



# Insurance Fraud Trends & NICB Intelligence Reports

---

Jamie Walsh, Director of Intelligence and Analytics

Rich DiZinno, General Counsel

# Disclaimer

---

The NICB strives to ensure the information contained in our training materials is as timely and accurate as possible; however, NICB makes no promise or guarantee regarding the accuracy, completeness, or adequacy of the contents of this information and expressly disclaims any liability for errors and omissions therein. Some of NICB's training materials may include hypertext links or references to information created and maintained by other public and/or private organizations. NICB provides these links and references solely for information and convenience. When selecting an external link in NICB learning products, you are subject to the outside website's privacy, copyright, security, and information quality policies. The information in NICB's training products is for general informational purposes only and is not intended to provide legal advice to any individual or entity. We urge you to consult with your legal advisor before acting based on information on any NICB product. Please note that NICB Learning and Development training materials are copyrighted; permission to copy these materials in whole or in part requires prior authorization from NICB.

# Agenda

---

- NICB Intelligence Product Types
- Accessing NICB Products
- Recent Fraud Trends
- NICB Intelligence and Analytics Resources

# NICB Intelligence Products

---

- Unique Local/National Intelligence
- Risk Mitigation and Management
- Actionable Data Insights
- Strategic Decision Support
- Foster Collaboration

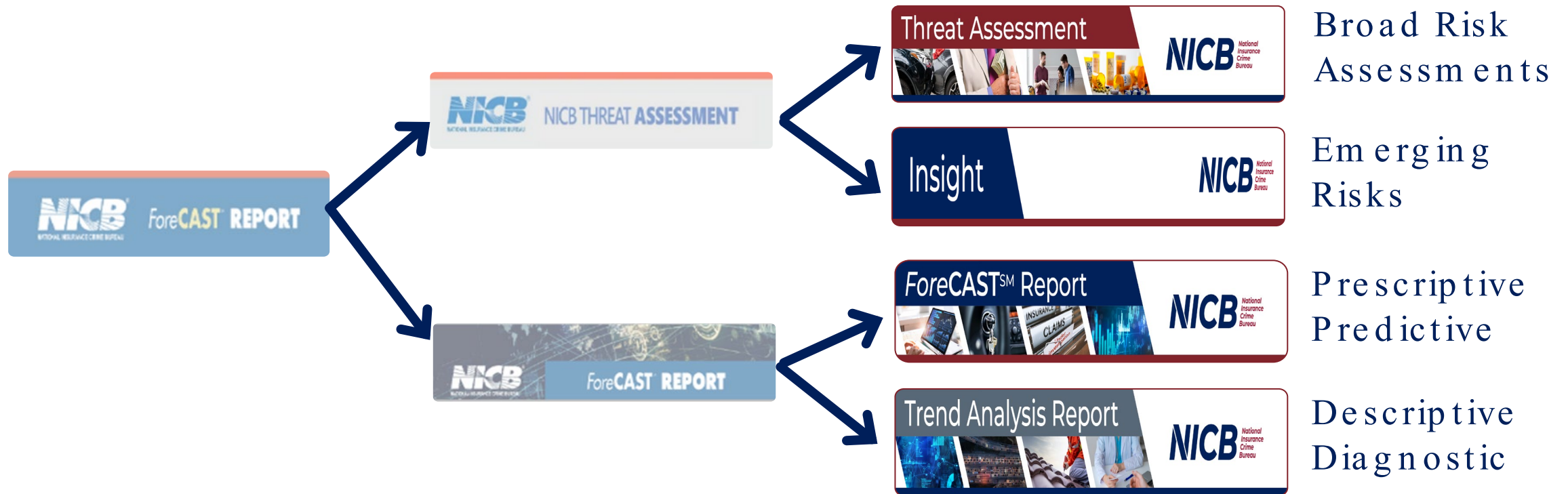


# NICB Intelligence Report Evolution

2006 - 2020

2021 - 2022

2023+



# Threat Assessment



# 2024 Publication Timeline



## 1<sup>st</sup> Quarter

### January

### February

- Q1 National QC ForeCAST

### March

- Q1 National Auto Theft ForeCAST

## 2<sup>nd</sup> Quarter

### April

### May

- Q2 National QC ForeCAST

### June

- Q2 National Auto Theft ForeCAST

## 3<sup>rd</sup> Quarter

### July

### August

- Q3 National Auto Theft ForeCAST
- Q3 National QC ForeCAST

### September

## 4<sup>th</sup> Quarter

### October

### November

### December

- Q4 National Auto Theft ForeCAST
- Q4 National QC ForeCAST

# Trend Analysis Report



# 2024 Publication Timeline



\*Reports in **BLACK** are published.

\*Reports in **GOLD** are in approval.





## 1<sup>st</sup> Quarter

### January

### February

- CA 3/4 Q LPR (LES)
- Generative AI Fraud
- Non-Emergency Transportation Fraud

### March

- Autel KM 100 Key Programmer
- Chicago, IL Rental Truck & Van Thefts
- Intermittent Urinary Catheters
- TX & AZ Q4 2023 LPR (LES)

## 2<sup>nd</sup> Quarter

### April

- Marine GPS thefts in FL
- 2023 Foreign Operation Vehicle Recoveries
- Rodent/Animal Vehicle Damage Claims
- At-Home Pain Relief Laser Devices
- FL Left Hand Turn Wave Down Caused Losses

### May

- TX & AZ Q1 2024 LPR (LES)
- MI Stolen Titles (LES)
- La Nina Catastrophe Claims

### June

- LLC Vehicle Registration Fraud
- Credit Privacy Number Scheme
- "Wasted" Cell Phone Application (LES)
- Common Powertrain Controller Thefts
- Lishi Key (LES)
- CAN Invader (LES)

## 3<sup>rd</sup> Quarter

### July

- LiDAR Spoofing in Autonomous Vehicles
- OBD Data Changer (LES)
- License Plate Flippers (LES)
- Storage Fraud Schemes

### August

- Emerging Camaro Thefts Threat (LES)
- Diclofenac Sodium Topical Medication
- TX & AZ Q2 2024 LPR (LES)
- OBDNator Vehicle Theft Threat (LES)

### September

- Brain Mapping Billing Risks
- Metadata Manipulation
- Unlicensed Rental Car Companies
- Emerging Infiniti Thefts Threat (LES)
- Life Insurance Body Double Scheme
- Third Party Billing Risks
- Q1/Q2 2024 Foreign Operation Vehicle Recoveries

## 4<sup>th</sup> Quarter

### October

- Vehicle Speed Filters Threat (LES)
- Questionable Jewelry Claims Emerging Risks
- Life Insurance Policies, Unclaimed Assets Scheme
- Tens Unit Fraud Risks
- Travel Insurance Fraud Schemes
- Worker Comp Fraud Schemes

### November

### December

\*Reports in **BLACK** are published.

\***LES** are law enforcement sensitive.

# Accessing NICB Intelligence Reports

The screenshot shows the ClaimSearch® interface. At the top, there is a search bar labeled "Search My Claims". Below the header, the "My Products" section is displayed with the instruction "Customize your work space with our new drag and drop product tiles." A grid of product tiles is shown, with the "NICB Services" tile highlighted by a red box. Other tiles include NICB Applications, My Learning Center, VINassist™, OFAC, Claims Inquiry, Research Hub, Equipment Valuation Service, CargoNet, ISO Claims Partners, XactAnalysis, and Anti-Fraud Solutions.

The screenshot shows the ClaimSearch® interface. At the top, there is a search bar labeled "Search My Claims". Below the header, the "NICB Services" section is displayed with a back link to "My Products". A grid of service tiles is shown, with the "NICB Intelligence Reports" tile highlighted by a red box. Other tiles include NICB Member QC Dashboard, NICB QCNet Dashboard, NICB ForeWARN™ Search, NICB Vehicle Theft & Recovery Dashboard, NICB Alert Resources, NICB ForeWARN™ Exposure Dashboard, and NICB Materials Ordering.

