

TALI '25

October 10-18, 2025

galveston, texas



TALI TIP OFF

IN THIS ISSUE

- 3 President's Message
- 5 Ethics: Even When It Costs You Something
- 6 Flipper Device
- 9 Murphy's Law
- 10 TALI '25
- 13 Leveraging Access Control
- 16 Welcome New TALI Members!



2025 Board of Directors

Bob Washington
President
washington@noteboom.com

Mike Thompson, TBCI
President-Elect
mike@beardenonline.com

Grace Rubio
Region 1 Director
grace.rubio@rubioforensics.com

George Rodrigues
Region 2 Director
grodriguez@da-forensics.com

Barry Dunn, TBCI
Region 3 Director
barry@realtexaspi.com

Samantha Santiago
Region 4 Director
samantha@premierpathfinders.com

Connie Vogler
Region 5 Director
eoi@eoiinc.net

Dave Shafer, TBCI
At-Large Director Position 6
dave@preferredintelligence.com

Connie Briggs
At-Large Director, Position 7
connie@briggspi.com

Michelle Mondo
At-Large Director, Position 8
mmondo@mondoinvestigations.com

Caroline Gear
At-Large Director, Position 11
carolinegear@kleininvestigations.com

TALI Mission Statement

The Texas Association of Licensed Investigators is an organization that promotes and encourages the highest standards of professionalism among licensed private investigators through information, education, training, legislative action, membership support and networking.

Code of Ethics

All members of the Texas Association of Licensed Investigators will subscribe to the following Code of Ethics:

- To be professional and to demonstrate integrity and honesty as an investigator and as a member of TALI.
- To give each client a full explanation of the work to be performed, rates to be charged and reports to be rendered.
- To preserve as confidential all information received in an investigation unless directed otherwise by the client or unless under specific order or legal authority.
- To conduct all aspects of investigation within the bounds of legal, moral and professional ethics.
- To apprise clients against any illegal or unethical activities and to cooperate with law enforcement or other governmental agencies, as required by law.
- To constantly strive for improvements as a professional, to respect the rights of others and to insure the same from and to one's employees and subcontractors.
- To loyally support TALI, its aims, purposes and policies as long as one remains a member.

2025 Board Support

Karl Snow
Treasurer
karl@purplemountainpi.com

Jolie Estes, MS, CAE
Executive Director
admin@tali.org



Robert Washington
TALI President

President's Message

As the first year of my TALI Presidency is drawing to a close, I am thrilled to share that our TALI community has grown to an impressive 714 members! This milestone reflects the strength and dedication of our organization, and I'm grateful for each of you who continue to drive our mission forward. Your commitment to advancing our shared goals is what makes TALI so vibrant and impactful.

With the October 10th voting deadline fast approaching, I urge every member to make their voice heard. Voting is your opportunity to shape the future of TALI – your participation ensures our leadership and initiative align with our collective vision. Please take a moment to cast your vote and encourage fellow members to do the same. Together, we can set the course for an even stronger TALI.

Looking ahead, I'm incredibly excited for TALI '25! This year's event promises to be our most dynamic yet, with inspiring speakers and unparalleled networking opportunities. Mark your calendars and get ready to connect, learn, and celebrate the spirit of TALI.

Thank you for your continued support and engagement. Let's keep the momentum going as we build an even brighter future together.



What will this partnership enable you to do, besides save money?

- **Increase Your Network.** Size matters when increasing your potential business or employment opportunities. Network among a few or cast a wide net to gain valuable exposure to thousands.
- **Obtain New Clients.** Many investigators have clients needing services in California or Florida occasionally. Big 3 provides more resources to assist those clients locally.
- **Provide New Services.** Expand your network, expand your services and explore additional revenue streams.
- **Expand Your Footprint.** Cultivate relationships with local investigators in these states. Focus on growing your business opportunities.
- **Legislative and regulatory support.** The goal of each of these associations has always been to protect their interests and their membership.
- **Lead generation.** Each association website and private Listserv is a great way for Big 3 members to communicate with, and locate someone to help with that new case.
- **Recognition.** As a member of the oldest, and largest statewide PI associations you are among your professional peers in every state.



To learn more about joining CALI click [here](#); or visit FALI [here](#) for more information on membership in those states.



