The Sentinel

IACSP.org
International Association of Certified Surveillance Professionals

January, 2023
Volume 2, Issue 1

Happy New Year 2023!

First of all, a huge thank you to our membership and our Board of Directors for another great year for the IACSP! During 2022 we made a lot of important decisions that will impact our association and our industry for the future. As we are all work primarily in the gaming industry and do so currently; we are able to keep focused on what is important to our membership. Because of that focus the Board, during 2022, accomplished the following:

- Completed and issued our 2nd Annual Surveillance Directors Survey. The results provided by the survey identified significant useful information concerning wages, staffing, training, operations, levels and types of criminal activity and advantage play, and the emerging trends in our industry. Thank you to all that participated in the survey and I encourage you to be on the look out for survey in 2023.
- Conducted for training webinars for our membership throughout the year. These webinars focused on surveillance tradecraft and the information necessary for members to prepare for the CSP examination.
- Thanks to the efforts of Board Member Stephanie Wallace, we are again publishing our Association's newsletter, "The Sentinel." The fruits of those efforts are what you are reading today! For those of you seeing fame and fortune as a writer, now's your chance, we need contributions!
- We have and are redesigning our website to make it easier to use and to be a repository of all things surveillance where we all can go to for information and assistance.
- We are completely updating and revising our body of knowledge, course syllabus, and certification requirements for the CSP certification. Surveillance is no longer just table games and slots. We are casino resort protection and all that entails. Our domains of knowledge and expertise are: Surveillance Tradecraft and Operations, Game Protection, Video Technology and Analytics, Investigation and Reporting, Risk Management/Loss Prevention, and, Emergency Planning and Response. It is these domains, as well as other, that we will need for the future.

2023 will be a fantastic year for us. Aside for the foundational changes that will come to fruition this year, we will also sponsor and present our first annual IACSP Conference in September. Our conference will address the knowledge and training needs for all surveillance personnel as they face the 21st century. There will be pertinent classes based on what we need to know to be successful at our work, increase our professionalism, to successfully protect our entire property. And to prepare us all for the emerging trends and issues we will need to handle in the near future. There will also be an opportunity for those individuals who wish to sit for the CSP exam to prepare and take the during the conference We will begin issuing conference information soon.
Please join us in September. Additionally, if you want to speak or contribute in any way, please let us know!

Looking forward to great year! Derk

Inside this issue

Save the Date

The IACSP is happy to announce

The Casino Resort Protection Conference

September 12-14, 2023

Location: The Westgate Las Vegas Resort and Casino

The Three "D's" of Surveillance

.....Malcolm Rutherford

In the movie Dodgeball the fictional Dodgeball All-Star Patches O'Houlihan talks about the "Five D's of Dodgeball: Dodge, Duck, Dip, Dive and Dodge", the joke being, of course that Dodge is mentioned twice.
In the Casino Surveillance field we can make an argument that there are "Three D's of Surveillance: **Deter, Detect, and Deal with**." Which at least means that I have not repeated myself with any of the topics. But what are these things really? Do we all agree with them and with their relative importance? What emphasis should each one get in the competition for resources and demands upon time?

Deter

Deter is the most overarching of the D's. The one that encompasses the greatest time frame and, to some degree, the one that is the most passive of the three, while simultaneously being the most important.
From the American Heritage Dictionary: **Deter** transitive verb

* To prevent or discourage from acting, as by means of fear or doubt.
* To prevent or discourage (an action or behaviour).
* To make less likely or prevent from happening.

The ultimate aim of any surveillance or security system is to deter activity, typically criminal activity. You do not want clients, or patrons, or staff to believe that they can steal from you, defraud you in any way, of collude with other to achieve one of these outcomes.

I used to phrase it as follows, everyone who aims to steal from, or defraud an organisation has a risk/reward scenario built up in their head. While the balance of the risks willing to be undertaken against the potential reward to be gained varies between individuals such a determination is, I believe, always there. My job, and the jobs of the teams I recruited and managed was to alter the perceived balance of that model: to raise the perceived risk of being caught, with all of the negative connotations that this gives rise to, while lowering the potential rewards available.