*Member company employee access - contact your Company's Claim Search Administrator.  
njsupport@iso.com or call 800.888.4476*

# Accessing NICB Intelligence Reports for LE

## LEEP

## HSIN

The screenshot shows the LEEP (JusticeConnect) interface. At the top, there is a navigation bar with 'Home', 'Profiles', 'Communities', and 'Apps'. Below this, a green banner states: 'JusticeConnect is an UNCLASSIFIED information system. Any Classified information that is found within should be reported immediately to 888-334-4536 or helpdesk@leo.gov'. The main content area is for the 'National Insurance Crime Bureau' community. It includes a sidebar with 'All Community Files' and 'Community Folders' such as 'Cargo Theft Bulletins', 'Events', 'ForeWARN Alerts', 'Intelligence Reports', 'MedAWARE Alerts', 'Recent Regional News', 'Specialized Equipme...', 'Training', and 'Vehicle Identification...'. The main area displays 'Community Folders' with a search bar and a list of folders with 'More' links.

The screenshot shows the HSIN (Homeland Security Information Network) interface. It displays a list of intelligence reports. The reports are organized in a table with columns for year, cause, date, and category. Some reports are redacted with black boxes.

Year	Cause	Date	Category	Other
2023	Cyber_Attack--Widely_Targeted	March 11	Physical Safety and Security	No
(U--FOUO)	Cause_Not_Applicable	March 8	Cyber fraud/Theft	No
(U--FOUO)	Cause_Not_Applicable	March 8	Cyber fraud/Theft	No
(U--FOUO)	Cause_Not_Applicable	March 8	Cyber fraud/Theft	No
(U--FOUO)	Cause_Not_Applicable	March 8	Cyber fraud/Theft	No
2024	Cyber_Attack--Widely_Targeted	March 7	Physical Safety and Security, Terrorist event	No

Toll-free Number - (888) 334-4536  
Email – [helpdesk@leo.gov](mailto:helpdesk@leo.gov)

[HSIN@hq.dhs.gov](mailto:HSIN@hq.dhs.gov)

# Vehicle Theft Trends

## Threat Assessment



**Report Date:** August 16, 2024  
**Report Title:** 2024 Vehicle Theft and Crime Threat Assessment  
**Dissemination:** Member Companies and Law Enforcement

**Geographic Scope:** National  
**Report Type:** Vehicle  
**Analysis Period:** 01/01/2021 – 12/31/2023

### Executive Summary


The 2024 Vehicle Theft and Crime Threat Assessment leverages the National Insurance Crime Bureau's (NICB) extensive network of partnerships with insurers, law enforcement, data providers, and anti-fraud organizations to deliver actionable insights into the trends and threats driving vehicle theft and related crimes across the United States. Vehicle thefts in the United States increased by 9.6 percent from 2021 through 2023. A monthly breakdown of vehicle thefts during the three-year period depicts a steady increase, with the highest number of reported thefts occurring in July 2023, totaling 94,696 vehicle thefts reported to law enforcement. While vehicle thefts have increased, the number of vehicle theft Questionable Claims submitted to the NICB by member companies in 2023 decreased 8.4 percent since 2021.

In 2023, the NICB reported and communicated to stakeholders the nationwide impact of Hyundai and Kia thefts, which saw a 95% increase in 2022 compared to 2021. Many states continue to experience a high volume of Hyundai and Kia thefts, with several of these vehicles crossing into Mexico. Hyundai and Kia models accounted for six of the top ten most stolen vehicles in 2023. In 2024, the NICB and law enforcement observed the growing impact of technology on the ease of vehicle theft. NICB agents reported an emerging trend of increased thefts involving Dodge Chargers, Challengers, and Durangos. Further analysis revealed that thefts of these models in 2023 increased by 18% to 27% nationwide, with a third of the stolen vehicles being model years 2020–2024. The NICB will continue to monitor the impact of this trend in 2024.

The primary methods of vehicle theft affecting the insurance industry and law enforcement remain consistent, but thieves are adapting and expanding their schemes from property crimes to more sophisticated crimes involving advanced technology, organized crime, and escalated acts of violence. Finance fraud remains a favored vehicle theft tactic, with criminals increasingly targeting dealerships, rental agencies, and car-sharing platforms as the market shifts to more online transactions. Thieves use advanced schemes to conceal the identity of stolen vehicles, employing techniques such as VIN switching, title washing, and counterfeit documents to legitimize a vehicle before selling it to an unsuspecting buyer or exporting it out of the country. The value of vehicle parts attracts many criminals, evident in the growing trend of Common Powertrain Controllers thefts and the surgical removal of high-performance parts, tires, and wheels. NICB investigations highlight the range of vehicle theft schemes and tactics, supporting the insurance industry and law enforcement in making a positive impact on our communities.


As motor vehicle thefts continue to rise in the U.S., the NICB remains committed to leading the industry in detecting, investigating, and preventing vehicle crime and fraud in all its forms. The

### KEY JUDGEMENTS




**19.6%**  
Vehicle Theft

Vehicle Theft in the United States increased by almost 10% in the past three years...




**FINANCIAL FRAUD**

Online based financial fraud continues to be a favored vehicle theft approach...




**18.4%**  
Questionable Claims

QCs submitted to NICB by member companies fell more than 8% 2021-2023...



**94,696**  
Vehicle Theft July 2023

The highest number of monthly vehicle thefts occurred in July of 2023...



**Advanced Schemes & Tactics**

Criminals change a stolen vehicle's identity before selling to innocent buyers...

### NICB Top 10 Vehicle Theft States, 2021-2023


#### TOP 10 STATES for Vehicle Theft 2021-2023



Rank	State	2021	2022	2023	2021-2023 Total	Theft % Change 2022 vs 2023
1.	CALIFORNIA	615,586			615,586	2.80%
2.	TEXAS	317,346			317,346	9.36%
3.	FLORIDA	136,985			136,985	0.42%
4.	WASHINGTON	126,452			126,452	-7.98%
5.	COLORADO	115,704			115,704	-19.73%
6.	ILLINOIS	109,544			109,544	7.15%
7.	OHIO	90,507			90,507	4.11%
8.	NEW YORK	84,582			84,582	15.68%
9.	MISSOURI	84,393			84,393	-8.28%
10.	GEORGIA	81,675			81,675	6.53%

All top ten states from last year's threat assessment (2020-2022) remain in the top ten for vehicle thefts between 2021-2023; however, Ohio and Missouri switched from 7th and 8th respectively, and New York and Georgia switched from 9th and 10th respectively. In 2023 alone, Illinois surpassed Colorado, ranking fifth nationally with 41,811 total vehicle thefts, a 7% increase from 2022


### Misuse of Autel KM100



In February 2024, the NICB published a report on the Autel KM100 Insight, a universal key generator and programming tool that can program blank key fobs for targeted vehicles, often allowing thefts to occur in under 60 seconds. These devices, which can be purchased online at a relatively low cost and are legal to own, are being misused to steal high-end vehicles and those equipped with V8 engines nationwide. Additionally, many recovered vehicles have had their VINs switched.

The NICB assisted the Indianapolis Airport Authority Police in interrupting a vehicle theft in progress. The following devices were recovered: an Autel MaxiIM KM100 advanced key and immobilizer touchscreen tablet, an OBD EL-50448 OEC-T5 Tire Pressure Monitor Relearn/Reset Tool for GM vehicles, and an Actron OBD II PocketScan Code Reader. Many of these devices can store historical VIN data, which is valuable for identifying additional vehicle thefts and outlining organized crime activities.

### Misuse of Xtool/AutoProPad Devices



The XTOOL is a key programming device manufactured by XTOOLTECH, an automotive intelligent diagnostic supplier based in Shenzhen, China. XTOOLTECH offers several versions of the XTOOL and several accessories which make it compatible with several European manufacturers. The XTOOPADS models boast support of 60+ manufacturers and 2000+ models and provide an array of data solutions for the user (i.e., immobilizer data, pin code data, ability to

# Vehicle Theft Tactics, Techniques & Procedures

UNCLASSIFIED/LAW ENFORCEMENT SENSITIVE



**NICB**  
NATIONAL INSURANCE CRIME BUREAU

## KIA BOYS CHALLENGE SNAPSHOT

(U) This snapshot provides information and predictions for Louisiana regarding the Kia Boys Challenge and is meant to aid law enforcement in investigations.