**EXPERT INVESTIGATIONS, INTELLIGENCE, AND
RISK MANAGEMENT** **ALL ACROSS CANADA!**

+1 514 309 1010

info@madpiglobal.com

madpiglobal.com

ETHICS

Even when it costs you something

Lloyd Young
SECURAC, Incorporated

I was retained by the defense on a double homicide case as an alarm systems expert. The case entailed a teen who was charged with the murder of the teen's parents who were killed in the middle of the night as they were sleeping.

The defense sought me out after hiring another expert from far away who had already billed the defense team in the neighborhood of \$50,000 for the case, with more to come. The defense team thought that finding an expert in the same city as the trial court would be a better financial decision.

The previous expert had proffered the scenario that a door was possibly left ajar and demonstrated how the alarm system could have been armed with the door unsecured and bypassed. There was even a video created by this other expert that demonstrated this bypass functionality in a reenactment. And it all sounds plausible and would in fact create some reasonable doubt, which was why the defense team showed their interest in my testimony following the same line of thought as the previous expert. The only problem was that it was a fabrication.

Upon review of the alarm monitoring records, it was immediately clear to me that the alarm system had not, in fact, bypassed the door in question on the night of the murders. The system records plainly showed that the door had been closed that evening when the alarm had been set for the night, and was armed and secure until the police observed through the window as the teen disarmed the alarm in the wee hours of the morning after the 911 call.

This simple fact was an apparent obstacle in the defense's portrayal of the accused's story.

So, I laid out the facts as they were. They didn't ask my opinion and I certainly didn't offer one, but it became clear that there wasn't a \$50,000 payday in my future. The attorney I was reporting my findings to simply wrote me a check for my time and said I was no longer needed on this case.

It never crossed my mind to fabricate a scenario that contradicted the facts. But apparently, that isn't the case with every investigator/expert.

Ethics Challenge Number Two: You know the truth. The team that retained you has shunned you because of your plain statements of fact that doesn't help the jury have doubt about their client's guilt. Do you reach out to the other side? The answer to that is also a hard no.

It is a no-brainer to not betray the trust of the courts and the principles of truth and honesty for monetary gain, but on the other side of that coin, it can be a struggle to not speak the truth in violation of a trust relationship you made with a team promoting a false narrative! But right is right, and agreements must be honored.

Fortunately, the prosecution pulled together the evidence without my help and convinced the jury of the teen's culpability. And justice was served. This time. But win or lose, we must hold the rudder on a straight path of honor, ethical conduct and trustworthy practices to our clients, to the courts and ultimately, to ourselves. No matter what the financial or emotional costs we bear.