As an aside this also implies that the risks should be real risks. Not just the loss of employment, but the potential for law enforcement involvement. Back when I started in the Casino business I know of a couple of cases where staff caught stealing were just allowed to resign because the operation did not want "bad publicity". This was, in my opinion, counterproductive since it sent the message that stealing from us only generated a "slap on the wrist" and that the criminal was able to simply move on without sanction to perpetrate their crimes elsewhere.

So, this said, how do we deter crime and criminal actors at our properties?

Solid, well written policies and procedures are an excellent start.

If you design these well then the **only** way left for people to defraud or steal is to circumvent what they should be doing and this provides a tell that we will deal with in **Detect** below. Also, there is no real reason that policies and procedures need be written so as to be so onerous, or complicated to carry out that people instinctively try to circumvent them. They can be written to keep the Games and Cage, F&B and Slots opera-

tions flowing smoothly, while also being secure. This is an area where knowledgeable stakeholders, who will have to be involved in the day-to-day running of their departments, and thus dealing with the practicality of the procedures developed, should be involved in their drafting.

Once you have the policies and procedures in place make sure that people know them and make sure that staff adhere to them. As alluded to above one of the best "tells" that something is suspicious is when policies and procedures are not being followed by people who should know better.

Enforcing policies and procedures closes loopholes for staff to work on their own account, or in collusion with Player Agents to defraud the system, enhancing security.

Make sure that Staff and Patrons know that they are being watched. At least potentially so. And that discrepancies will be investigated thoroughly. This is where "active" Surveillance comes in, although when I use the term I use it from a primarily data-driven perspective where resources are concentrated in areas that seem to have an issue or problem, not in random patrols of the Gaming Floor, hoping to stumble across something.

With the real dangers to operational profitability out of the way; Staff and Staff/Patron collusion, what is left is outside theft, which is usually much harder to pull off and much less lucrative. Where it is not you can, almost inevitably, trace the root cause back to a failure of policy and procedure. I cannot stress enough that this is, first and always, your major deterrent.

..continued on pages 4-5

MARK YOUR CALENDAR!

World Game Protection Conference	March 7-9, 2023	Tropicana Las Vegas 3801 Las Vegas Blvd S Las Vegas, NV
ISC West 2023	March 28 –31, 2023	The Venetian Expo 201 Sands Ave Las Vegas, NV
Global Table Game/ Game Protection Conference	April 24—27, 2023	Sahara Las Vegas 2535 S Las Vegas Blvd Las Vegas, NV

Detect

verb (used with object)

* to discover or catch (a person) in the performance of some act: *to detect someone cheating.*
* to discover the existence of: *to detect the odour of gas.*
* to find out the true character or activity of: *to detect a spy.*

As mentioned above, one of the easiest ways to detect issues such as fraud, theft and collusion is to watch for the patterns of activities that they have to make to bypass policies and procedures.

Sometimes these procedural violations stand out between peers, because the activities and processes undertaken by the would-be thief have to, naturally, differ from the activities of the honest employee. This is where the likes of exception based reporting come into play. As a colleague of mine in wont to say "the thief has to cash out", what we can infer from this is that anyone who wishes to commit fraud, or theft, has to obtain financial instruments (most typically cash or chips, or even TITO vouchers) and then has to turn them into cash if they are not that already. They then have to get away with this cash.

Every step in the process gives an opportunity for the Surveillance department to detect part of the transaction, and to **deal with** it, which is the next step in the process.

There may be attempts made to obscure the trail of funds, but this leads to the problem of each link in the chain is another opportunity for surveillance to detected the activity and ultimately to thwart it. But this is an area which absolutely demands the ability and willingness, on the part of Surveillance, to analyse the data.

If the reliance is on "active patrols" then only the simplest of thefts will be detected. You might stumble upon someone taking money from a cash drawer and putting it in their pocket; or someone dropping a cash chip on the floor and placing it in their shoe, but little that is more sophisticated than this will be "witnessed live".

No, the requirement here has to be to utilise all possible data analytics tools, and therefore all possible associated data, to build up a picture of what is going on. Indeed, in my experience it has often been the case that until you have a working, if tentative, hypothesis of what is being done it is difficult to decide what you need to watch on the camera. Only when you have a clearer picture of the steps that the suspected fraudster is taking can you determine when elements of the theft are even visible.

