



CGI

Casino & Gaming International



EMPLOYEE THEFT & CRIMINAL INVESTIGATIONS: IS TECHNOLOGY, TRAINING OR DEFINING A CRIME THE ANSWER?

BY DOUGLAS L FLORENCE SR.

Fraud detection and prevention systems are becoming highly effective but there are certain aspects – including investigative techniques, interview methods and legal issues – that are reliant on what happens at a casino prior to any criminal proceedings. With the largest areas of increased criminal activity occurring in promotions, including players clubs, and in table games, the battle to stem losses remains as vital as ever.



Some straightforward questions were recently posed to me: "Is there much discussion now over how much operational knowledge can be imparted to staff or is there simply a cunning work around that can never be prevented and that will inevitably mean yet another security innovation to combat the weakness staff/players may exploit?" The scepticism for technology or digital media this suggests is further apparent: "...it would be interesting to hear about how digital media is used as evidence. But also, if there is a rise in staff theft, then what new prevention measures can be brought in? At what point is there intrusion that affects morale or is that never an issue?" These are all relevant questions that we as gaming operators should be asking ourselves.

The first and most respected resource that I turned to for continued research on this topic was the Chief of Enforcement for the Nevada Gaming Control's Division of Enforcement, Jerry Markling who is based in Las Vegas. Chief Markling has been evaluating the statistical data for employee theft and criminal investigations for over a decade now. Although, when you look at criminal matters strictly by the numbers it can be a double-edged sword. Keep in mind that in the majority of criminal cases that resulted, the Gaming Enforcement Agents who respond to these properties do so as a result of the work of the surveillance and security staff. So this call to service relies on the acts that we see before a detention or investigation is started by the gaming authorities.

Although most surveillance and security staff may be thoroughly trained on how games are dealt and played, they are typically not trained enough on good investigative techniques, interview techniques or definition of criminal elements to support that a crime has resulted and can be proven. This certainly contributed to the statistical data that

>> PROBABLY THE MOST NOTICEABLE CHANGE HOWEVER HAS BEEN IN THE DOLLAR AMOUNTS OF THE EMPLOYEE THEFTS. EMBEZZLEMENTS INVOLVING TENS AND HUNDREDS OF THOUSANDS OF DOLLARS ARE MUCH MORE COMMON THEN THEY USED TO BE; IN 2008 THE AVERAGE EMPLOYEE THEFT WAS APPROXIMATELY \$4,056, SO FAR THIS YEAR THAT AMOUNT IS OVER \$11,000 AND WHAT WE CATCH AND ARE AWARE OF IS PROBABLY ONLY A DROP IN THE BUCKET COMPARED TO WHAT IS ACTUALLY TAKEN. WE ARE ALSO SEEING A GREATER NUMBER OF SUPERVISORS, MANAGERS AND EXECUTIVES BEING INVOLVED IN THEFTS AND/OR EMBEZZLEMENTS. >>

we see here. The only thing missing is the disposition of the criminal case for comparison which I believe would show very good results knowing my past experiences while a surveillance director for two major properties where we successfully resolved employee matters and the reason my relationship with gaming regulators and law enforcement in Las Vegas was highly positive...my staff was trained on all aspects of investigations, use of digital media for forensic purposes and interviewing.

Chief Markling said that "In the last four years we have seen a 3.6 percent decrease in the total number of arrests made. However, during that same period the number of employee arrests has increased by 6.4 percent and the percentage of employee arrests to all arrests has gone from 33 percent in 2005 to 40 percent last year. So far this year the percentage is holding at around 40 percent.

The downturn in the total number of arrests can be largely attributed to the changeover to coinless slot machines. While coin operated machines still exist in some of the older locations, ticket-in ticket-out (TITO) technology has had a tremendous effect on reducing the occurrence of slot cheating. In addition, we used to find that slot cheaters were fairly resilient to technological change and were able to come up with new cheating techniques fairly quickly, but that has not been the case with TITO technology and slot cheating remains rare and sporadic.

The largest areas of increased criminal activity have been in promotions, including players clubs, and in table games. The manipulation of player ratings and/or points, have increased considerably and is an ongoing concern. We have also seen a marked increase in the number of incidents related to the increasing and decreasing of wagers after acquiring knowledge affecting the outcome of the game (Fraudulent Acts NRS 465.070).