Flipper Device

Ian Mason, DSMO
DNA Security Services

Understanding the Risks of Duplicating Access Cards with a Flipper Device

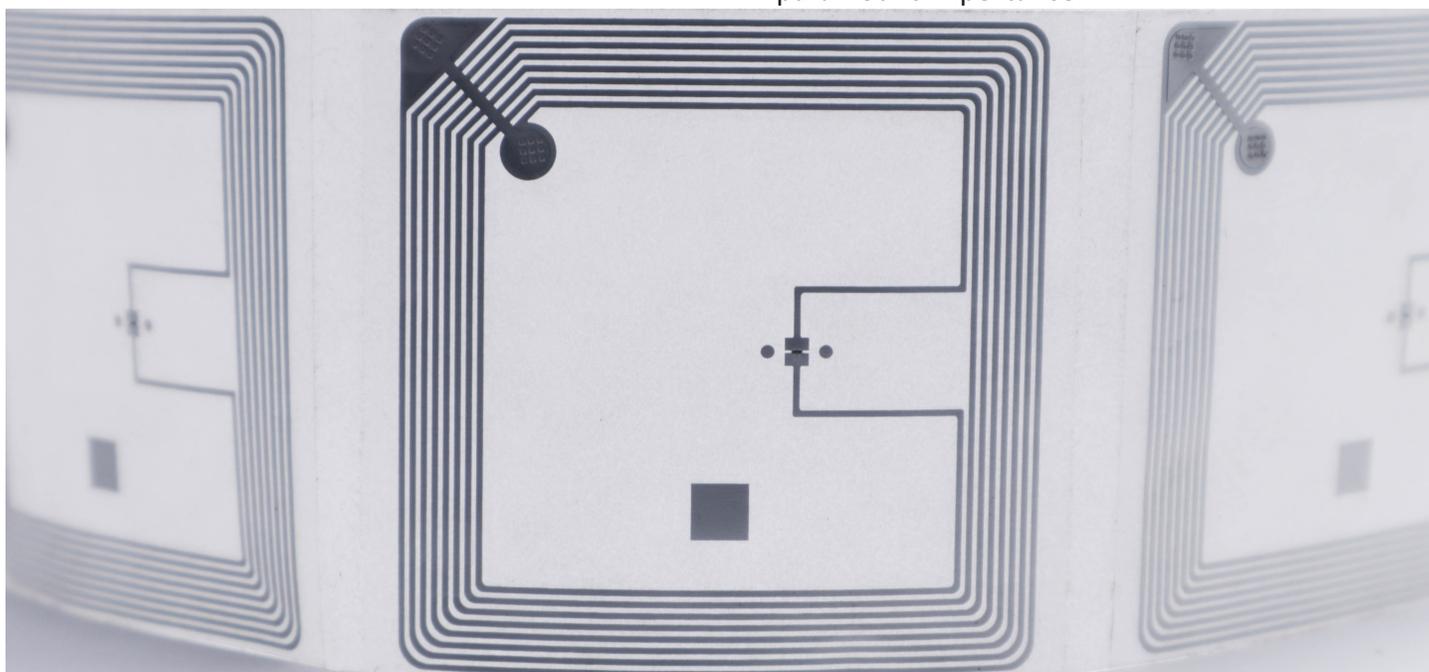
As licensed investigators, especially members of the Texas Association of Licensed Investigators (TALI), it is crucial to stay informed about evolving security threats and the methods used to bypass security measures. One rising concern in the field of access control is the use of devices such as the Flipper Zero to duplicate access cards. As convenient and versatile as these devices can be for security testing and ethical hacking, they also pose significant risks when used maliciously.

In this article, we will explore what a Flipper device is, how it can be used to duplicate access cards, the potential implications for investigators and security professionals, and what can be done to mitigate these risks.

What is a Flipper Device?

The Flipper Zero is a multi-functional device often marketed as a portable tool for pen-testing and security research. It's capable of reading, storing, and emulating various types of wireless signals, including RFID (Radio-Frequency Identification), NFC (Near-Field Communication), and even infrared. With its small form factor and user-friendly interface, the Flipper Zero allows security researchers to interact with access control systems, unlock doors, clone access cards, and more—all for legitimate testing purposes.

However, with great power comes great responsibility, and there is a growing concern that such devices can be misused by individuals with malicious intent. This is especially relevant for investigators who often encounter sensitive environments where access control is of paramount importance.



The Process of Duplicating Access Cards Using a Flipper Device

Duplicating an access card with a Flipper device generally involves the following steps:

- 1 *Reading the Card's Information:* The Flipper Zero can scan and read the information embedded in many types of RFID and NFC access cards. By holding the Flipper close to the card, it can capture the signal frequency and the card's unique identifier.
- 2 *Storing the Information:* Once the information is read, the Flipper stores the card's data in its memory. The device can store multiple card identifiers, allowing the user to switch between different credentials as needed.
- 3 *Emulating or Cloning the Card:* After capturing the card's data, the Flipper can emulate the original card's signal, effectively functioning as a duplicate card. Alternatively, the data can be written to a blank RFID or NFC card, creating a physical duplicate that behaves exactly like the original.

