REQUESTS OR REQUEST FOR ADDITIONAL INFORMATION ABOUT SEMINAR-FEE
To be directed to: franky.dedeurwaerder@telenet.be (Treasurer IAATI EB)

Step 3: Your payment

Your registration is only official with prove of payment attached or with valid creditcard number

Payment by credit card or by international bank transfer or PayPal.
Please select your payment method and provide the necessary information.

If you pay by credit card:

Please check one: ☐ VISA ☐ MasterCard ☐ Eurocard

Account Number: (_ _ _ _) (_ _ _ _) (_ _ _ _) (_ _ _ _) Expiration Date:……../……

Name of the cardholder: ……

If you pay by international bank transfer:

Name of the account: IAATI European Branch izvw, Bergstraat 50, B9820 MERELBEKE, Belgium
IBAN: BE43 310-1909360-01
BIC: BBRUBEBB

PayPal:

Account-number: IBAN: BE43 310-1909360-01
Swift-code: BBRUBEBB
Email: franky.dedeurwaerder@telenet.be

CANCELLATION POLICY:

Until 31 August, 2016 without costs.

Note: In case of a "no-show" or any other cancellations after Aug 31, 2016, IAATI has to charge you for the total amount of your registration !

Step 4: Send us your reservation form!

We do not accept registrations without a completed registration form !!!!

Return the registration form to:

Franky Dedeurwaerder
E-mail : franky.dedeurwaerder@telenet.be

And CC to : davy.borysiewicz@baloise.be
: ukraned3@live.nl