Native American Insider

Issue #14 October 2013

Contact List

TRIBAL FIRST
INSURING NATIVE AMERICA

Through the transfer of knowledge to you, the tribal government, or enterprise, Tribal First enables you to increase your self-sufficiency in all aspects of risk management. For more information, contact:

Robert Shearer
Senior Vice President
(800) 552-8921
rshearer@tribalfirst.com

LowersRiskGroup
Protecting People, Brands, and Profits

Trust your risk mitigation needs to Lowers Risk Group, an independent, internationally recognized provider of loss prevention, investigation, and enterprise risk management (including human capital risk) services to the Casino & Gaming Industry. For more information, please contact:

Steve Yesko, ARM
VP, Business Development
(540) 338-7151
syesko@lowersriskgroup.com

GREAT AMERICAN
INSURANCE GROUP

Great American is prepared to provide the insurance protection your casino needs to guard against fraud, theft, robbery, kidnap and ransom, or computer crime. For more information, please contact:

Stephanie Hoboth
Vice President
(860) 285-0076
smhoboth@gaic.com

Hazard Communication Standards—
New Regulatory Update

Don't delay and start training your employees today! The Federal Hazard Communication Standard 29 CFR 1910.1200 has been revised to align with the United Nations Globally Harmonized System of Classification and Labeling of Chemicals (GHS). The three major areas of change are as follows and explained below:

- ☑ Hazard Classification
- ☑ Labeling
- ☑ Safety Data Sheets (SDS)

Hazard Classification

The definitions of hazard have been changed to provide specific criteria for classification of health and physical hazards, as well as classification of mixtures. These specific criteria are intended to ensure that evaluations of hazardous effects are consistent across manufacturers, and that labels and safety data sheets are more accurate.

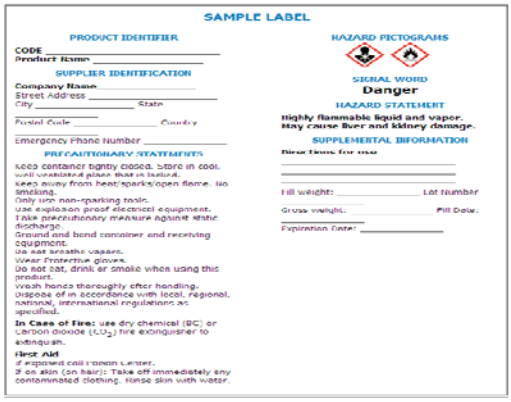
Under both the previous Hazard Communication Standard (HCS) and the revised HCS, an evaluation of chemical hazards must be performed considering the available scientific evidence concerning such hazards. Under the current HCS, parameters for the evaluation were provided, but not specific, detailed criteria.

The revised HCS has specific criteria for each health and physical hazard, along with detailed instructions for hazard evaluation and determinations as to whether mixtures or substances are covered.

Labeling

Labels will require the following elements:

- ☑ **Pictogram***:* Eight pictograms are required under the HCS.
- ☑ **Signal words***:* A single word used to indicate the severity of the hazard. "Danger" is used for the more severe hazards, while "Warning" is used for less severe hazards.
- ☑ **Hazard Statement:** Describes the nature of the hazard(s) of a chemical, including, where appropriate, the degree of hazard. For example, "Toxic if Swallowed. Flammable Liquid and Vapor."
- ☑ **Precautionary Statement:** A phrase that describes recommended measures to be taken to minimize or prevent adverse effects resulting from exposure to a hazardous chemical or improper storage or handling of a hazardous chemical. For example, "Do not taste or swallow. Keep away from heat. Use only with adequate ventilation."


SAMPLE LABEL

PRODUCT IDENTIFIER

CODE
Product Name

SUPPLIER IDENTIFICATION

Company Name
Street Address
City State
Postal Code Country
Emergency Phone Number

PRECAUTIONARY STATEMENTS

Keep container tightly closed. Store in cool, well ventilated place that is locked.
Keep away from heat/sparks/open flame. No smoking.
Only use non-sparking tools.
Use explosion proof electrical equipment.
Take precautionary measure against static discharge.
Ground and bond container and receiving equipment.
Do not breathe vapors.
Wear Protective gloves.
Do not eat, drink or smoke when using this product.
Wash hands thoroughly after handling.
Dispose of in accordance with local, regional, national, international regulations as specified.
In Case of Fire: use dry chemical (BC) or Carbon dioxide (CO_2) fire extinguisher to extinguish.
First Aid
If exposed call a poison center.
If on skin (on hair): Take off immediately any contaminated clothing. Rinse skin with water.