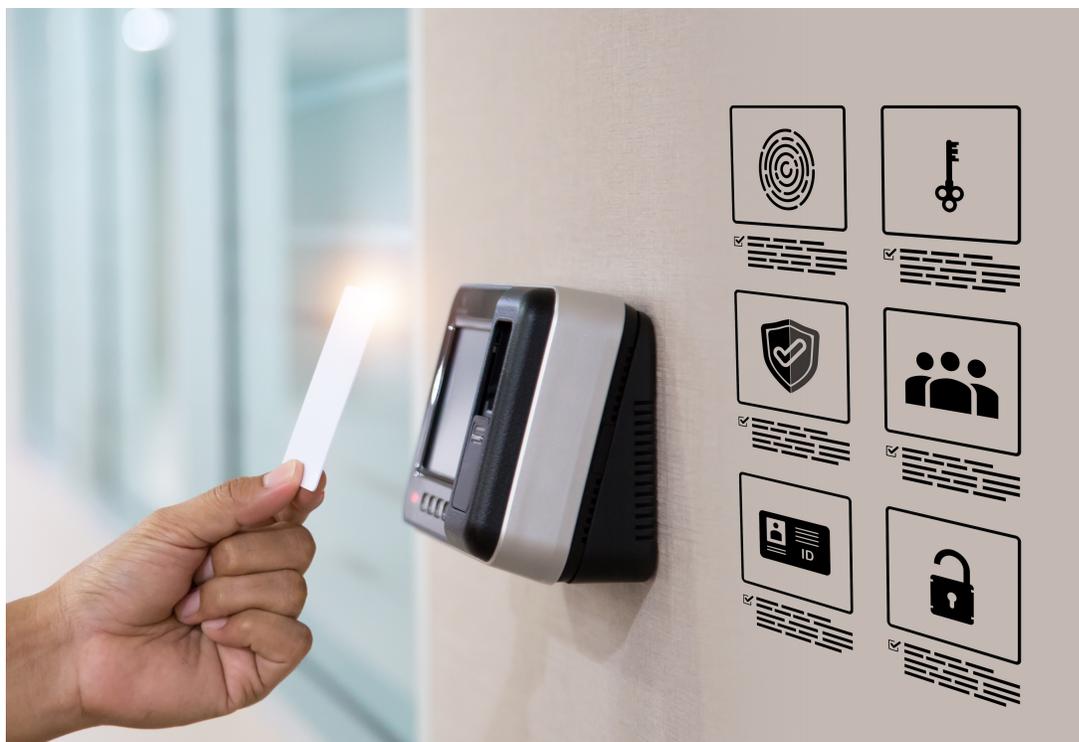
The process is straightforward, making it accessible even to individuals without a deep understanding of security systems. As such, it presents a significant risk to facilities that rely on RFID or NFC-based access control systems.

Implications for Investigators

For licensed investigators, understanding the potential threat posed by devices like the Flipper

Zero is crucial for several reasons:

- 1 *Assessing Security Vulnerabilities:* As part of your investigative work, you may be tasked with evaluating the security of a client's facility. Knowing that access cards can be easily duplicated using affordable devices like the Flipper allows you to better assess the risks and recommend stronger security measures, such as multi-factor authentication.
- 2 *Preventing Unauthorized Access:* When investigating sensitive cases, such as corporate espionage, employee theft, or internal fraud, you need to be aware that potential suspects could gain unauthorized access using cloned access cards. This insight can inform your security recommendations and investigative strategies.
- 3 *Legal and Ethical Considerations:* While using a Flipper device for testing purposes may be lawful if conducted with the proper permissions, duplicating access cards without authorization can breach legal boundaries. Investigators must be cautious to stay within the scope of their legal rights and adhere to ethical standards while conducting security assessments.



How to Mitigate the Risk of Card Duplication

Given the ease with which devices like the Flipper Zero can duplicate access cards, it's essential for investigators to advise clients on measures to secure their access control systems. Here are some best practices:

- 1 *Use Encrypted and High-Frequency Access Cards:* Not all access cards are created equal. Low-frequency cards (125kHz) are typically more vulnerable to cloning than high-frequency (13.56MHz) cards, especially if the high-frequency cards are encrypted. Consider advising clients to upgrade their access control systems to use more secure card types.
- 2 *Implement Multi-Factor Authentication (MFA):* Adding a secondary form of authentication, such as a PIN or biometric verification, can significantly reduce the risk of unauthorized access, even if a card is duplicated. MFA provides an additional layer of security that attackers cannot easily replicate.
- 3 *Regularly Audit and Update Access Credentials:* Encourage clients to routinely review and update their access credentials. This may include deactivating unused cards, rotating access codes, or resetting permissions for users who no longer require access.
- 4 *Install Anti-Cloning Detection Systems:* Some advanced access control systems can detect cloned cards by identifying irregularities in the signal frequency or the card's data structure. Installing such systems can help catch cloning attempts in real-time.