Surveillance department should have access to all the data systems the Casino generates and as many analytical tools as are available, as well as training in how to undertake data analysis and how to use the tools obtained. Only then will they be capable of undertaking the detection of the more complex, and thus more lucrative, frauds and thefts perpetrated against their operation.

Deal With

Not being a single word **deal with** is slightly different when it come to a definition. However, we might think of deal with as:
verb

* to handle verbally or in some form of artistic expression; to address or discuss as a subject.
* to take action with respect to (someone or something).
* to consider, as an example.

Here, as you might imagine I am going to concentrate on the second definition listed above. A major factor in any plan of **deterrence** is that one you have **detected** wrongdoing you act swiftly, decisively and without fear or favour to **deal with** the perpetrators and the overall situation.

So, what could be meant by this, somewhat ambiguous phrase?

Well, clearly what I do not mean here is to "deal with" in the same manner as used to happen to people who ended up on the wrong side of the Casino Management and Owners back when the Mob ran Las Vegas for example. Here, being dealt with might see you stuffed in an oil drum and dumped in Lake Mead, only to re-surface in 2022, when the lake levels dropped far enough to expose your final resting place. While satisfying as a flight of fancy we live in a Corporate world now, thank goodness, and there should be rules for dealing with almost any eventuality.

Indeed, this is another area where firm policies and procedures will reap dividends. Staff, in my experience, crave consistency in the application of policies and in the rewards and punishments that Operational Management are authorised to hand out. There is little more detrimental to staff moral than seeing "one rule for them and one rule for us." Humans, actually most animals in general, have an intrinsic conception of "fairness", and even fairly draconian solutions will be accepted if they are perceived to be both fair and applied even handedly.

Therefore, the Company should have a clearly stated policy as to what they will do if someone is detected stealing from them, or committing fraud against them. This should be widely promulgated to staff, so that they are all aware of it and so that no one can later plead ignorance; it should include an initial assumption of innocence, but investigations should be carried out in an unbiased manner and without regard to who the individual being investigated is, and who he or she might be related to. This can be difficult in certain times, locations and situations. But as an aim, at the least, it should be maintained.

If the evidence of some form of malfeasance is deemed sufficient then the previously decided upon sanctions, as detailed in the Company policies and procedures, should be followed. Whether this would require termination, or the involvement of law enforcement, of some civil penalty.

I also consider it very important, for the benefit of **deterrence** that these outcomes should be publicised widely within the organisation, if not necessarily, outside of it. There is often a temptation to keep things secret when "clearing house", a desire "not to air dirty laundry in public", But this can be damaging to an organisation when staff, who may be, at least vaguely, aware of what has been going on are then left in ignorance of the outcome. Clear, decisive outcomes are always better that obscure, unclear ones. In addition knowing that they will be dealt with openly and fairly will reassure innocent employees while deterring those who might, in other circumstances, be willing to "take a chance" with fraud or theft.

So, these are, for me the major planks on which a Surveillance department can operate in a modern Casino environment.

In addition, while I have concentrated on fraud and theft in these descriptions, as a model it works equally well if we substitute **anti AML** or **Responsible Gaming** for **fraud and theft**. In each case you would like to **deter** those who may wish to circumvent legal requirements for the operation, whether that would be through laundering money, or coming back in the Casino to play after self-excluding themselves. You would aim to **detect** those who have not been sufficiently deterred and who have tried to gamble when they should not, or launder money or the proceeds of crime. Then, once you have detected these individuals, or groups of individuals, you want to **deal with** them, in line with the policies and procedures that you have decided upon.

Which States Will Legalize Sports Wagering In 2023?

Three states — Kansas, Maine, and Massachusetts — legalized sports betting in 2022. Those three additions leave 16 U.S. states without legal sports betting platforms.

Among those 16 are states with massive populations that hold the attention of sports betting operators, including California, Florida, and Texas. While legal sports wagering in those states doesn't appear imminent, they could make progress in 2023, and a few other jurisdictions appear poised to legalize this year.