HAZARD PICTOGRAMS

SIGNAL WORD
Danger

HAZARD STATEMENT
Highly flammable liquid and vapor.
May cause liver and kidney damage.

SUPPLEMENTAL INFORMATION

Direct Uses for use
Fill weight: Lot Number
Gross weight: Fill Date:
Expiration Date:

Employers may choose to label workplace containers either with the same label that would be on shipped containers for the chemical under the revised rule, or with label alternatives that meet the requirements for the HCS standard.

Safety Data Sheets (SDS)

Under the new standard, Material Safety Data Sheets (MSDS) are now called Safety Data Sheets (SDS). The revised standard also requires all SDSs to have a specific 16-section format.

Continued on page 4

Inside This Issue

Who Do You Trust?

When employers hire staff, they hope to develop a relationship of trust. No matter the size, every business owner needs to delegate important tasks to a trusted employee at some point in time. Bookkeepers, office managers, controllers, vice presidents, CFOs, and other positions may all have the responsibility of maintaining bank statements, authorizing payments, or making deposits on behalf of the company. Unfortunately in business, trust can also act as a double-edged sword. It can help free up time to allow a company to grow, or it can give a dishonest employee the opportunity to steal. Temptations can be even higher in the gaming industry, due to the significant cash exposures that exist.

A bookkeeper for a popular racetrack and casino was hired for her positive employment history and accounting experience. Her duties included managing the horserace accounts, which gave her the responsibility of maintaining the money account and paying out the appropriate prize amounts. The bookkeeper came to work every morning without missing a beat. She was well liked by her co-workers and got along with her supervisors and customers. No one could have imagined that she was covering up a deep secret with her friendly smile and charming personality. After ten years of employment, she decided to retire. If it wasn't for a routine audit, no one would have ever discovered what she was able to hide.

A year after she retired, the racetrack and casino conducted an internal audit which uncovered a serious issue. A significant amount of money was missing from their account. Deposits had been forged, cash was misappropriated, and several payments were made to an unfamiliar vendor. This all traced back to one person, and one person only, the trusted bookkeeper. The internal audit revealed that the trusted bookkeeper was able to siphon $1.7 million dollars from the company's horserace account during the last seven years of her employment.

Since the bookkeeper had the sole authority of managing the horserace account, she had the opportunity to forge the deposit reports while pocketing a significant amount of money each time. She also created a fictitious business account and made unauthorized payments to this account using the horserace account. Year after year, she used her employer's funds to pay for her lavish expenses, including jewelry, cars and exotic vacations. Her employer didn't notice, her co-workers didn't notice, and her neighbors never had a clue. Even though an internal audit caught the scheme a year after she retired, the bulk of the loss could have been avoided if the racetrack and casino implemented a separation of bank account duties and utilized stronger vendor controls.

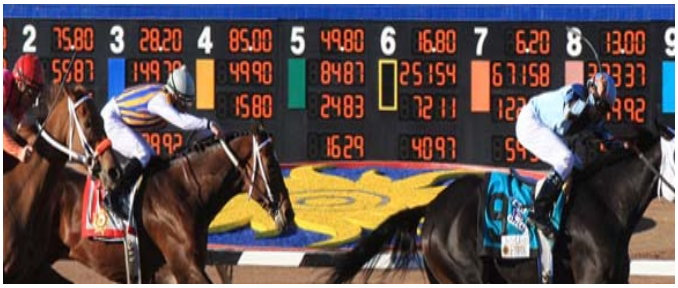
Trusting employees can be costly to all businesses. Casino operators should put their trust in their own internal controls rather than the individuals they employ. The same person should not have the ability to authorize payments, make deposits, and reconcile the bank accounts. Every banking transaction should be separated and/or cross-checked by another employee or owner. The higher the cash exposure, the higher the need for a segregation of duties.