(U//FOUO) During the summer of 2022, a group referring to themselves as the “Kia Boys” reportedly based in Milwaukee, Wisconsin, posted a TikTok video explaining how to exploit a flaw in certain Kia and Hyundai models making them easy to steal. Although the original video has been removed from TikTok, Kia and Hyundai thefts in the United States continue to rise. Compared to the same time frame in 2021, across Louisiana in 2022, Kia thefts are up by 117% and Hyundai thefts are up by 83%.

(U//FOUO) The video highlighted a flaw in certain 2011–2021 Kia and 2015–2021 Hyundai models that are not equipped with anti-theft alarm systems and engine immobilizers. Teenagers have been referring to the video as a challenge and posting videos online after stealing vehicles utilizing this method. Due to the media attention this trend has recently been given, it is likely Kia and Hyundai thefts will continue to rise in Louisiana during 2023.

### (U//FOUO) Theft Tradecrafts:

- (U//FOUO) Gain entry into the vehicle, which is typically accomplished by breaking a window.
- (U//FOUO) Remove the plastic shroud from steering column. This is often completed without tools, simply by applying brute force to the plastic shroud and breaking it off. On some vehicles, the component may not fully break off and will hang below the steering column.
- (U//FOUO) Remove the ignition cylinder from the vehicle. Doing so allows the internal mechanism to be accessed, allowing the vehicle to be manually started. This will require the use of a screwdriver, which is the only tool required for these thefts.
- (U//FOUO) Utilize an object that fits over the internal starting mechanism (typically a USB drive). Turn the mechanism to start the vehicle similar to starting a vehicle with a key.

**ANALYST NOTE:** The lack of an engine immobilizer is what makes these vehicles prime targets because there is not a security chip in the vehicle key that the engine is checking for prior to starting.

### (U//FOUO) Photo of the Internal Starting Mechanism on a Defeated Kia



IMAGE CREDIT: LOUISIANA STATE POLICE INSURANCE FRAUD & AUTO THEFT UNIT

(U) For more information or to report similar events, contact the National Insurance Crime Bureau at [IntelligenceandAnalytics@nicb.org](mailto:IntelligenceandAnalytics@nicb.org) and LA-SAFE at [LA-Fusion.Center@la.gov](mailto:LA-Fusion.Center@la.gov).

UNCLASSIFIED/LAW ENFORCEMENT SENSITIVE

### (U//LES) Suspicious Activities Possibly Related to the Kia Boys Challenge:

- (U//LES) Kia and Hyundai vehicles abandoned in random areas
- (U//LES) Kia and Hyundai vehicles with the drive shaft removed that can be seen from window
- (U//LES) Suspicious persons being reported walking around parking lots or streets carrying a number of USB cables
- (U//LES) Reckless joyriding in Kia and Hyundai vehicles

### (U//LES) Possible Investigative Resources for Kia and Hyundai Thefts.

- (U) Subjects participating in this challenge have posted videos of themselves joy riding with the hashtag “KiaBoys.”
- (U//LES) Some models may have infotainment systems that can be forensically downloaded that could provide information on connected devices and locations.

LA-SAFE SINS: LA-11050, LA-14040, LA-27020

This information should be considered LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies, intelligence agencies, and Department of Defense organizations only, unless prior approval from FBI, NOPD, and LA-SAFE is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution list. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact NICB and LA-SAFE, if you have any questions or need any further information.

UNCLASSIFIED//FOR OFFICIAL USE ONLY



**NICB**  
NATIONAL INSURANCE CRIME BUREAU

## RAILYARD APPLE AIRTAG AUTO THEFTS

(U) This snapshot provides information and predictions for Louisiana regarding an emerging threat in auto thefts and is meant to raise awareness amongst vehicle manufacturers, dealerships, and transportation companies along with aiding law enforcement agencies in investigations.

(U//FOUO) In August 2023, the Louisiana State Police Insurance Fraud and Auto Theft Unit received information of a new technique being used by criminal actors in an effort to steal new vehicles being sent from manufacturing plants to dealerships from railyard vehicle storage facilities. Criminal actors broke into a railyard in Louisiana and subsequently removed key fobs from different vehicles and left an Apple Airtag within the vehicle for tracking purposes. These actors then proceeded to steal one of three vehicles once it had been delivered to the dealership using the key fob they had previously acquired. The other two vehicles targeted during this theft were unsuccessful after the receiving dealerships noticed the missing key fob and located the Apple Airtag.

(U//FOUO) LA-SAFE and NICB believe that is likely the use of Apple Airtags or similar devices will continue to be used given the relative simplicity and fact that railyard vehicle storage facilities have been targeted using multiple tradecraft techniques on a regular basis in recent years in Louisiana. At this time, all of the known incidents have involved Apple Airtags. Devices made by other brands such as Tile, Samsung Galaxy SmartTag, and Chipolo One could also potentially be used for this tactic.

### (U//FOUO) Possible Preventative Measures to Combat Apple Airtag Railyard Thefts:

- (U//FOUO) Target harden the facility where the vehicles are being stored to include fully enclosed fence lines, security cameras, and alarms;
- (U//FOUO) Use of security guards / detail officers to conduct roving patrols around the facility; and
- (U//FOUO) Removing key fobs from vehicles and storing them in a secure location while vehicles are being stored at the facility from the time that the vehicle is delivered until the vehicle is loaded onto a transportation to be taken to the dealership.

**ANALYST NOTE:** The common vulnerability exploited during vehicle thefts at railyards including the Apple Airtag thefts and vehicle thefts at railyards is that key fobs are left in the vehicle during transportation.

LA-SAFE SINS: LA-18020(A), LA-27020(O), LA-29020(A,C), LA-31020(A)

This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under Louisiana Revised Statutes. It is to be controlled, stored, handled, transmitted, distributed, and disposed, of in accordance with LA-SAFE's policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a need-to-know without prior approval of an authorized LA-SAFE and NICB official. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution list.

### (U) Photo of Apple Airtag Device



IMAGE CREDIT: APPLE INC.

(U) For more information or to report similar events, contact the National Insurance Crime Bureau at [IntelligenceandAnalytics@nicb.org](mailto:IntelligenceandAnalytics@nicb.org) and LA-SAFE at [LA-Fusion.Center@la.gov](mailto:LA-Fusion.Center@la.gov).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

### (U//FOUO) Suspicious Activities Possibly Related to the Apple Airtag Railyard Thefts:

- (U//FOUO) Break-ins at railyard auto storage facilities with no property reported stolen.
- (U//FOUO) Vehicles arriving at dealerships with a missing key fob;
- (U//FOUO) Persons going to dealerships and using their mobile device to locate a vehicle that they would like to test drive;
- (U//FOUO) Suspicious persons being reported around railyard vehicle storage facilities; and
- (U//FOUO) Surveillance or security testing of railyard auto storage facilities.

### (U//FOUO) Possible Investigative Resources for Apple Airtag Railyard Thefts.

- (U) Apple Airtags are set to play a sound if separated from the registered owners device for more than 24 hours; and
- (U) Apple Airtags can be held near an NFC enabled smartphone to obtain the device serial number and possibly a partial phone number for the registered owner.

# Vehicle Theft Tactics, Techniques & Procedures



## Insight

### The Flipper Zero

Date: February 24, 2023  
Scope: National  
Type: Vehicle

This *Insight* provides information for NICB member companies and law enforcement and is meant to aid in the combat and prevention of insurance crimes and fraud.

The **Flipper Zero** is a portable, multi-function device currently available online for \$169 which uses open-source software to read, record, playback, and manipulate over the air signals including Radio-Frequency Identification (RFID), Radio Frequency (RF), Near-Field Communication (NFC), and infrared. Though the device itself is legal to own and approved by the Federal Communications Commission (FCC), there are opportunities to use the device in criminal tradecraft.

#### Criminal Tradecraft:

While opportunity exists to use the Flipper Zero for unlawful purposes, the device does not do anything that wasn't previously available on the market. It does, however, combine many functionalities into one, small, easy-to-use device that does not require a computer or phone to interact with it. Examples for possible unlawful usage include:

- A user could scan a keycard utilizing NFC technology, record the signal, and then play it back to gain unauthorized entry without possessing the physical keycard.
- A user could intercept, record, and attempt to emulate a garage door signal.
- A user could intercept, record, and attempt to emulate credit and bank card information transmitted through NFC.
- A user could intercept, record, and attempt to emulate the signal sent from a vehicle's key fob and play that signal back to unlock and start the vehicle.