Let's take a closer look at the states that could legalize sports betting, or expand to include mobile wagering, in 2023

Most likely to legalize in 2023

Georgia: No. 1 University of Georgia plays for the College Football Playoff title Monday, but fans won't be able to legally wager on the game inside Georgia state lines. Could that change in the future?

North Carolina: North Carolina is toward the top of the list of states most likely to legalize mobile sports betting in 2023, given the state's close call in 2022. Retail sports betting is allowed in North Carolina at a pair of tribal casinos.

Minnesota: With 11 gaming tribes in the state, Minnesota's path to legalization will run right through Indian Country. For the first time, the tribes in 2022 got behind a House bill that would have given them exclusivity, but they pulled their support when the Senate stripped that out of the bill.

Vermont: The study group created in 2022 offered up a paper to lawmakers in September that outlines what a wagering framework would look like in the state, which, after Massachusetts legalized in August, is the only non-legal state in New England. No bills have been filed yet, but it appears lawmakers are educating themselves.

Casino Gaming by the Numbers

AMERICAN GAMING ASSOCIATION

Do you Know….

$261 **billion** Annual Economic Impact	$41 **billion** In Tax Revenue Generated Annually Impact	44 **States** With legal Casino Gaming	1.8 **million** Jobs Supported by U.S. Gaming Industry

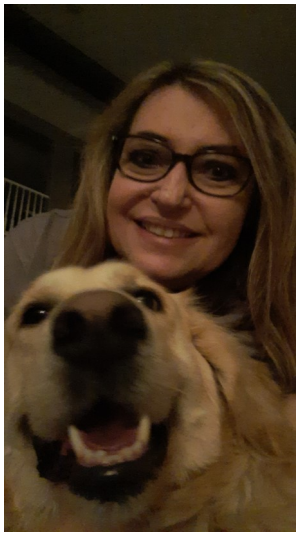
Stephanie Wallace

Vice President of Surveillance
Wynn | Encore Las Vegas

MEET OUR BOARD OF DIRECTORS

Stephanie is currently the Vice President of Surveillance for the Wynn|Encore Las Vegas.

Stephanie started her gaming career in 1994, with the opening of ITT Sheraton in Mississippi. She moved to Las Vegas in 1997, where she started working at the Stratosphere. While at the Strat, which became ACEP, llc., she worked her way up to the Corporate Director of Surveillance where she had oversight to 4 properties including Las Vegas and Laughlin, NV.



In June, 2008 she accepted a position with Wynn|Encore Las Vegas where she continues her career as the Vice President of Surveillance. Since working at Wynn, she has been the driving factor for the system upgrade from analog to full digital, changing from one VMS to another without downtime and includes a 7400+ camera network. She has also assisted in the Surveillance design and opening of Encore Boston Harbor, and provided guidance, project management and Surveillance standards for numerous property construction projects in and out of the country.

Information Resources

http://www.indiangaming.org/	https://www.americangaming.org	https://ggbmagazine.com
https://www.globalgamingwomen.org	https://www.globalgamingexpo.com	https://news.worldcasinodirectory.com
https://globaltablegamesprotection.com	https://www.worldgameprotection.com	https://www.asisonline.org
https://iacsp.org	https://www.acfe.com	https://www.discoverisc.com/west/en-us.html
https://www.securitymagazine.com	https://www.fincen.gov	https://www.dhs.gov

Global Gaming Women

National Indian Gaming Association

ASIS INTERNATIONAL

Crystal Ball Gazing, what will change in casino surveillance over the next 10 years?

Where do I think we will go in the next 10 years? It is my firm belief that the next 10 years will be the decade of AI (Artificial Intelligence) for the industry. Video analytics are nothing new in Surveillance, we've had analytics at some level for the last 20 years but now the processing power of the camera and the software that resides on the cameras and other equipment are at a level that they can perform a large part of the investigator's job automatically. More and more casinos are shifting from a live monitoring Posture to a forensic investigation posture.

What I mean by this is in the past we would have the majority of our investigators performing live monitoring on a casino operation and they would only have one or maybe two investigators actually doing reviews and performing reports after the fact. Now it is basically the opposite, currently live monitoring only consists of one or two operators and the rest of the staff is doing post incident investigations this is a side effect of our improved data collection ability. As we have more devices in the filed collecting data for us automatically, this trend will continue and at some point, I see live monitoring only being used during the course of an active incident.