Recommendations for Investigators

As an investigator, your role extends beyond merely identifying security flaws; you also have a duty to provide actionable recommendations that can enhance your client's security posture. When addressing potential threats from card cloning

devices like the Flipper Zero, consider the following:

- **Conduct Penetration Testing with Permission:** If you have obtained the proper authorization from your client, use devices like the Flipper Zero to test the vulnerabilities of their access control systems. This can help you provide a comprehensive assessment of their security.
- **Educate Clients on Security Awareness:** Many organizations may not fully understand the risks associated with outdated access control systems. Educating your clients on the benefits of using encrypted cards, implementing MFA, and regularly updating security protocols can help prevent breaches.
- **Stay Updated on Emerging Security Threats:** The landscape of security threats is continually evolving. Stay informed about new techniques, devices, and countermeasures that could impact access control systems. This knowledge will enable you to provide up-to-date advice and maintain your credibility as a security expert.

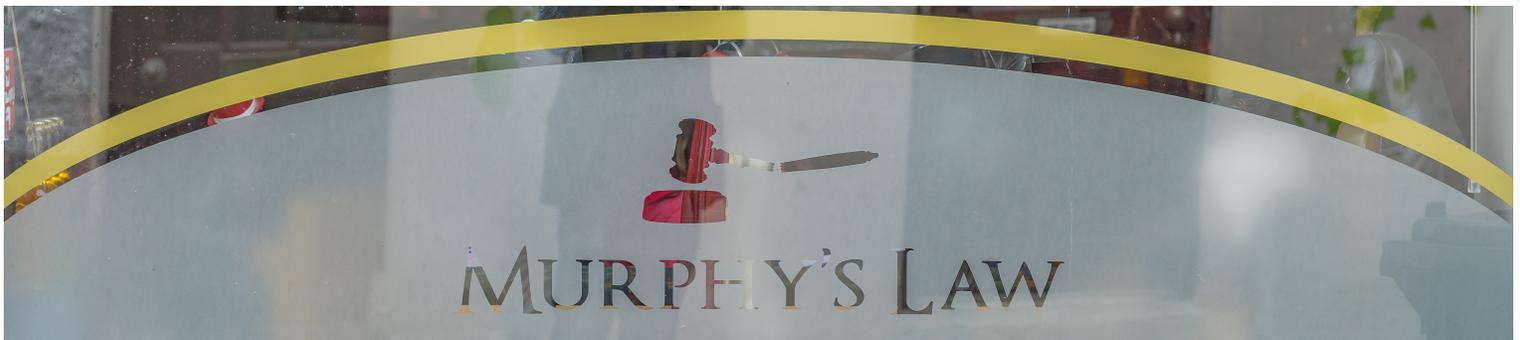
Be Prepared

The ability to duplicate access cards using a device like the Flipper Zero poses a real and growing threat to security systems that rely on RFID and NFC technology. For licensed investigators, understanding this threat and its implications is crucial to maintaining the integrity of your investigative work and advising clients on how to protect their facilities. By implementing modern access control solutions, conducting regular security audits, and adopting multi-layered authentication strategies, investigators can help their clients stay one step ahead of potential attackers.

Murphy's Law, White Collar Investigation version

Fred Olivares
Talon Investigations

- 1 Victims of fraud will always be more willing to cooperate than subjects.
- 2 That "smoking gun" document, if it exists, lies in some attachment to a mundane email, a box in the far corner of the evidence room, or in a storage device you misplaced.
- 3 You never will know as much as the subject/client in the case about what truly happened.
- 4 That question you just asked was stupid, but needed to be asked.
- 5 The briefing you give to your boss/client/board will have an informational gap that you failed to fill. You will be asked about it.
- 6 Your case will take a turn you didn't predict, or couldn't have even imagined.
- 7 An insignificant document early in the case will be important later in the case. You will forget where it is.
- 8 The approximate ratio of pertinent emails to non-pertinent is about 1:125. But you must review each one.
- 9 That important witness that's cooperating in your case has not told you everything. What they haven't told you will blow a hole in their credibility, and maybe the case.
- 10 That important document is worthless until the person who created/received it can bring it to life. And that person isn't cooperating.
- 11 What's important to the case, is not necessarily important to the person you're interviewing. And vice versa.
- 12 Small cases, small problems; big cases, big problems.
- 13 When you know more about the case's subject matter than your expert witness, it's time to get a new expert witness.
- 14 If your client is the subject of a Government investigation, remember the Government has no budget.
- 15 The Government has not revealed everything they know. The defendant/client knows the same information but has not told their attorney.