**Analyst Note:** These devices are not illegal to possess but could be misused as described above for criminal activity.



#### Related Information:

- [Wired – What is Flipper Zero?](#)
- [Flipper Zero Specifications](#)
- [FCC Declaration of Conformity](#)
- [NFC Grant of Equipment Authorization](#)

For more information or to report similar events, contact the National Insurance Crime Bureau at [IntelligenceandAnalytics@nicb.org](mailto:IntelligenceandAnalytics@nicb.org)

Copyright ©2023 by the National Insurance Crime Bureau. All rights reserved

#### Vehicle Theft:

While the Flipper Zero device may be capable of unlawfully unlocking and starting some vehicles, the threat appears to mostly apply to older model year vehicles with fobs transmitting **fixed** codes.

- A **fixed code** is a numeric code that never changes making it easier to copy.
- **Rolling codes**, an industry standard on modern vehicles and first implemented in the mid-90s, change with each use, limiting the capabilities of the device.

**Analyst Note:** Electric vehicles, while resistant to the use of this device to open the doors or start the vehicle, do appear to be vulnerable to having the charging port opened. This is mostly a harmless prank.

Though rolling codes make it harder to copy a fob's signals, with enough time and knowhow, a would-be thief could theoretically "hunt" for a code in the radio frequency range and stumble upon the right code.

This intelligence product is provided to NICB member companies and law enforcement for informational purposes only and is not intended to be the basis for claims or other operational decisions. NICB's intent is to share pertinent information for the proactive detection, prevention, and deterrence of insurance related crime. This information is provided "AS-IS" and independent investigation and verification should be conducted prior to making any decisions based upon the information contained in this document. NICB retains all rights, title, and interest to this document. Any



## Insight

### Autel KM100

Date: 02/26/2024  
Scope: National  
Type: Vehicle

This *Insight* provides information for NICB member companies and law enforcement and is meant to aid in the combat and prevention of insurance crimes and fraud. The Autel KM100 is a universal key generator (programming tool) that utilizes what is called "universal remotes." These remotes are not manufacturer specific and can be re-used on multiple vehicles. They are readily available for purchase in online markets for a relatively low cost. **Analyst Note:** These devices are not illegal to purchase or possess and have a legitimate purpose but could be misused as described below.

The NICB received intelligence of a new technique to steal vehicles by misusing the Autel KM100 device. The device may possibly be misused to program blank key fobs to start a vehicle targeted by a thief. Additionally, the Autel device may reportedly be misused to start a vehicle with no need to program a key fob. Allegedly, thieves break a door window to crawl into a car, hook up the device to the OBD II port, then run the program to start the car, and drive off. This method would potentially be faster than programming a key onsite and a key might be programmed after the stolen vehicle has been moved to a more concealed location. Lastly, NICB has received information that other Autel device models could potentially be similarly misused.

#### Tradecraft: Tactics, Techniques, and Procedures

- Thieves, who allegedly misused the device to steal vehicles, primarily targeted vehicles with push to start ignitions.
- The device can reportedly be used as a as a smart key replacement for more than 700 vehicles.
- It is easier and faster to target unlocked vehicles.
- There are numerous online guides and how-to forums discussing the use of this device. One example can be reviewed at the following link: <https://www.locksmithledger.com/print/content/21285653>
- Online video of an individual utilizing the Autel KM100 device to start a vehicle: <https://www.youtube.com/watch?v=VwX4Yf5vbY>



Autel MaxiIM  
KM100 Advanced...  
\$510.00  
Autel.com

For more information or to report similar events, contact the National Insurance Crime Bureau at [IntelligenceandAnalytics@nicb.org](mailto:IntelligenceandAnalytics@nicb.org)

Copyright ©2024 by the National Insurance Crime Bureau. All rights reserved.


#### Suggested solutions to avoid theft with this device.

- The addition of third party kill-switches such as the ones that require the entry of a pass code to allow the vehicle to start.
- Use physical immobilizers such as The Club.
- [Follow the NICB list of recommendations for avoiding vehicle theft.](#)
  - Lock your doors.
  - Remove your keys from the ignition.
  - Close your windows completely.
  - Park in well-lit areas.
  - Use a visible or audible device.
  - Install a vehicle immobilizer.
  - Invest in a tracking system.

This intelligence product is provided to NICB member companies and law enforcement for informational purposes only and is not intended to be the basis for claims or other operational decisions. NICB's intent is to share pertinent information for the proactive detection, prevention, and

This intelligence product is provided to NICB member companies and law enforcement for informational purposes only and is not intended to be the basis for claims or other operational decisions. NICB's intent is to share pertinent information for the proactive detection, prevention, and

# Vehicle Theft Trend *Forecast*

**ForeCAST<sup>SM</sup> Report** 

Report Date: August 9, 2024      Geographic Scope: National; NY, TX  
Report Title: Q3 Vehicle Theft Forecast      Report Type: Vehicle  
Dissemination: Member Companies and Law Enforcement      Analysis Period: 01/01/2024 – 06/30/2024

**Executive Summary**

The following NICB ForeCAST<sup>SM</sup> was produced alongside the Q1-Q2 2024 Vehicle Theft Trend Report and includes a six-month national vehicle theft forecast, as well as sections focusing on areas at the CBSA and city levels that were highly impacted by vehicle thefts in the first half of 2024. The CBSA level analyses included in this report forecast theft numbers for Brownsville-Harlingen, TX, while the city level analyses forecast vehicle theft rates for Rochester, NY.

National vehicle theft totals are forecasted to increase in July and August. Thefts are projected to have the largest decrease in September, increasing briefly again in October before decreasing through the end of the year. The predictive models focusing on the monthly national theft totals included in the last edition of this report performed well, with an accuracy that implies high confidence in the values that were forecasted.

While the state of Texas experienced a 10% decrease in vehicle thefts reported in the first half of 2024 compared to the same time in 2023, the Brownsville-Harlingen, TX CBSA has experienced a 74% increase that is expected to continue increasing each month from July through December 2024.

Conversely, the city of Rochester, NY, previously identified as a high impact area in the 2023 Q1-2 Vehicle Theft Forecast<sup>1</sup> due to the 150% increase in vehicle thefts reported there at the time, had a 61% decrease during the first two quarters of 2024. The theft percentage decrease in Rochester, NY has contributed to the overall 18% decrease in vehicle thefts in the state of New York and are projected to continue decreasing each month through December 2024.

**Contents**

Section 1: Introduction.....	2
Section 2: U.S. National Vehicle Theft Forecast.....	2
Section 3: Brownsville-Harlingen, TX Forecast.....	3
Section 4: Rochester, NY Forecast.....	4
Section 5: Conclusion.....	5
Appendix: Methodology.....	6
Model Description.....	6



Monthly Vehicle Thefts, June & July

Texas CBSA Thefts, June & July

California City Thefts, May-August

# 2024 Medical Data Trends

---

- Medical QCs spiked in both Q1 & Q2 2024
- High-Impact States for Medical QCs
- Top Referral Reasons