Probably the most noticeable change however has been

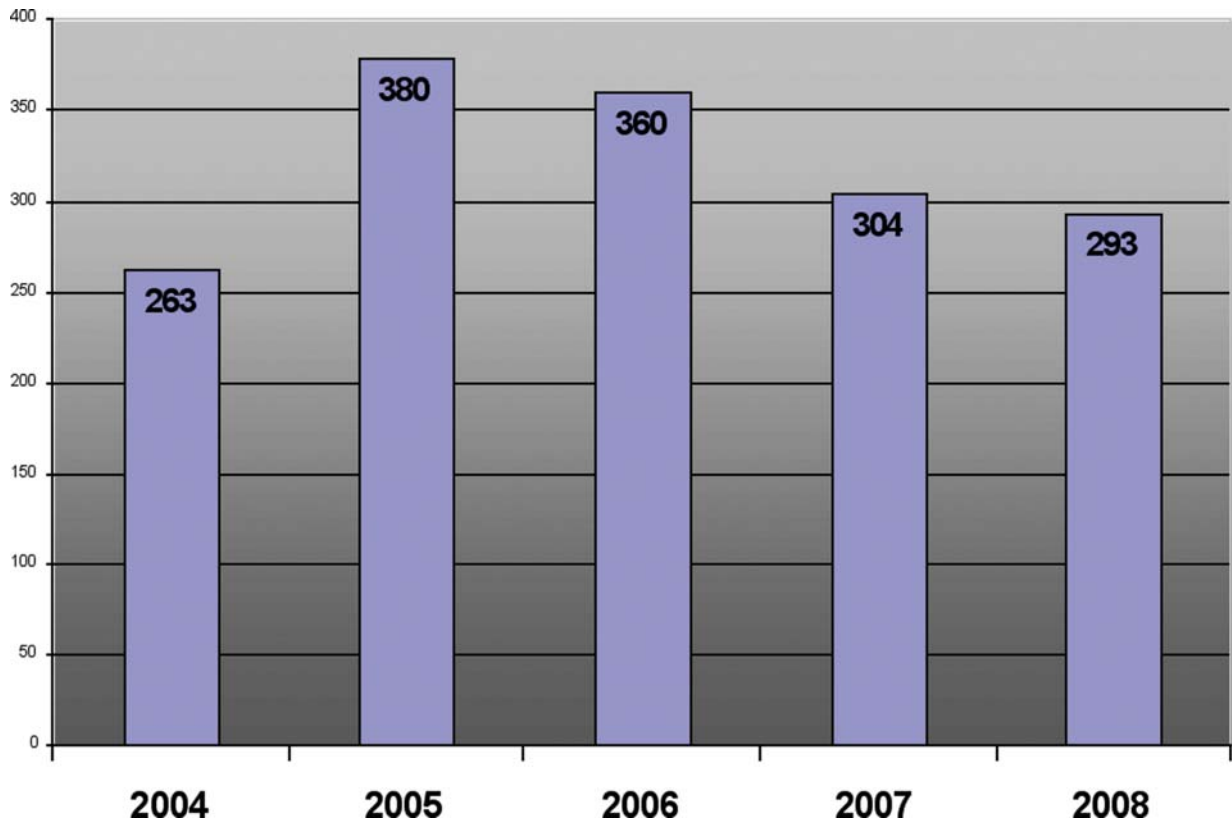
in the dollar amounts of the employee thefts. Embezzlements involving tens and hundreds of thousands of dollars are much more common then they used to be; in 2008 the average employee theft was approximately \$4,056, so far this year that amount is over \$11,000 and what we catch and are aware of is probably only a drop in the bucket compared to what is actually taken. We are also seeing a greater number of supervisors, managers and executives being involved in thefts and/or embezzlements. The bottom line is, the licensees must remain diligent in creating and maintaining strong internal controls to discourage criminal acts while at the same time continue to be proactive in their efforts to detect them."