Vendor controls are also very important. Casino operators should perform background checks on all vendors to ensure that the businesses actually exist. Vendor background checks should include verifying Employer Identification Numbers, researching how long they've been in business, and reviewing their current financial strength. Once a vendor is cleared, operators should maintain a list of approved vendors and have a separate individual verify that payments are only made to the vendors on the approved list. Simple tasks like these can make the difference between a hundred dollar mistake and a multi-million dollar loss.

A dishonest employee will always find a way to get around a regulated system, however proper internal controls can help a business minimize a large loss. If properly insured, a casino, racetrack, or other business can help protect itself from a catastrophic loss. However, it will never be able to recover the opportunity to use those funds during the time the loss occurred. Many factors affect why employees decide to steal. It could be a financial hardship, it could be an addiction, or it could simply be the fact that the opportunity presented itself. The more opportunities an employee has, the more likely an employee will be dishonest. Strict internal controls can only minimize the various opportunities, and trusting employees will always have a part in business. However, if you had to bet on employee theft, trusting your good controls will always win over trusting the individual you hire.

By Tyrone R. Bell, Account Manager
Great American Insurance Group
Fidelity / Crime Division

The above narrative is fictional; however, it is based on situations that have been reported.



Debit Card Fraud: The Movement Toward EMV Chip Card Technology in the U.S.

The United States is often viewed as a world leader in many respects; however, there are a number of areas, especially from a technology standpoint, that the U.S. lags behind much of the world in the implementation of new technologies. One of these areas that has a direct impact on the rate of identity fraud is the use of EMV chip technology in debit and credit cards.

Identity fraud affects millions of people each year. There are many factors driving the increased levels of identity theft crime to include the general nature of the criminal element, economic challenges, and advances in technology available to fraudsters, to name a few. Among the many areas of identity theft fraud, one that continues to grow in recent years is debit card fraud. According to Javelin Strategy and Research, a provider of independent research focused on the financial services and payment industries, identity fraud increased 13 percent in 2011, with more than 11.6 million adults becoming victims in the United States. Javelin's research also indicates that debit card fraud accounted for 36 percent of all payment card fraud in 2011. Javelin's more recent research indicates that identity fraud occurrence increased again in 2012, affecting 5.26 percent of adults in the U.S. as opposed to the 4.9 percent affected in 2011. The result of this increase is an additional 1 million consumers being affected, a total of 12.6 million consumers in 2012.

With the continually increasing use of debit cards as opposed to cash or checks for making payments, the opportunities for financial account information to be compromised are continually on the rise. Lost, stolen, or compromised debit cards can result in fraud detrimental to an individual's finances. (The fact that the debit card is directly linked to your checking account and that any misuse can quickly empty your account resulting in missed payments, suffering all of the related circumstances and hardships, is a concern for many individuals.)

Some instances of debit card fraud relate to lost or stolen cards. Another scenario that is becoming more and more common is when an individual becomes the victim of debit card fraud having never lost possession of their debit card. Therefore, securing your information, such as your account number and personal identification number (PIN), is as important as securing the card itself. The criminal element is daily becoming more and more sophisticated and technologically savvy. They are continually devising new ways to steal your data from ATM machines, merchant payment terminals, or from you personally via email or telephone communication.

In recent years, there has been a steady increase in the controls implemented and information required for access to financial information. Among these are requirements for more complex passwords, specific computer authentication, and the use of security questions to verify identity. Many countries outside of the United States have even started using a microchip, which is more secure than the magnetic stripe, to prevent the duplication of cards.

This microchip technology is known as EMV. EMV (a collaboration between EuroPay, MasterCard, and Visa) has created global standards for chip technology in debit and credit cards. The EMV standards define the specifications and procedures for all elements of the EMV chip payment cards and related devices, such as point of sale (POS) terminals and ATMs.

Chip cards are embedded with a microchip that has proven to be more secure than the current magnetic stripe used on most U.S. issued payment cards. The chip has the ability to store encrypted information that is used to verify the card's authenticity when it is entered into an EMV enabled device such as a POS terminal or ATM. A personal identification number (PIN) is required in what are referred to as "chip and PIN" transactions or a signature is required in what are referred to as "chip and signature" transactions. The encrypted chip and related security features make it extremely difficult to counterfeit the cards, which has been a problem with traditional magnetic stripe cards.