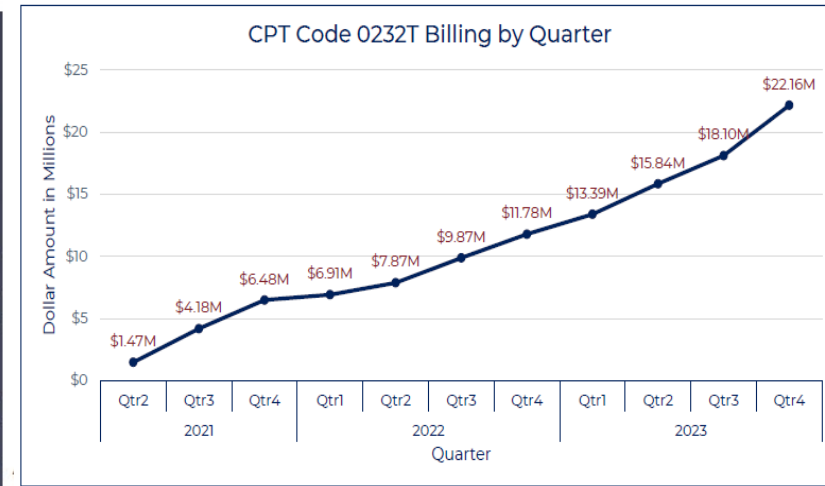
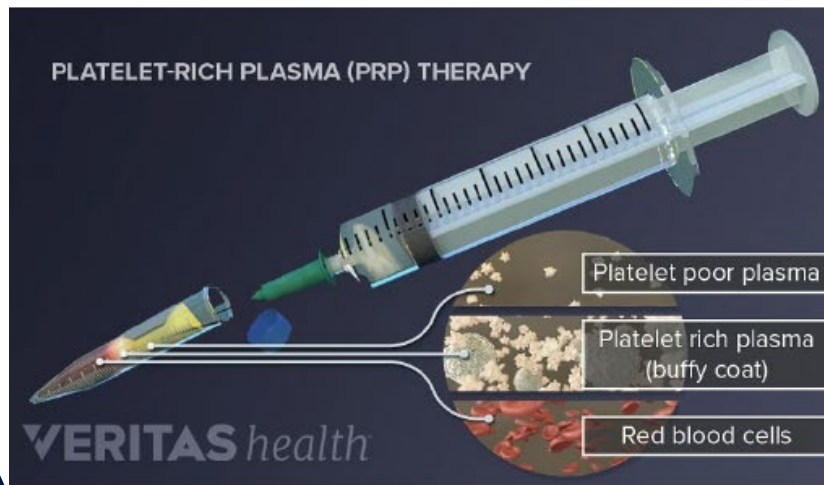


# Brain Mapping

---



# Platelet Rich Plasma Therapy



**CPT Code 0232T Billing by State – Top 10**

State	2021 (Q2 – Q4)	2022	2023	Total Billed	% Change 2022 – 2023
Florida	\$4,890,610	\$14,121,621	\$21,991,875	\$41,004,106	56%
California	\$2,638,654	\$8,100,133	\$16,609,004	\$27,347,791	105%
Georgia	\$1,438,998	\$4,765,916	\$9,675,755	\$15,880,669	103%
New Jersey	\$797,816	\$3,595,763	\$6,541,392	\$10,934,971	82%

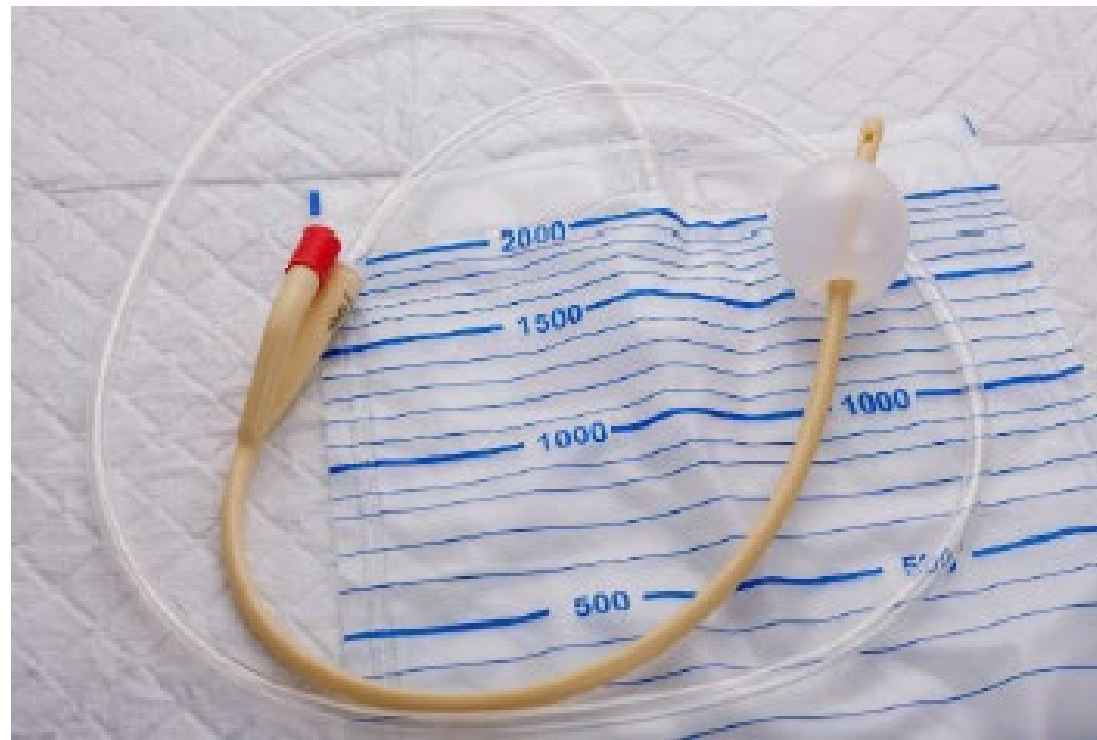
## Emerging States

**CPT Code 0232T Billing by State – Emerging States**

State	2021 (Q2 – Q4)	2022	2023	Total Billed	% Change 2022 – 2023
Missouri	\$4,697	\$9,699	\$66,726	\$81,122	588%
Michigan	\$645,154	\$901,246	\$4,633,517	\$6,179,917	414%
New Mexico	\$1,425	\$2,175	\$10,500	\$14,100	383%
Delaware	\$16,000	\$24,000	\$101,341	\$141,341	322%
Mississippi	\$0	\$400	\$1,650	\$2,050	313%

# Intermittent Urinary Catheters

---



# Slip and Falls

---



# Additional Trends

---

## COVID-19 Testing

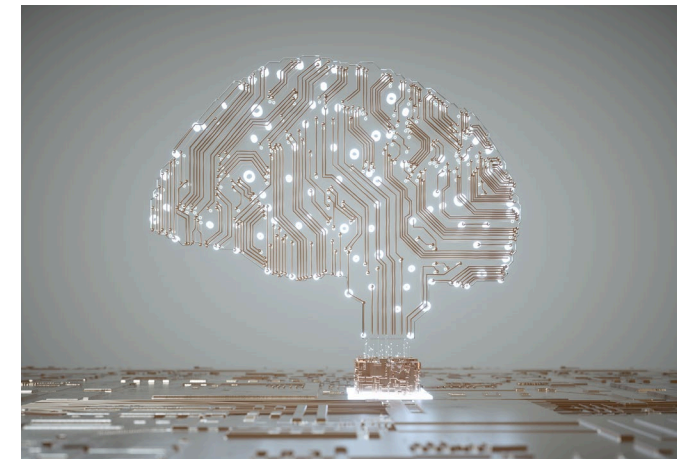
- Increase in volume of claims
- High dollars billed for tests
- Billing for services not rendered

## Durable Medical Equipment (DME)

- Increase in volume of claims / referrals
- Billing over-the-counter items as custom
- Misuse of HCPCS Code E1399

## Artificial Intelligence (AI)

- Altered medical bills
- Altered imaging reports



# Emerging Medical Scheme

---

## Mail-Order Prescriptions for WC Claims

- Cold calls to individuals pursuing W/C claims
- Claimant's info. DOB, SSN, Claim #
- Mail-order prescriptions
- Claimants deny authorizing treatments / meeting doctor



# Roofing

---



# Insight Report: CPN Fraud Risk

## Insight

### Credit Privacy Numbers Fraud Risk

Date: 6/28/2024  
Scope: National  
Type: General



DISSEMINATION: MEMBER COMPANIES AND LAW ENFORCEMENT//ORIGINATOR CONTROLLED (ORCON)

This Insight provides information for NICB member companies and law enforcement and is meant to aid in the combat and prevention of insurance crimes and fraud. The rise of incidents involving the misuse of credit privacy numbers (CPN) to commit fraud, file false police reports, and generate misrepresentation on official documentation has been steadily increasing over the past few years. Analyst Note: A CPN is not illegal to acquire or use and has a legitimate purpose but could be misused as described below.