TALI '25

October 10-13, 2025

galveston, texas



Texas Association of Licensed Investigators
5014 FM 1500
Paris, TX 75460
877-605-7055
Conference Chair: Philip Klein, 409-729-8798

FRIDAY



- 9:00 AM TILT, New Investigator Training**
East Mainsail
TBCI Mock Scenario & Testing
Leeward
Pre-Con
West Mainsail
- 5:00 PM Welcome Reception**
Foyer of Conference Center
- 6:00 PM Conference Kick-Off Clam Bake**
Pool Deck/Hill

SATURDAY

- 7:30 AM Breakfast**
Foyer of Conference Center
- 8:00 AM Welcome & Legislative Update**
Mainsail
- 9:00 AM Mastering the Art of Impactful Communication**
Mainsail
- 10:30 AM When Worlds Collide: The Investigator and Human Trafficking**
Mainsail
- 11:30 AM Conducting Investigations Utilizing AI; Identifying the Deep Fake**
Mainsail
- 12:30 PM Lunch & Business Meeting**
Foyer of Conference Center
- 2:00 PM Board Rules**
Mainsail
- 4:00 PM The Role of the Private Investigator in Criminal Defense Cases**
Mainsail
- 5:00 PM Reception**
Foyer of Conference Center
- 6:00 PM Awards Banquet & Silent Auction**
Mainsail

A blue, metallic-looking rectangular badge with rounded corners and four small circles at the corners, containing the word "SUNDAY" in white, bold, sans-serif capital letters.

- 7:30 AM Breakfast**
Foyer of Conference Center
- 8:00 AM Branch Davidian Trial**
Mainsail
Connecting the Dots
Elissa
- 9:00 AM Leveraging Cell Phone Data**
Mainsail
Judgment Enforcement & Asset Recovery
Elissa
- 10:30 AM Recognizing & Utilizing 3D Data in Private Investigations & Court**
Mainsail
TLO/TransUnion/Indigo
Elissa
- 11:30 AM Ethics for Lunch**
Mainsail
- 1:00 PM Investigating the Worst of Society**
Mainsail
- 2:30 PM School Massacres: Why They Continue to Occur and How to Stop Them**
Mainsail
- 4:00 PM Focus Groups and the Criminal Process**
Mainsail

A silver, metallic-looking rectangular badge with rounded corners and four small circles at the corners, containing the word "MONDAY" in black, bold, sans-serif capital letters.

- 8:00 AM Civil Process Server**
Elissa

Leveraging Access Control

Ian Mason, DSMO
DNA Security Services

Leveraging Access Control and Video Surveillance for Investigators: Key Insights and Best Practices

As professional investigators, you know firsthand the importance of having the right tools at your disposal to uncover the truth, protect clients, and resolve cases efficiently. As fellow members of the Texas Association of Licensed Investigators (TALI), we at DNA Security Services understand the unique challenges you face. With the rise of sophisticated security threats and the need for actionable evidence, leveraging technology—particularly Access Control and Video Surveillance—can significantly bolster your investigative capabilities.

In this article, we delve into how modern security solutions can serve as powerful tools in the field of investigation, enhancing your ability to gather evidence, verify claims, and maintain security protocols.