Identity theft is a major challenge throughout the world; however, most industrialized countries have transitioned to chip card technology in an effort to curtail the occurrence of card-present fraud. This technology has the potential to significantly decrease POS card fraud. Statistics show that other countries have seen a substantial decrease in card-present fraud since their introduction of EMV chip technology. Given that the U.S. is one of the few large economies that has not transitioned to the more secure chip technology, this fact only contributes to the focus of the fraudster on the U.S. as a target for counterfeit card fraud. With that being said, U.S.-based card issuers, financial institutions, and retailers are currently in the process of a shift to the use of chip technology in payment card transactions. Major U.S. card issuers American Express, Discover, MasterCard, and Visa have all announced EMV migration plans. In a press release dated July 30, 2013 from MasterCard and Visa, they announced plans to make "certain proprietary EMV chip technologies available to each other and other networks, enabling a debit chip transaction originating from a single chip application to be routed by the merchant to Visa, MasterCard, or any other U.S. PIN debit network that elects to participate in these same solutions," further stating that by "opening their investments and technologies

Continued on page 4

Debit Card Fraud: The Movement Toward EMV Chip Card Technology in the U.S.

Continued from page 3

to the industry, the two brands will further accelerate the U.S. to a more secure chip-enabled marketplace."

Despite the announcements and efforts being made with respect to the transition to chip card technology in the U.S., it should be noted that there are also significant logistical challenges and financial commitments that will still need to be addressed to include the following:

- ☑ Card issuers will be required to reissue debit and credit cards that contain the EMV microchip technology.
- ☑ Merchants will be required to replace POS devices with newer devices that are capable of reading the EMV cards.
- ☑ Financial institutions will be required to ensure that ATMs are capable of reading and processing EMV cards.

The U.S. also has a much greater number of card companies, financial institutions, and merchants that will be affected by this transition in comparison to the other countries that have preceded the U.S. in the transition to EMV chip technology. The financial commitment from all parties involved is substantial and has been one element contributing to the delays in the U.S. implementation of EMV.

The threat and cost of fraud will continue to be a focus of the financial and security industries. The criminal element will carry on its efforts to compromise data. However, the continued implementation of technologies such as EMV chip technology is one more step toward the global reduction in card fraud.

By Keith Gray
Director, Cash Audits
Lowers & Associates

Hazard Communication Standards— New Regulatory Update

Continued from page 1

Impact Assessment

Companies will need to take action to comply with the revised federal hazard classification, labeling, and safety data sheet requirements. Management should develop a plan to ensure compliance with these new requirements.

Actions necessary for compliance include:

Hazard communication training materials will need to be revised to address the new labeling requirements and SDS format, and subsequently staff will need to complete the revised training by **December 1, 2013**. Tribal First will be conducting a webinar that will assist TF clients in this area. The webinar will be a "Train-the-Trainer" format and will offer training materials for the tribe.

Employees must receive training on any new hazards indicated on revised SDS sheets by June 1, 2016.
Companies will need to replace all of the "older" versions of the material safety data sheets (MSDSs) with revised SDS sheets no later than June 1, 2016.

Compliance Dates

The table below summarizes the phase-in dates required under the revised Hazard Communication Standard (HCS).

Effective Completion Date	Requirement(s)	Who
12/1/2013	**Train employees on the new label elements and safety data sheet (SDS) format.**	**Employers**
6/1/2015 12/1/2015	Compliance with all modified provisions of this final rule, except: The Distributor shall not ship containers labeled by the chemical manufacturer or importer unless it is a GHS label.	Chemical manufacturers, importers, distributors, and employees
6/1/2016	Update alternative workplace labeling and hazard communication program as necessary, and provide additional employee training for newly identified physical or health hazards.	Employers
Transition Period to the effective completion dates noted above	May comply with either 29 CFR 1910.1200 (the final standard), or the current standard, or both.	Chemical manufacturers, importers, distributors, and employees

Resources

The revised HCS, along with additional supporting information, frequently asked questions, and a fact sheet can be accessed on the Federal OSHA Hazard Communication website at www.osha.gov/dsg/hazcom/index.html.

By Jean Velez, Risk Control Consultant
Tribal First, Risk Control Consulting