A credit privacy number is a nine-digit number formatted to mimic a Social Security Number (SSN). CPNs aren't issued by the federal government and have no official legal standing. Social media and credit repair companies have purportedly pushed the idea that the use of a CPN as a SSN is a quick way for people to repair or hide their credit history, stating that CPNs fall under the Privacy Act of 1974. This Act allows individuals to protect themselves from unwarranted invasion of privacy resulting from the collection of their personal information, such as an SSN. CPNs are sometimes misrepresented as tools for establishing new credit identities. Legitimate uses of CPNs are strictly limited and do not include misusing them as an SSN when opening new credit cards, bank accounts, purchasing vehicles, applying for rental property, or filing insurance claims. Instead, CPNs should only be used for authorized purposes such as protecting personal information during transactions were providing an SSN is not legally required.

#### CPN Fraud Tactics, Techniques, and Procedures:

- Exploiting internet resources such as Tik-Tok tutorials, to learn about the misuse of CPN numbers and their benefits for fraud.
- Procuring a synthetic identity, including obtaining a CPN number through illicit means.
- Falsifying personal information on insurance applications or claims using the CPN number.
- Creating fake police reports or other documents to substantiate fraudulent insurance claims.
- Coordinating with accomplices to execute various stages of the fraud, such as fabricating documents.



For more information or to report similar events, contact the National Insurance Crime Bureau at [IntelligenceandAnalytics@nicb.org](mailto:IntelligenceandAnalytics@nicb.org)

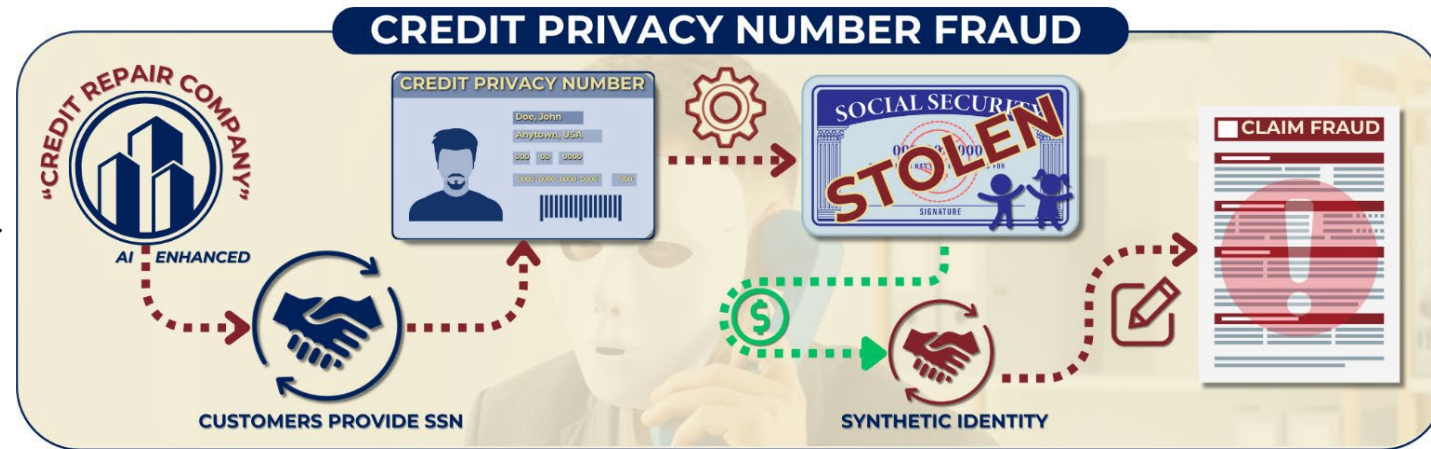
Copyright ©2024 by the National Insurance Crime Bureau. All rights reserved.

#### Investigative Strategies:

- Ensure a thorough background check on any individual suspected of using a CPN illicitly.
- Verify that the name and date of birth (DOB) match the individual's identity.
- Confirm that the CPN (being used as an SSN) corresponds to only one individual—the one listed.
- Compare all provided information with other official documentation, such as a driver's license.

**Analyst Note:** Unethical businesses and individuals may provide CPN numbers to individuals that are actual SSN numbers. For example, children, the elderly, and the incarcerated can often fall victim to their SSNs being sold as CPN numbers due to their lack of use. If the misuse of a CPN number is identified, it is important to report it.

## “Synthetic Identities: Powered by AI and CPNs”






# Photo Metadata Manipulation

photoinvestigator.co  
<https://photoinvestigator.co/the-app>


## The App - The Photo Investigator

WEB The **Photo Investigator** is an iOS **app** to view all image metadata (all the possible data stored ABOUT and within each photo). You can also remove photo metadata with an in-app purchase. The Investigator can also open ...



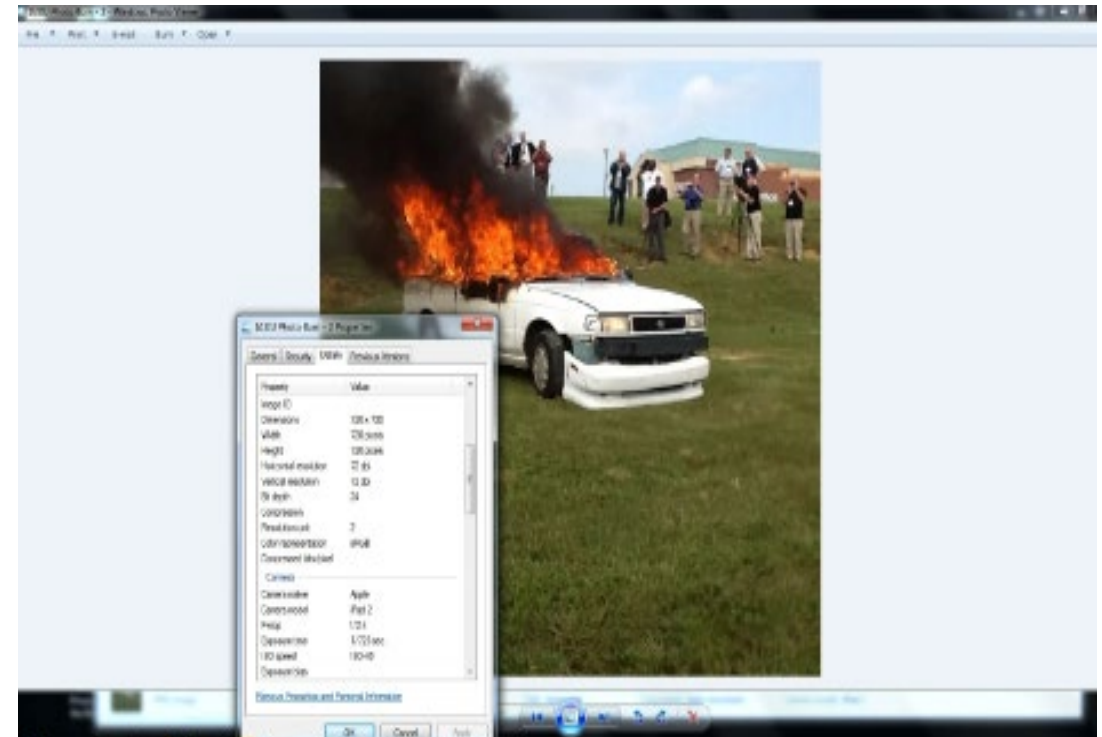
App Store  
<https://apps.apple.com/us/app/exif-metadata/id1455197364>