Regarding analytics, currently object recognition is being used within cameras to tag and classify objects within the camera view, such as a car, a person or a bus and the color of those objects. That classification data is stored as META Data within the video stream and that META Data can be searched as stored video. An example is that we no longer need to search only on camera, time, and date but now we can search for a person in the red shirt on all cameras. This dramatically reduces the workload for the investigator and can provide additional information such as an individual's known associates quickly, and many times as the innocent is still unfolding.

This technology is available now but is still being adopted in the industry. In the next ten years this will be commonplace as the cost of the technology comes down. Currently this "Object Classification" is accomplished by what is known as "Machine Vision". This is accomplished by scanning individual snapshots of video as they are being captured by the camera. As this technology matures, we will be able to identify and classify more objects. Instead of just people and vehicles, but weapons, smoke, and other items that we would want to bring to a human's attention. The big improvement that I see in the next ten years is that this technology will be able to identify objects in relation to other objects and compare to neighboring frames. So instead of just identifying a handgun, is the handgun in a holster or in someone hand? Did the patron slip and fall or just pick up something off the ground that they dropped? If a person is captured running inside the casino, provide a ten second clip just before the person started running. These are only a few examples that I foresee becoming commonplace within the next ten years.

Game protection will also benefit from the advancement of AI. Currently there are analytics that can recognize the pips on cards to identify win/loss per hand and even record the pace of the game. In the future we will see player betting patters being incorporated, identifying advantaged players automatically and possibly even automatically rating the individual's play

and linking that to facial recognition.

As IOT (Internet of Things) devices become more intelligent, I see an opportunity for Surveillance departments to be the custodian of all this data. Not just video but license plate data, access control data, facial recognition data, real time information sharing with local law enforcement and emergency services, and the list goes on. All of this data will help Surveillance Departments become more efficient, protecting guests, employees and assets faster with more accuracy. This might sound a ton of additional work, but do we really want to trust other departments with this vital data? With this technology advancement, we need to evolve our technical staff as well. Changing the traditional Surveillance Technician that installs cameras and maintains recorders, to Surveillance Systems Engineers that manage and administrate all the intelligent data being received by our IOT devices. I honestly believe the days of deferring to the IT department are over, we need to develop this expertise within the Surveillance Department. I foresee this being commonplace within the next ten years, so we need to start planning and developing our teams now.

Looking back about 10 years ago I gave a presentation at the Global Gaming Exhibition (G2E) in Las Vegas on this very topic. At that time my look forward was the following.

We will have modular cameras that can be inserted into locations that we previously never thought of such as gaming tables, ticket redemption machines, slot machines and basically anyplace your imagination can think of. We will have Vehicle license plate and facial recognition systems that are far more accurate than we had in the past. These systems will not only link offender information but valued player information, identifying desired patrons and making the staff aware of these patrons so a higher level of guest service can be rendered. These systems will feed a database where desired and undesired patrons Activity can be reconciled against players club accounts Again reducing fraud and increasing the guest experience. Facial recognition and LPR are part of a larger topic discussed 10 years ago, Big Data and The Internet of Things (IOT). IP cameras and other devices will not only capture video for recording but collect multiple data points for storage. That "firehose" of data will cumbersome and costly to store but highly beneficial for post incident investigations. Lastly, the connectivity of the IOT environment will allow surveillance rooms to be consolidated. Multiple casinos can be monitored from one location and even allow surveillance investigators to work at home if allowed by regulatory agencies.

10 years later most of these predictions have come to pass and even the remote monitoring of casinos has been allowed by some select jurisdictions during the pandemic. If the pandemic has taught us nothing else, it is that we must be agile and have the ability to adapt to the ever-changing business landscape quickly whether it be a public health crisis or civil unrest we must be able to adapt quickly.

As with all new technology, the two things that will hold us back is cost and regulations. One thing that has always been constant with technology is the cost will go down as the technology matures. Regulations on the other hand have not done very well in keeping up with new technology. Many regulations across the country are still based in analog technology, even naming quads and multiplexers by name. We as an industry should be pressing regulators to modify regulations accordingly and bring them up to date. It is my believe that this pressure should come from Casino operators and organizations such as IACSP, not driven by vendors. This requires us to get involved because at the end of the day the future will be what we make it to be.

