Contact Us: contactus@nigc.gov

July 13, 2023

Phone Scams at Tribal Gaming Operations

Washington, D.C. – The National Indian Gaming Commission (NIGC) is alerting tribes, tribal gaming regulatory authorities (TGRAs), and tribal gaming operations of several nationwide impostor scams involving individuals claiming to be vendors, state, or tribal officials. We are urging tribes to report the calls immediately to tribal or local law enforcement, the local FBI office, and the U.S. Secret Service. These agencies can detect patterns of fraud from the information collected and share it with other law enforcement agencies. We urge tribal officials to ensure that persons working in the tribal gaming operations, such as cage, vault or accounting staff, who have direct access to cash assets or bank accounts are made aware of the scam and know what to do in the event of such a call or other communication. We also ask that you report these incidents to the NIGC Region Offices so that the information can be shared with other tribes through updated alerts, trainings, and other communications.

Recently, there have been multiple instances of scams at commercial and tribal gaming operations with losses in the hundreds of thousands of dollars. The NIGC has been made aware of several failed attempts as well.

During these calls, scammers attempt to collect a cash payment or facilitate a cash deposit under the pretense of a false "emergency," such as a past due payment, a stalled delivery of goods or services, immediate need for transfer of funds, or other pressing event that, if not immediately addressed, will result in "dire" consequences to the operation, the tribe, or the other party. The scammer then tells the victim that the alleged dire consequences can be avoided by taking cash and transferring it to another party or entity, while they remain on the phone with the victim until the transfer or deposit is made. The transfer of the cash may take the form of a hand-delivery to an individual with whom the victim is directed to meet (usually off-site), by depositing the cash into Bitcoin deposit kiosks, or by a wire transfer of funds from one bank account to another. These are but a few examples of known cases, and scammers may attempt to use other means to get the victim to illegally transfer the cash or funds.

The following is a recent example of a reported scam: Someone impersonating a tribal official called the victim working in the vault, stating that a payment must be made immediately to ensure that a vital shipment of equipment is made. The victim was told to remove a specific amount of cash (i.e., $100,000, or more in some instances) from the vault. The victim was then directed to use their personal cell phone to remain on the line with the scammer. The victim was directed to drive, while on the phone, to a location(s) where the money was

to be deposited into a Bitcoin deposit kiosk (a victim may be directed to use multiple Bitcoin kiosks within the area). The victim was then instructed to send the QR code scanned at the Bitcoin deposit kiosks.

These social engineering scams utilize perceived authority, fear, and urgency to manipulate employees into breaking internal controls. The scammers may sound and appear credible, often pretending to be a named casino manager, a gaming regulator, a vendor, a tribal official, and/or some other person of authority to whom the victim may feel obligated to listen. The scammer may provide the victim with what appears to be first-hand knowledge of the operation and procedures, and if initially questioned, the scammer may push back and intimidate the victim with fear of job loss or some other imminent legal action. The scammers may enhance their credibility through the use of spoofed phone numbers that appear on caller IDs, as if they are calling from a business, a government agency, a manager's phone, or another phone number familiar to the victim. The call may come after normal business hours (e.g., between 5:00 PM and 8:00 AM), when most officials or top managers have already left for the day or there is a reduced number of gaming operations staff with whom the victim can confer.

Scammers' Methods:

- **Scammers pretend to be someone of authority.** They use social engineering to learn about your business. Scammers will seem believable by pretending to be a known vendor, a customer or company, a government agency, a tribal official, or other individuals in positions of authority.

- **Scammers will create urgency.** They will rush you into making a quick decision, creating a sense of urgency and trying to persuade you to not follow internal controls or approval process, or other verification procedures. Scammers will likely keep you on the phone or remain in contact with you to prevent you from searching for proper verification.

- **Scammers may use intimidation and fear.** Scammers will tell you that something terrible is about to happen if they do not receive payment immediately. They may tell you that the casino's electricity or slot accounting system will be disconnected or that you may be fired if you do not execute the payment immediately. Scammers may blame you for a past alleged error, and try to convince you that this is a way to correct the alleged error without anyone finding out.

- **Scammers use untraceable payment methods.** Scammers often want payment through peer-to-peer payments, Bitcoin, wire transfers, reloadable cards, gift cards, or cash. These are methods that are nearly impossible to reverse or track.

Helpful tips:

- Train staff with access to cash and financial accounts to be aware of these and other similar scams.

- Ensure that approved internal controls, policies, and procedures are up-to-date and provide protection of casino assets.

- Remind staff to follow the approved internal controls for movement of cash, transfer of funds, or payment of outstanding invoices.

- Remind staff to verify the request independently by calling or communicating directly with their supervisor or manager using the methods and means provided for in the internal controls or through established procedures.

- Train staff to be alert and understand what suspicious activities may look like with both guests and employees, and to report any such activities to a supervisor or manager. Such suspicious activities may include instances of other casino employees not following internal controls and/or policies and procedures.

- Train staff to not deviate from established controls and procedures, regardless of who is allegedly on the phone, and to be aware of any caller who demands to stay on the phone and will not hang up or end the conversation.

- Direct staff who receive such calls to immediately alert co-workers, security, surveillance, the supervisor or manager on duty, TGRA, and law enforcement.

- Train staff to consider limiting the direct transfer of external callers to sensitive areas, and instead transfer those calls to the Security Office for service.

- Report phone scams or other similar incidents (whether successful or not) to the NIGC Region Offices so that the information can be shared with other tribal facilities to raise awareness and prevent other scam attempts.

The NIGC offers technical assistance, training, audits, and other tools and resources to help identify potentially vulnerable areas and improve security and internal controls. For additional information, please email training@nigc.gov, or contact your local NIGC Region Office.

Resources

FBI Field Offices:
https://www.fbi.gov/contact-us/field-offices

U.S. Secret Service Contact:
https://www.secretservice.gov/contact/field-offices

FBI Internet Crime Complaint Center:
https://www.ic3.gov

NIGC Region Offices:
https://www.nigc.gov/compliance/regional-offices