## Exif Metadata on the App Store

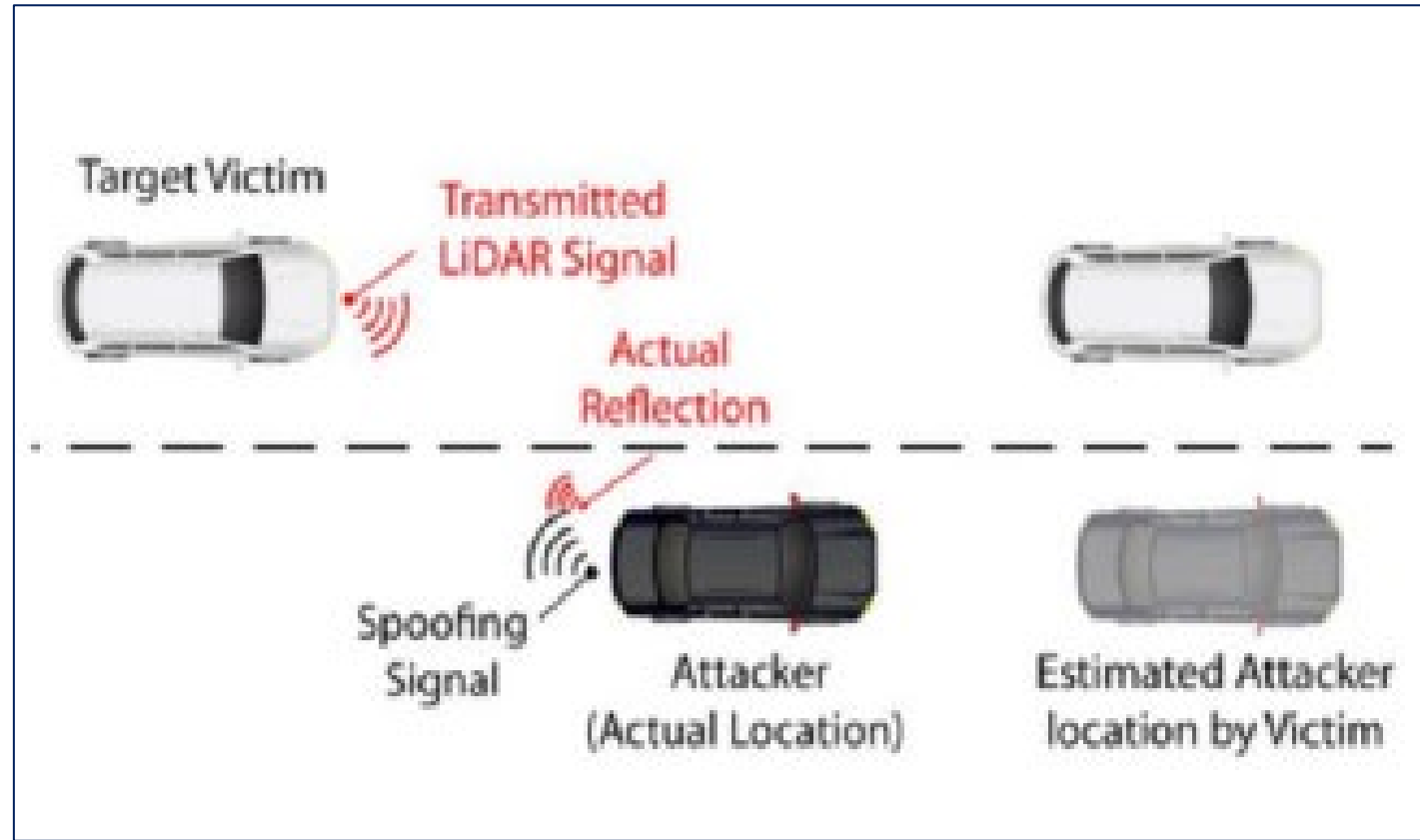


Newly added features make this app even more powerful than before. Give it a try! Exif Metadata lets you quickly and easily view, edit, and remove ... +

**4.6/5** ★★★★★ (5.3K)      **Size:** 14.2 MB  
**Age Rating:** 4+      **Category:** Photo & Video  
**Developer:** New Marketing Lab, ...