Robert Prady CPP PSP CSP, is currently the Area Technical Manager (West) for Axis Communications. He is an IACSP Board member, a long-time volunteer leader for ASIS International and has been active within the casino gaming industry since 1993.

Surveillance Case Study

Restaurant Managers and Supervisors Fired for Allowing a Huge Fraud to Operate Under Their Leadership
In this case a restaurant located in a casino loses tens of thousands of dollars for years due to massive employee theft and poor oversight.
Case Type: Internal Theft and Fraud
Case Outcome: Restaurant Manager and supervisors terminated. Line employees were left in place dure to reputational concerns. Accounting/Audit departments required to improve their monitoring and audit process.
Loss Amount: Estimated loss of over $90,000.
Detected by: Surveillance department through routine video
audit.

What Happened?
During an assigned audit of the gaming resorts 24-hour coffee shop, a surveillance investigator observed a waiter entering a transaction into the register that looked odd. The waiter used a key called "service recovery" that apparently comped the meal off. The waiter was then observed to put cash of an unknown amount directly into his pocket. Upon review of the suspicious transaction by senior surveillance personnel, the observation was deemed highly suspicious and a Close Watch assigned.
The Close Watch soon revealed that the "service recovery" key was being used by almost all of the wait staff, as well as supervisors to comp off cash paying customers. Once comped off the cash was, of course, taken as a toke. As cash paying customers were approximately forty percent of the customer base, this fraud was costing the restaurant a considerable amount of their daily receipts. Initial investigation determined that the service recovery key was to be used only by a manager or supervisor in the event of a customer dispute, service breakdown, or the customer complained about the food itself

The Investigation:
Surveillance used various methods to gather the evidence necessary to present the case to senior management. First, at least one investigator was assigned to monitor the activity within the restaurant at all times, with the primary focus being on the use of the key. Secondly, surveillance investigators and/or their family members went undercover to eat at the restaurant and left cash on the table to pay for the meal. This was done to address the potential claim by the waiter that the customer had complained about their meal or service, and the meal was comped for that reason.
Additionally, surveillance met with the general manager and the CFO to report what was found and to determine how it had occurred. Regrettably, we found that the service recovery key had been placed at the points of sale in the restaurant to allow managers (only) to comp meals in the event of bad service or the guest did

not like the food. The key was to be removed at least two years prior as the restaurant developed another way to correct service issues. However, the key was not removed and the managers and wait staff soon realized that they use the key to augment their tokes, and they did so.

Further, no one from the finance team followed to ensure the key was removed as directed, nor did they track or audit its continued use which did show in the receipts and other analytics. Moreover, the massive reduction in the cash received from customers on a daily basis was not noticed by Finance or the Director of Food and Beverage though this is a common report issued daily to assist in the detection of theft.

Investigation Results:

The restaurant manager and supervisors were terminated. No one was arrested, although, a prosecutable case for theft/fraud could have been submitted against every waiter and their supervisors and managers. However, due to the reputational concerns for a casino property in a small town where everyone knew everybody else, that route was not taken.

Changes were made to the restaurant operations and the service key was removed. Finance began reviewing key transactions information from the points of sale.

Remarkably, the restaurant's profits improved almost immediately. The thefts had occurred over a two-year period and base on the number of times the service key was used in that time, a near $100K loss is a reasonable estimate.

Key Takeaways:

The detection of the theft in the restaurant was made by using a surveillance audit of the area. The investigator "followed the money" by watching transactions from start to finish. Surveillance audits are one of the most effective tools in the surveillance tool belt and should be used as often as possible in all areas of the gaming resort.

Notable in this case was that although the information necessary to detect the massive theft in its earliest stages was available, none of the persons or departments responsible did so This is a common issue in many casinos, where too often, the individuals who should review the "numbers" on a regular basis, do not do so or are not trained to do so. Surveillance departments must not count on other departments reporting indicators of issues. This is a rare event and should not be part of the surveillance plan of operations.