Access Control: A Crucial Element for Investigators

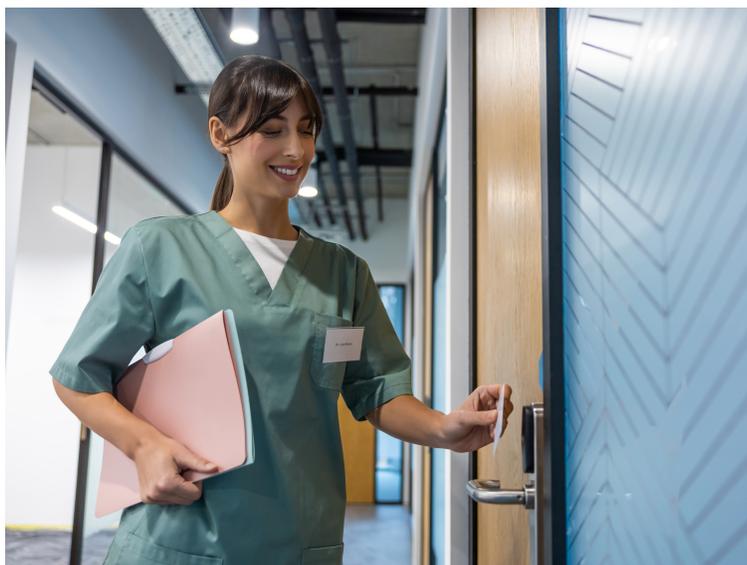
Access Control isn't just about restricting physical entry; it plays a critical role in helping investigators manage and monitor sensitive environments, especially in situations where the timeline of movements and activities needs to be documented precisely.

How Access Control Supports Investigative Efforts

1. **Timeline Verification:** When investigating incidents like employee theft, data breaches, or unauthorized access, you can

use access logs to establish a timeline. Knowing exactly who accessed a specific area and when can often be the missing piece that helps connect the dots in your investigation.

2. **Secure Handling of Evidence:** Investigators may need to control access to evidence rooms, surveillance footage storage, or other critical areas. Access control allows you to set permissions, ensuring that only authorized personnel can handle or view



sensitive materials. This supports the chain of custody and ensures compliance with legal standards.

3. **Preventing Tampering:** In cases where you need to restrict access during an investigation—such as locking down a crime scene or securing data servers—access control can enforce those restrictions without having to physically be on-site, adding a layer of security to

protect crucial evidence.

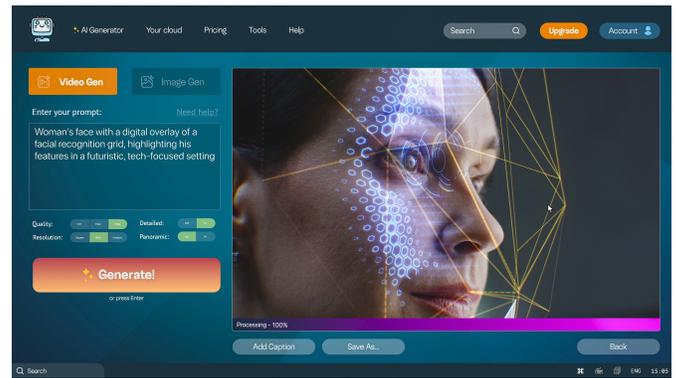
Key Features of Advanced Access Control Systems for Investigators

- **Detailed Reporting:** Comprehensive access logs can help you identify suspicious patterns. For instance, if certain areas are accessed during unusual hours, or if someone frequently attempts to enter restricted zones, it could indicate misconduct or preparatory actions for a larger crime.
- **Remote Management:** Cloud-based access control systems allow you to remotely lock or unlock doors, add or revoke access permissions, and monitor entry logs from any location. This can be particularly useful during multi-location investigations or when managing teams in the field.

Video Surveillance: A Vital Tool in Evidence Gathering

Video Surveillance goes beyond just monitoring—it's about capturing crucial details that can make or break a case. For investigators, high-quality footage and analytics capabilities are invaluable for validating claims, supporting testimonies, and providing irrefutable evidence in court.

How Video Surveillance Enhances Your Investigative Work



1. **Corroborating Statements:** Surveillance footage serves as an unbiased witness. In scenarios where different parties provide conflicting statements, video evidence can clarify what actually occurred. Whether it's a slip-and-fall accident in a commercial establishment or a suspected case of harassment, cameras often provide the definitive account.
2. **Identifying Key Players:** In criminal investigations or missing persons cases, footage can help you identify suspects, witnesses, or individuals involved. AI-powered facial recognition can even match people captured on camera with existing databases, saving valuable time.
3. **Tracking Movements and Behavior Patterns:** High-quality surveillance footage allows investigators to track the movements of individuals over time, analyze behavior patterns, and identify potential accomplices. This can be



especially useful in cases of organized crime or ongoing fraud investigations.