Chief Markling put it well, the responsibility lies with the 'licensees' or gaming operators use of the internal controls and I would add the training, technology and use of these resources by surveillance and security must be expected. Gaming regulatory agencies typically respond to service and even in those instances where State Gaming Authorities have personnel on property that even they are limited in what they can discover which leaves the responsibility on the licensee or operator. Regardless of the findings Chief Markling should be applauded for his diligence in this area and the professionalism of his team of agents, in my experiences they work with us versus against us...we are all really in the same business to protect the interests of the public and our properties.

Other questions arose: "...Presumably you can explain how the changes in technology over decades have eliminated different types of successful/attempted fraud or theft. Although, with every problem solved, a couple more tend to emerge. As far as players are concerned, isn't the best defence against adverse player behaviour a matter of knowing almost literally everything about an individual, but thereby risking infringement of his or her rights and liberties?"

AREA	2005	%	2006	%	2007	%	2008	%
SLOTS	28	23%	24	21%	26	24%	17	15%
CAGE	24	19%	20	18%	18	17%	26	22%
TABLE GAMES	38	30%	31	27%	25	23%	29	25%
PROMOTION	9	7%	11	10%	8	7%	15	13%
COUNTER GAMES	17	13%	15	13%	19	17%	14	12%
OTHER	10	8%	13	11%	13	12%	15	13%
TOTAL EMPLOYEE ARRESTS	126	100%	114	100%	109	100%	116	100%
Total employee arrests as a % of total arrests	380	33%	360	32%	304	36%	293	40%

The chart above outlines employee criminal arrests by area of work in the casino or gaming operations. It is obvious that Table Games is in the lead followed by the Cage areas, Slots with Promotions showing the most significant increase for 2008.



The chart above shows the trend of criminal arrest matters over a 5 year period that indicates that criminal gaming related arrests has gone down since 2005 by close to 23% so we have to ask ourselves why?

Do biometric systems pose that possibility if not handled carefully?"

Again, these are things that we must think about and that are changed, to some degree, either by culture or geographical location. So how technology or information is gained and used can vary, but the end result protects the interests of the public and property. Fraud is and will continue to be a large contributor to losses either by scheme or criminal act. The US has Title 31 which, simply put, is knowing that the money came from legitimate sources and that transaction accountability is in place to determine whose money it is...ok, so I over simplified it: then you add the Sarbanes Oxley Act (another US-sourced responsibility) or SOX as it is called, where executives have a responsibility to know their business is legitimate, and you have the formula for technology resources to have to be applied. Given our digital formats for TITO and Server based technology on the slot and table games areas, counting machines, electronic player development tools and so on and so on.

One such technology that is being brought forward is unique: it has been adopted by some major commercial casino operations in Las Vegas and provides an identity validation and data management solution that helps protect commercial casinos and tribal enterprises from fraudulent transactions. That is also able to mitigate reputational and regulatory risks, allowing organisations to transact with confidence. While employed at one major Las Vegas Strip property I reviewed submissions to the District Attorney for Clark County of markers or 'counter checks' issued for credit play for table games that went uncollected due to fraudulent ID or information. These submissions totalled in the hundreds

of thousands of dollars, sometimes more than a million dollars in a month.

Countless times I would review a submission that the identification presented or ID was a passport or driver's license that clearly, if the document had been challenged, would have been found to be a fake ID and could have prevented loss or fraud or the name used flagged up in a private database, credit systems or law enforcement watch list. These technologies are limited today to a handful of companies such as the Veridocs® solution that validates worldwide, government-issued identifications by ensuring that all of the security features required by the issuing government are present. Our technology confirms the information contained within the identification document's magnetic-strip and/or barcode matches what is on the physical ID. Once the identification is validated, it simultaneously checks each person against internal and external watch lists as governed by internal business practices or local, state, and federal government mandates. This process takes under 10 seconds.