Surveillance personnel should always bear in mind that the areas outside the casino (such as Food and Beverage) have value also that can be by employees. This fraud occurred over two years, a common period of time for a fraud to continue prior to detection. Don't spend all of your time and resources in the casino looking for cheats and advantage players. Have a plan for checking all areas and departments for theft and fraud on a regular basis. You won't be disappointed.

IACSP.org
International Association of Certified Surveillance Professionals

More details to come…

Casino Resort Protection Conference
September 12 -14, 2023
Westgate Las Vegas Resort & Casino

Poker Players Call Out Mike Postle After He Resurfaces at Beau Rivage

Mike Postle, the man accused of cheating on the now infamous Stones Live streams, has resurfaced more than two years after allegations of foul play first emerged.

As we've seen in the past, accused wrongdoers, such as Howard Lederer, Annie Duke, and Ali Imsirovic, always find their way back to a poker table. Postle's comeback happened this week at Beau Rivage Resort & Casino in Biloxi, Mississippi.

The casino's Million Dollar Heater series ran from Jan. 5 to 16, and Postle was one of those taking part in the $1,200 main event. American poker player Maxwell Young was the first person to spot him. He informed fellow pro Angela Jordison, who made it her duty to tell the poker community.

Without eagle-eyed Young spotting Postle, we may have never known about his return to live poker.

As per Jordison's tweet, he was allowed to register for the tournament using his first name (Michael) and middle name (Lawrence). Whether or not it was an attempt to avoid detection, Postle's identity was outed on Twitter.

New York Senator Wants Big Apple Casinos Licensed This Year

A New York lawmaker is pushing for full casinos to be licensed in the New York City area this year.

Sen. Joseph Addabbo, D-Queens, told Gambling.com he doesn't want the licensing process for three Las Vegas-style casinos in the metropolitan area to "linger." Addabbo is chairman of the state Senate Committee on Racing, Gaming and Wagering.

Any delay in licensing New York City-area casinos will cost the state needed tax revenue and postpone job creation, he said.

"I want this to hit in 2023," Addabbo said

Alvin Chau, Fallen Suncity 'Junket King' Gets 18 Years in Prison

Alvin Chau, once one of the most powerful men in Macau's gambling industry, was sentenced to 18 years in prison on Wednesday for 162 charges of fraud, illegal gambling, and criminal association.

As chairman and CEO of now-defunct Macau mega-junket Suncity, the playboy businessman was once responsible for an estimated 25% of VIP market revenue in the world's biggest gambling hub. In 2014 that would have equated to US$11 billion.

For perspective, that beats the gaming revenue generated by the entire state of Nevada in the same year, including Las Vegas.

Prosecutors accused Chau, 48, of running illegal gambling operations that cost the Macau government HK$8.2 billion (US$1.1 billion) in tax revenue. Chau denied the charges.

$100B in Sketchy Bets

Twelve of Chau's 20 codefendants in the four-month trial — largely Suncity executives, partners, and managers — were also found guilty of similar charges and sentenced to between nine and 15 years in prison.

All defendants, including Chau, were acquitted of money laundering charges because of lack of evidence. Suncity was also accused of operating digital gambling platforms from the Philippines and Cambodia that targeted players in Macau and mainland China, where online gambling is illegal.

Chau and six other defendants were ordered to pay HK$6.5 billion (US$830 million) to the Macau government and HK$2 billion to five of the gambling hub's six major operators. They claimed they were also cheated by the operation.

Chau was arrested in Macau in late November 2021, just days after prosecutors in the city of Wenzhou in mainland China issued a shock warrant for his arrest.

Las Vegas to Welcome First Cannabis-Forward Hotel

The Artisan Hotel will become Las Vegas' first cannabis-forward property. According to a press release from its new owner, Elevations Hotels and Resorts, the 64-room nongaming hotel just off the Las Vegas Strip will undergo a multi-million-dollar renovation to become The Lexi, a resort focused on marijuana consumption. Reports indicate The Lexi will open by April.

As part of its transformation, the entire fourth floor of the hotel will be designated for smokers, with each room boasting a RestorAir filtration system. In addition, the hotel will feature a membership-only cannabis lounge on the ground floor.

