Operational Topic

Case studies involving radiation sources and fraud.

Case Studies of Fraud Associated with the Use of Radiation Sources: Practical Avoidance Strategies Based on Lessons Learned

R. J. Emery and D. C. Howell[1]

Abstract: *Periodically the radiation protection profession has experienced purposeful deception practices that remained undetected for some time. Upon discovery, the cases of fraud revealed gaps in confirmation or validation practices that the radiation protection community should note. Summarized here is a convenience sample of actual cases of fraud involving radiation sources along with the exploited process vulnerabilities. Recommended process improvements that the radiation safety community may consider are presented to improve the collective fidelity of radiation protection processes. Health Phys. 126:168–172; 2024*

Key words: *operational topics; radiation protection; radioactive materials; risk analysis*

INTRODUCTION

Periodically the radiation protection profession has experienced purposeful deception practices that remained undetected for some time. Upon discovery, the cases of fraud revealed gaps in confirmation or validation practices that the radiation protection community should be aware of. Because the profession relies on the transmittal of records and documents, Ferguson and Lubenau pointed out, "a major vulnerability of the process for licensing radioactive sources is its susceptibility to fraud" (Ferguson and Lubenau 2003). Further investigation indicates that the issue of fraud is not limited to sources of radioactivity but also impacts the radiation safety profession in various ways.

FRAUD BASICS, PREVALENCE, AND MANIFESTATIONS

The term "fraud" can be defined as "wrongful or criminal deception intended to result in financial or personal gain (or objective)" or "a person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities" (Black's Law 2023). Fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment" (Black's Law 2023).

In 1953, Donald Cressey, a criminologist whose research on embezzlers produced the term "trust violators" and identified the "fraud triangle," which consists of three elements: rationalization, financial or other pressures, and opportunity (Van Akkeren 2018). Based on his work, Cressey noted that a consistent rule existed, termed the 10-80-10 rule. The concept is that 10% of a population will never commit fraud, 10% will, but 80% may, given changes in the fraud triangle model.

Fraud is rampant in society and comes in many forms:

- Consumer fraud occurs when a person suffers from a financial loss involving deceptive, unfair, or false business practices;
- Identity theft occurs when thieves steal personal information, assume an identity, open credit cards, bank accounts, and charge purchases;
- Mortgage scams are aimed at distressed homeowners to get money from them;
- Credit and debit card fraud occurs when someone takes the information off a card and makes purchases;
- Fake charities and lotteries that prey on people's sympathy or greed; and
- Debt collection fraud, which tries to collect on unpaid bills whether they are yours or not (Investopedia 2023).

In occupational safety and health (OSH), fraud cases have been encountered where an employee claims a workplace injury that was, in reality, incurred outside of work. Other

The University of Texas Health Science Center at Houston Safety, Health, Environment & Risk Management 1851 Crosspoint Avenue, OCB 1.330 Houston, Texas 77054.

Robert Emery is Vice President for Safety, Health, Environment & Risk Management for the University of Texas Health Science Center at Houston and Professor of Occupational Health at the University of Texas School of Public Health. He holds master's degrees in both radiological hygiene and environmental health, and a doctorate in occupational health. His email is ***Robert.J.Emery@uth.tmc.edu****.*

examples include multiple submissions (known as "double dipping") on insurance claims, fraudulent certificates of insurance, education or certifications, and altered permits (Clayton 2023).

To address fraud specifically with regard to the use of radiation sources, we focused on reports of deception associated with all types of ionizing radiation sources (both radioactive materials and radiation-producing devices) and the services provided thereto.

Summarized here are six case reports of fake qualifications, fake or altered permits, actions and/or fake facilities or entities. Because no known central repository currently exists for these specific types of cases, the cases described here were identified through professional interactions with peers (e.g., professional listservs), sporadic news reports, web searches and government documents. It is important to note that some of the cases are yet to be settled legally or no further information is available on the disposition of the case. This effort focused on describing the fraudulent acts, alleged or otherwise, to identify vulnerabilities for prevention.