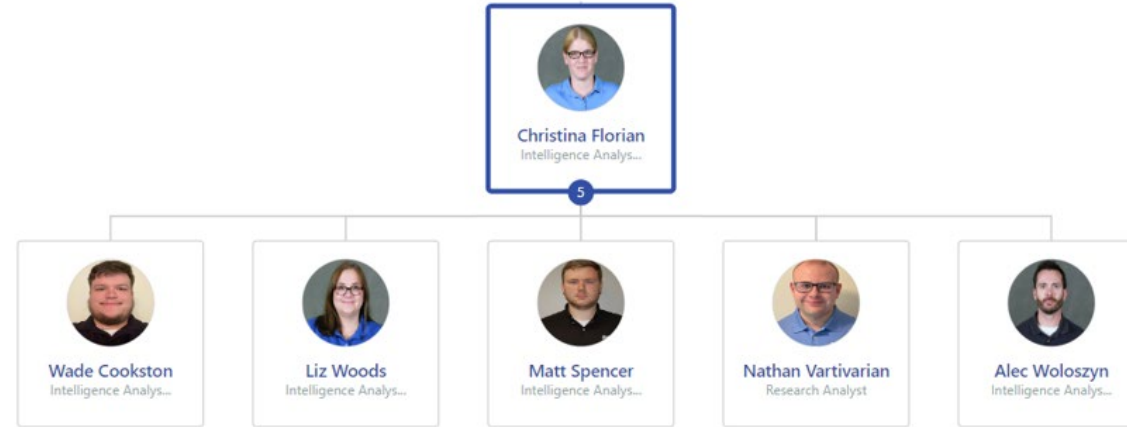


# LiDAR Spoofing (Autonomous Vehicles)

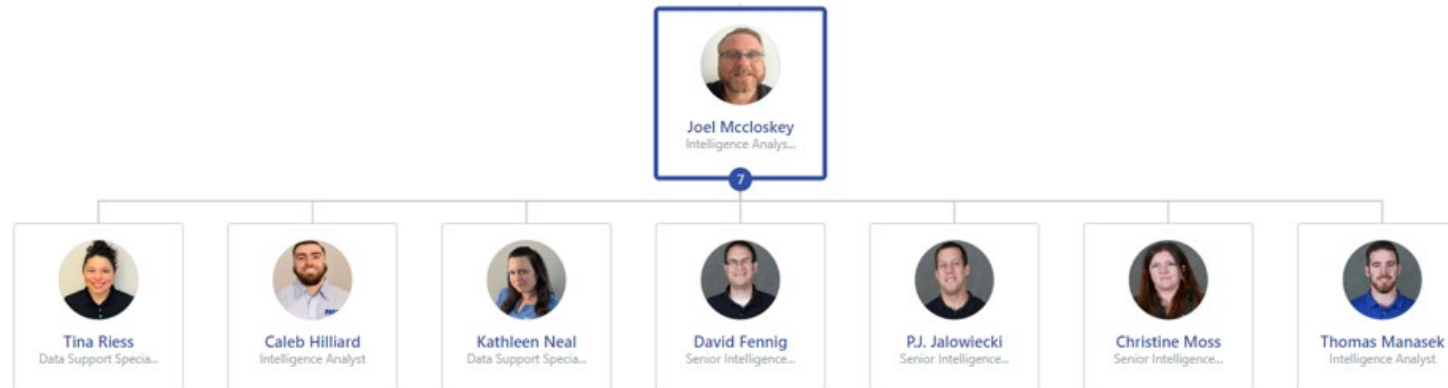


# NICB Analytical Teams

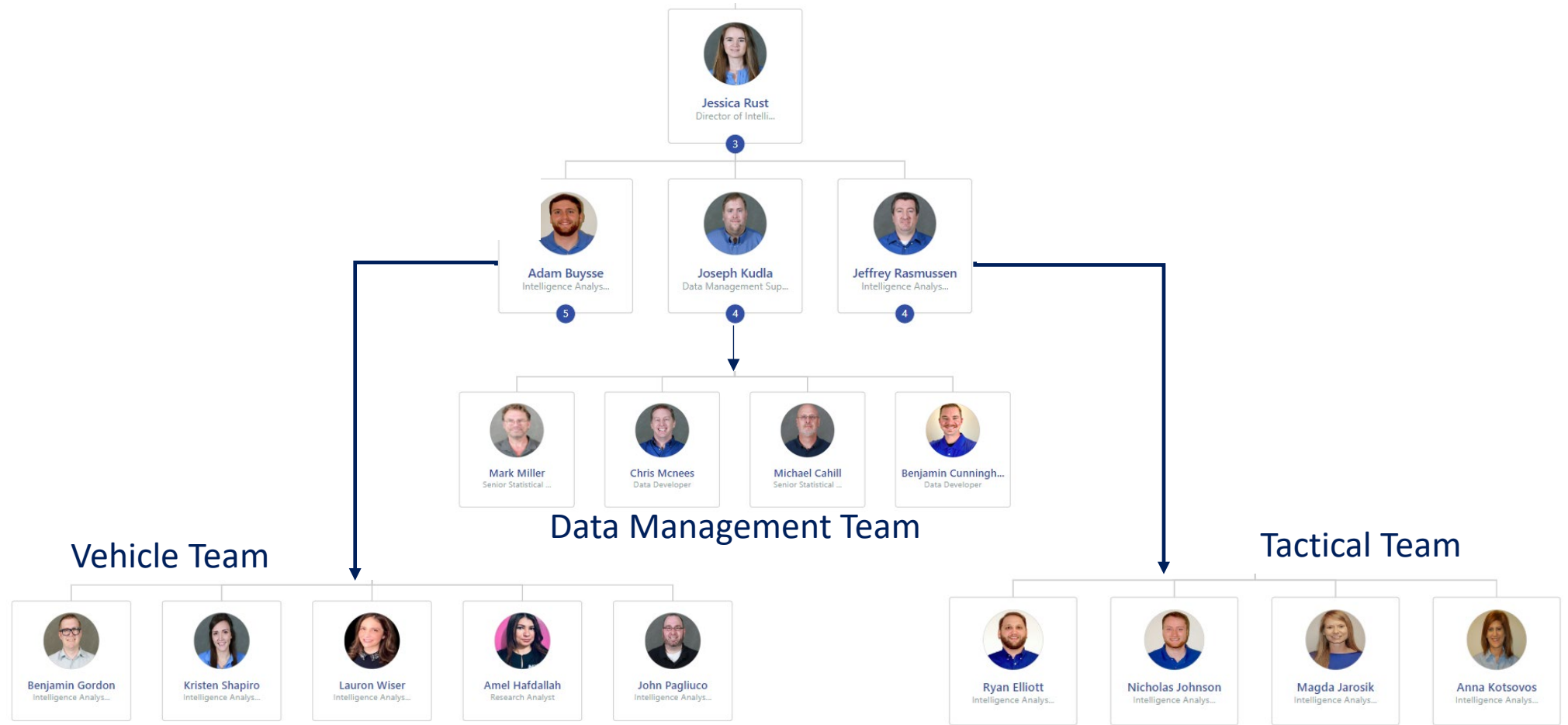
## Medical Team



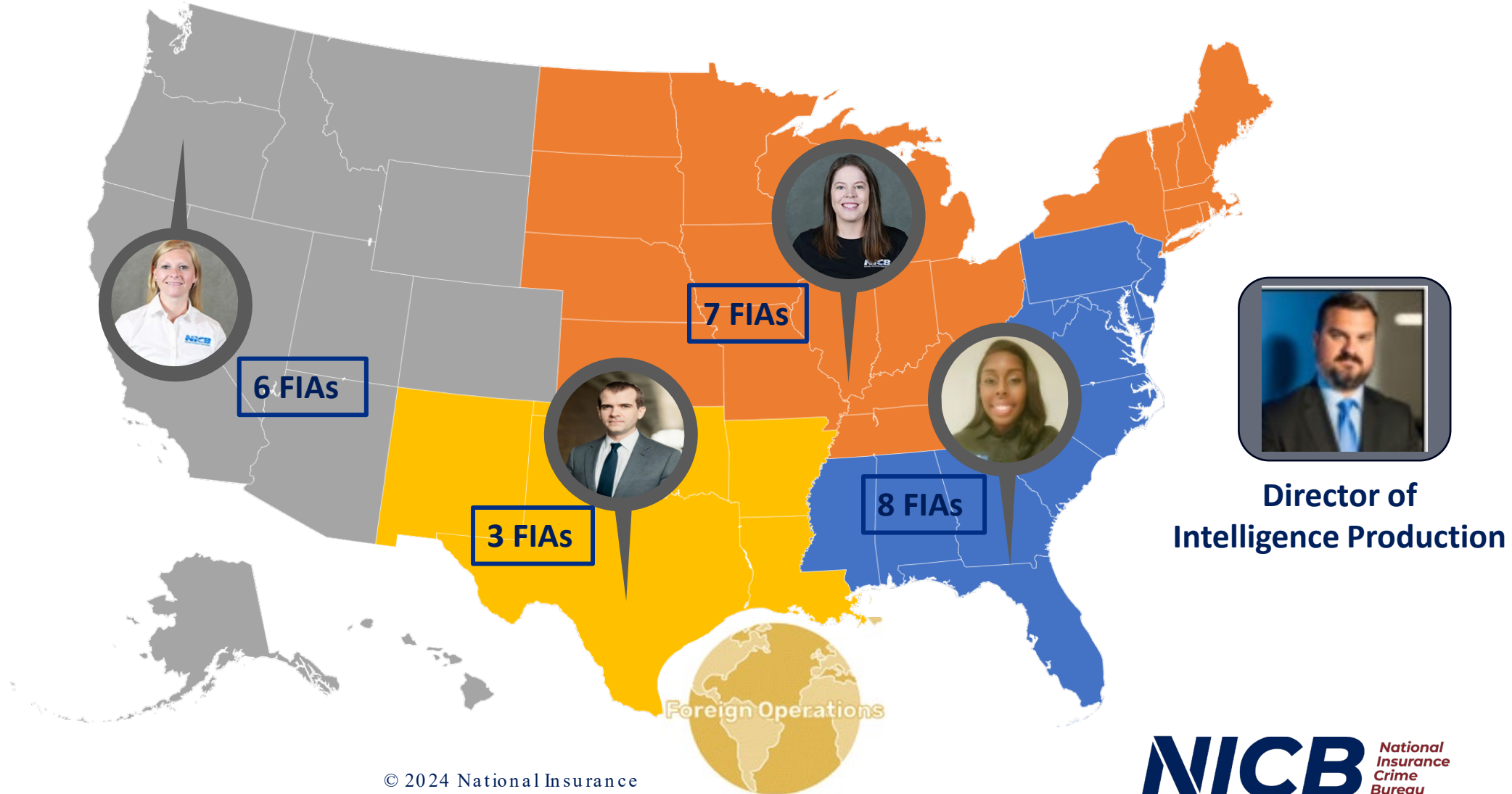
## Commercial & CAT Team



# NICB Analytical Teams



# NICB Analytical Teams



# NICB Cybersecurity & Data Privacy Policies

---

## *Ethical and Responsible Use of Data*

- *NICB Cybersecurity Incident Response Policy*
  - Updated 2023
  - Includes specific protocols for “High Severity Incidents”
  - Consistent with standards set by the National Institute of Standards and Technology (NIST)
- *NICB Privacy and Security Policy*
  - Updated 2024
  - Consistent with current law and best practices



# Data Privacy Laws

- *California*
- *Colorado*
- *Indiana*
- *New Jersey*

# California CCPA Fraud Exceptions

---

## § 1798.105

- *(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:*
- *(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.*



# Indiana Privacy Law Fraud Exception

---

## IN Senate Enrolled Act No. 5 (2023)

- Chapter 8. Limitations
- *Sec. 1. (a) This article shall not be construed to restrict a controller's or processors' ability to do any of the following:*
- ....
- *(7) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, investigate, report, or prosecute those responsible for any such action, and preserve the integrity or security of systems.*

# Data Privacy Laws

---

- *Connecticut*
- *Delaware*
- *Florida*
- *Iowa*
- *Maryland*
- *Minnesota*
- *Montana*
- *Nebraska*
- *New Hampshire*
- *Oregon*
- *Rhode Island*
- *Tennessee*
- *Texas*
- *Utah*
- *Virginia*

# Virginia Exemption

---

## Va. Code § 59.1-576

- *B. This chapter shall not apply to any ... (iv) nonprofit organization ...*

## Va. Code § 59.1-575

- *"Nonprofit organization" means ... any organization exempt from taxation under § 501(c)(4) of the Internal Revenue Code that is identified in Va. Code § 52-41....*
- NICB is explicitly named in Va. Code § 52-41.

# Thank you!

---

Jamie Walsh  
847-376-9349  
jwalsh@nicb.org