Details of the monthly lounge membership have yet to be announced. The hotel won't be licensed to sell cannabis products on -site – though the Planet 13 cannabis superstore is within walking distance.

The Lexi will become the flagship property for Elevations, formerly known as the Pro Hospitality Group. The Phoenix-based company acquired the Artisan Hotel for $11.9 million last March from the Siegel Group, which bought the hotel out of foreclosure in 2010. According to the *Las Vegas Review-Journal,* Elevations invested more than $15 million to purchase and renovate the 1.3-acre property at 1501 W. Sahara Ave., just west of the Las Vegas Strip.

The Lexi will also be home to a new Cajun-inspired steakhouse from executive chef Jordan Savell, a newly designed Artisan Bar & Lounge, and the Lexi Pool, a European-style pool that encourages topless swimming.

Everything you need to know about the Year of the Rabbit

Jan. 21 will mark the end of the Year of the Tiger and the beginning of the Year of the Rabbit in the Chinese zodiac.

The Tiger meant 2022 was a fast-paced year of strength, vitality and growth. But like the animals, rabbits are much tamer in comparison to tigers. So you can expect 2023 to be a much chiller, more restful period, according to Japan Times.

What does the Year of the Rabbit mean for 2023?

The rabbit is the luckiest of the 12 animals in the Chinese zodiac. Expect this year to bring prosperity, hope and calm.

While 2022 was a yang year (meaning it was more about action), 2023 will be a yin year and much more passive. There will be moments for reflection, rest and renewal.

Rabbits are gentler, but they're also agile and cunning. So in 2023, you will be able to navigate life quickly and thoughtfully while avoiding stressors and dangers.

This softer approach may be the necessary reprieve after an action-packed 2022.

Note from the Editor

Please submit all newsletter articles and or postings to

Stephanie Wallace

stephanie.wallace@wynnlasvegas.com

- Area News
- Job Openings
- Announcements
- Articles

Tech Talk

Video Analytics

Video analytics is a technology that processes a digital video signal using a special algorithm to perform a security-related function. There are three common types of video analytics:

Fixed algorithm analytics * Artificial intelligence learning algorithms * Facial recognition systems

The first two of these try to achieve the same result. That is, they try to determine if an unwanted or suspicious behavior is occurring in the field of view of a video camera and the algorithm notifies the console operator of the finding. However, each takes a dramatically different route to get to its result. Fixed algorithm analytics use an algorithm that is designed to perform a specific task and look for a specific behavior.

Each fixed algorithm looks for a very specific behavior. The client must pay for each individual algorithm for each individual video camera in most cases.

Artificial intelligence learning algorithms operate entirely differently. Learning algorithm systems begin as a blank slate. They arrive completely dumb. After connecting to a given camera for several weeks, they begin to issue alerts and alarms. During that time period the system is learning what is normal for that camera's image during the day, night, weekday, weekend, and hour by hour. After several weeks, the system begins to issue alerts and alarms on behavior in the screen that it has not seen before or that is not consistent with what it has seen during that time period for that day of week.

An example illustrates the usefulness of this approach. In one early installation at a major international airport that was intended to spot children climbing on a baggage carousel, the system alerted on a man who picked up a small bag from the carousel and placed it inside an empty larger bag. The man was intercepted and interrogated only to discover that the luggage inside his did not belong to him and that he was part of a ring who came to the airport regularly to steal baggage in this way. The airport had no idea this was even occurring, so there was no way they could have purchased a fixed behavior algorithm for this, even if such existed (which it did not). This approach to video analytics is most useful.

The third type of analytic is facial recognition. Facial recognition systems can be used for access control or to help identify friend or foe. Facial recognition systems can also be used to further an investigation.

Typical facial recognition systems match points on a face with a sample stored in a database. If the face does not match a record, it will try to create a new record from the best image of that person available. These are capable of making real-time matches of one image against many. The latest version of facial recognition systems constructs 3-D maps of faces in real time and compares those to a truly vast database. One manufacturer claims to be able to match individuals in real time against a country-sized database of images (millions of records).

Traditional facial recognition systems require well-lit scenes and fairly static backgrounds. The latest versions are reported to work under fair to poor lighting and with dynamic backgrounds.