CASE STUDIES INVOLVING SOURCES OF RADIATION

Case study #1

In the early 1990s, a service company was created by an individual in Maryland who possessed a doctorate in mathematics but was not a medical doctor or licensed physician. The company was principally a mobile diagnostic medical service provider of x rays, diagnostic ultrasound tests, electrocardiograms, echocardiograms, and other medical tests. In 1993, the founder hired a radiologic technologist to provide diagnostic services.

In 1997, the founder instructed the technologist to interpret x rays, medical tests, ultrasounds and cardiologic exams in lieu of licensed radiologists and physicians. He was also instructed to draft a licensed "physician's" examination report in the name of a licensed physician, to which the founder affixed a copy of the handwritten signature of the actual physician to the report. The company routinely submitted insurance claims to Medicare and Medicaid that, among other things, exaggerated the services performed by its technologists or exceeded the services ordered by the treating physician, overcharged for transportation costs, and falsely represented that the company was properly overseen by supervising physicians. The financial loss to Medicare alone for the misconduct of ADS was in excess of $2.5 M from January 2007 through October 2012.

Once law enforcement discovered the fraud, the technologist pled guilty and received a 48-month prison sentence and 1 year of supervised release. The founder received a 10-year prison sentence, followed by 2 years of supervised release, for charges related to healthcare fraud and wire fraud conspiracy resulting in the deaths of two patients, as well as false statements and aggravated identity theft related to a scheme to defraud Medicare and Medicaid (US DOJ 2014).

This case revealed process vulnerabilities, including the absence of original source verification, the apparent absence of a random audit process, and the failure to verify that a physician was performing the work.

Case study #2

In the early 1990s, a Michigan teenager posed as a high school physics instructor and wrote several government agencies requesting information on radioactive materials required for neutron experimentation. A US DOE scientist answered his questions about alpha particle reactions, beryllium, radium, fission, chain reactions, purifying thorium, and breeder reactors. The teenager also inquired about the risks involved; the DOE scientist assumed that existing laws, insufficient technical expertise, cost, and common sense would prevent anyone from attempting this work.

The teenager would eventually acquire smoke detectors, lantern mantles, radium clocks, tritium from gun sights, and small quantities of pitchblende. He then posed as a college professor and contacted firms in the Czech Republic that sold small uranium samples. For a $140 money order, he received a marble-sized sample of uraninite, a brick of pitchblende, and UO2 containing ^{235}U and ^{238}U.

He eventually fashioned a crude neutron gun and measured appreciable radiation levels with his Geiger counter. He was arrested on August 31, 1994, on suspicion of theft. A search of his vehicle revealed a stash of duct tape, cubes of a mysterious gray powder, small metal discs, lantern mantles, mercury switches, a clock face, ores, and vacuum tubes. The teenager subsequently told the authorities about using his mother's potting shed as his nuclear laboratory. In November 1994, state officials arrived to conduct radiation surveys at her house in eastern Michigan.

In January 1995, US EPA officials visited his mother's house and surroundings to conduct their own surveys for contamination and radiation levels. In late June that year, a Superfund cleanup occurred at the mother's house at a cost of $60,000. All the radioactive waste was taken for burial in Utah.

In August 2007, the individual (now age 30) was arrested for larceny (16 stolen smoke detectors from his apartment building for the ^{241}Am sources); he was sentenced to 90 days in jail after receiving medical treatment in the psychiatric unit of Macomb County Jail (Silverstein 2004).

Process vulnerabilities exposed were the absence of original source verification and the apparent absence of random audit process.

Case study #3

In 2007, General Accounting Office (GAO) investigators posing as West Virginia businessmen obtained

a US NRC radioactive materials license within 28 days that allowed them to buy enough radioactive material from US suppliers to build a "dirty bomb." US NRC officials approved the request with a minimal background check that included no face-to-face interview or visit to the purported company to ensure it existed and complied with safety rules. The GAO undercover personnel used a post office box at a commercial mailing company, a telephone, and a fax machine to obtain the license "without ever leaving their desks." The GAO undercover agents made counterfeit copies of the license and ordered 45 portable moisture density gauges containing ^{137}Cs and ^{241}Am. The GAO personnel never took possession of the radioactive material.