The solution allows casino enterprises to vet their patrons, vendors, and employees, and provides the ability to maintain a complete historical database that stores other document images in addition to the identification initially provided. These features allow different businesses and departments to share information. Offering a first line of defence in detecting fraud at the Cage, Credit, Table Games, Player's Club, Slot, and Security Departments by validating the identity of patrons and provides operational efficiencies by searching multiple watch lists simultaneously. This technology provides security the ability to verify age on the

>> WHILE EMPLOYED AT ONE MAJOR LAS VEGAS STRIP PROPERTY I REVIEWED SUBMISSIONS TO THE DISTRICT ATTORNEY FOR CLARK COUNTY OF MARKERS OR 'COUNTER CHECKS' ISSUED FOR CREDIT PLAY FOR TABLE GAMES THAT WENT UNCOLLECTED DUE TO FRAUDULENT ID OR INFORMATION. THESE SUBMISSIONS TOTALLED IN THE HUNDREDS OF THOUSANDS OF DOLLARS, SOMETIMES MORE THAN A MILLION DOLLARS IN A MONTH. >>

casino floor and assists Compliance in addressing Title 31 and other federal and gaming regulatory issues and directly interfaces with patron loyalty programmes. Human Resources can validate the identity credentials of potential employees ensuring compliance with hiring requirements set forth by government agencies and facilitates management of data files.

The system uses a document capture device that is optimised for ID-1 sized documents such as driver's licenses, green cards and certain military IDs. The document library used in the authentication processes should contain as many as 1,700 of the known documents. That can consist of passport and card-sized documents and should be read front and back of ID simultaneously. These technologies uses White UV-A, UV-B, Near Infrared, Coaxial light, are high resolution of 400-600 dpi, automated document feed for speed and capable of reading all levels of government-issued ID types of 1D, 2D bar codes, magnetic stripes and provide USB2 interface for plug and play ease of use.

I can only imagine how effective these would have been in detecting the fraud I saw at my property on the Las Vegas Strip, making the investment worthwhile to consider and knowing the amount of money written off each year by casinos worldwide. Not to forget our responsibility to keep dishonest people from working in and supporting gaming operations.

Another technology that has been used for almost a decade now is facial recognition. The primary provider today is Biometrica which has helped some casinos. I spoke with Jim Pepin a Vice President of the company to relay a common story that he has seen result from use of facial recognition. He told me about one very interesting incident involving a group of patrons who were hitting virtually all the casinos in Aruba on their 'Three Card Poker'. One of the casinos targeted had sent out an alert from the Biometrica system asking for help in identifying a couple of people who were just suspects at possible card marking. A few minutes after seeing the alert, Biometrica staff responded with a SIN response alert reply providing the name and identification of the key person in their photos and that the person was indeed already known to be a card marker.

The Aruba Casino followed up with another SIN Alert a couple days later, this one thanking Biometrica with our very prompt and helpful response to their request. There were three in the group and all were detained at the airport now that they knew the name(s) and when they were trying to flee to Venezuela after their spree when they felt the heat. The casino also learned from another Biometrica casino client that these same individuals were known to have done the same thing previously at a casino in St Kitts.

Facial recognition is only as good as the data that is

provided and can, when used properly, provide gaming surveillance operations vital information on known cheaters and scams throughout the world. The caution lies in the need to protect the information and to follow laws that apply in the country that your gaming operations are being conducted. There is a resource available that can provide the legal department or compliance department of your gaming operations with vital information on gaming laws and regulations: this is the International Masters of Gaming Law (IMGL), an association of gaming attorneys, regulators, in-house counsel, consultants, and educators.

In conclusion, it is becoming obvious that more technology is being used today to detect and thwart fraud and criminal acts in our casino operations. With the future of Table Games using server based technologies to observe and document each hand or game played by a patron, the consideration of security and surveillance to use these resources to improve game integrity and game protection is apparent as well.

Gaming Regulatory Agencies can do only so much, the rest is up to us as operators to adopt the technology tools that are being developed and to raise the level of expectation in the security and surveillance operations in order to improve the resolution of criminal matters and to avoid potential litigation that would result from a wrongful accusation or case lost in a court of law. **CGI**

DOUGLAS L FLORENCE SR.



Douglas L Florence Sr., CPP Director, Gaming Sector for NiceVision, is a Surveillance and Security subject matter executive with over thirty years comprehensive security experience involving security management, surveillance, investigations, systems integration and consulting. Designated a CPP and 'Board Certified in Security Management' by ASIS International, he also serves as the VP of Affiliate Member for the International Masters of Gaming Law (IMGL); He was also formerly a Director of Surveillance for The Mirage and for the Rio Suite Hotel & Casinos. To reach the IMGL: www.gaminglawmasters.com that has many links and important information impacting gaming law available on this website. Email: douglas.florence@nice.com