Leveraging Advanced Surveillance Technology



Today's video surveillance systems offer capabilities that extend well beyond traditional CCTV cameras:

- **Facial Recognition and AI Analytics:** Modern systems can identify known individuals, detect unusual behaviors (e.g., loitering, rapid movements), and even alert investigators to unattended objects. This enables you to be proactive in detecting threats or suspicious activities. But do keep in mind Facial Recognition Searches in the state of Texas are prohibited by law.
- **High-Definition and Low-Light**

Performance: Clear, detailed footage is essential for making accurate identifications and observations. Advanced cameras with low-light capabilities ensure that you don't miss critical details, even in dimly lit environments.

- **Mobile and Remote Access:** You can monitor live feeds or review footage from any location using your smartphone or laptop, making it easier to stay on top of cases when you're on the go.

Best Practices for Investigators Using Access Control and Video Surveillance

To maximize the impact of Access Control and Video Surveillance in your work, consider implementing these best practices:

1. **Integrate Systems for a Comprehensive View:** Combining access control with video surveillance provides a more complete picture of events. For instance, linking an access control log entry with corresponding video footage allows you to verify who entered a room and what they did while inside.
2. **Use Metadata and Analytics to Streamline Investigations:** Search for specific behaviors, times, or events within video archives using metadata tags and AI analytics. This significantly reduces the time needed to find relevant footage.
3. **Maintain Regular Audits and Equipment Checks:** To ensure your tools are always ready for use, perform routine maintenance on both access control and surveillance systems. Firmware updates and camera cleanings can prevent technical issues that could impede your investigations.

Welcome to our newest TALI members.



Region 1

Jonathon Appleby
Steven Appleby
Blakely Bates
Kristi Bates
Noah Beaudette
Kevin Brownlee
Scott Cook
Tracey Copeland
Virginia Curry Ph.D
Clint Eastep
Shawnte Kinney
Coleman McKoy
David Melrose
Devin Morgan
Katy Osthoff
Dillon Richardson
Barbara Russell
Kim Sanders
Jennifer Sedwick
Nurettin Senol
Trenton Steen
Jesseca Williams

Region 2

Zoya Bernadas
Carl Bialorucki
Michelle Brown
Stephanie Buta
John Clark
Steve Hickman
Brian Lonidier
Graham McGruer JD
Krissy Morrison
Lindsay Nichols
Cristin Gray Vargas
Stephane Vodio

Region 3

Dayana Alas
Lucien Camara
Neal Carlson
Christian Casson
Hope Edmondson
John Fernandez Jr.
Mark Gilbert
Sean Hanley
Steven Hayden
Orville Hudson
Judith Johnston
Barney (Rob) Johnston III
Jimmie Kaelin Jr.
James Patrick Kennedy
Kelley Leslie
Ashley Miller
Henry Moffett
Noe Rincones
Andre Robinson Sr
W Schwartz
Ana Sexton
Betty Simons
Celeste Sutherland
Jimmie West
Michael Ybanez
Rosalinda Ybanez

Region 4

Abel Acuna
Ashley Clay
Jim Cole
Cindy Fisher
Madeline Frazier
Melanie Harrington
Margaret Jones
Rogerio (Billy) Lopez
Jason McLendon
Ashley Napariu
Ryan Plumley
Timothy Quinn
Harry Reyes Romero
Holly Todd
Stefanie Villarreal
Tucker Witt

Region 5

Roger Brown
Joseph Confessore
Gerardo Morales
Rafael Ruiz
Melissa Stallings

Out of Texas

Debra Allen
Toby Braun
Thomas Cashio
Jim Casteel
Moses Castillo
Bill Clutter
Leisha Fenton Fauth
Troy Fleming
Daryl Flowers
Caesar Gonzalez
Nathan Goode
Anthony Green
Olga Hasbón
Paul Ingels
Lindon Lilly
Gregory McCormick
Matthew Palmer
Stephanie Palmer
Kenneth Paulson
Nicholas Sandberg
Matt Seavey
Jeremy Skehan
Richard Stride
David Williams