In 2016, the GAO established three shell companies and successfully obtained a valid license for one of these companies that was altered to secure commitments to purchase a dangerous quantity of radioactive material.

In 2022, the GAO communicated with radioactive material vendors to determine the availability of the radioactive materials, cost, and existing shipping options; using fraudulent licenses, they bought high-risk radioactive materials (US GAO 2022; NPR 2007).

Process vulnerabilities exposed were the absence of original source verification, the apparent absence of a random audit process, and failure to personally interview personnel or visit the facility proposed for operations.

Case study #4

In October 1996, an individual allegedly contacted the radiation safety office at a university in upstate New York and requested a copy of their radioactive materials license (well before the existence of 10 CFR 37 security regulations). There was no valid reason not to provide him with a copy of the license; at this time, these licenses were considered public information.

The individual allegedly used a credit card to order radioactive material from a vendor and provided an address on campus that was not the radiation safety office. He stood outside the building at the address, signed for the package upon delivery, and drove off with the radioactive source.

He reportedly acquired radioactive materials on three occasions from other brokers by saying he had authorization from the university as well as claiming association with the university. The FBI investigated him after suppliers became suspicious; prosecutors said that the individual (who holds a doctorate degree) is not associated with the university. They allege that he used the material to calibrate equipment and distributed it to researchers; investigators said that the individual did not use the radioactive material for life-threatening purposes.

If ultimately convicted on charges of wire fraud, the individual faces a maximum penalty of five years in prison and a $250,000 fine. If convicted on charges of obtaining nuclear material by fraud, he faces a maximum sentence of 20 years in prison and a $250,000 fine. To date, there has been no public notice of the disposition of this decades-old case (Buffalo News 1997).

Process vulnerabilities exposed were the absence of original source verification, apparent absence of random audit process, and failure to confirm the change in delivery address.

Case study #5

Late in the 1990s in central Virginia, Individual A conducted medical physics audits and surveys (one of ~150 private inspectors authorized by the state health department). In 2000, one hospital became dissatisfied with his work, so they contacted Individual B to take over the medical physics work.

The US Attorney needed help understanding what a medical physicist is and does, so he retained Individual B to help prosecute Individual A. In 2005, Individual A pled guilty to lying about his background and failing to do the work he was paid for; he received 4½ years in prison and was assessed $375,831 in restitution. Individual A had previously worked in several prestigious government agencies.

Soon after Individual B testified against Individual A, Maryland authorities began investigating Individual B; it turns out he was bogus too. They enlisted the help of Individual A while he was still in prison to prosecute him.

Individual B obtained online degrees and offered his certificate from the "American Board of Diagnostic Medical Health Physics" to the FDA, the Department of Veterans Affairs, and state licensing agencies as proof of his graduate studies, clinical experience, and a passing score on a qualifying exam. Apparently, no one inspected the certificate because no such professional organization exists.

Individual B maintained a 13-page list of 220 clients along the Atlantic coast and did have his supporters. One hospital RSO stated: "I have worked with many different physicists in the past 18 years, and I can say without reservation that (Individual B) is the most proficient physicist I have ever met."

In April 2007, Individual B pled guilty to 48 counts of mail fraud and 1 count of perjury. The mail fraud represented the money he received from his clients. At the same time, the perjury occurred during his testimony against Individual A, because while he was on the witness stand, a defense attorney asked specific questions about his degrees. In September 2007, Individual B was sentenced to 4½ years in prison and ordered to pay $400,000 in restitution to hospitals and clinics in five states.

These occurrences of fraud spurred the creation and implementation of the NRC 313A form for attesting to valid education, experience, and credentials for physicians,

physicists, nuclear pharmacists, and radiation safety officers (Hall 2007).

Process vulnerabilities exposed were the absence of original source verification and the apparent absence of a random audit process.

Case study #6

In December 2016, an individual was hired as a regional manager at a Hawaiian industrial radiography company. He planned to take over his employer's business by misappropriating their equipment and personnel and setting up two side companies.

By 2018, the individual, with his two side companies, allegedly tried to perform non-destructive testing in West Virginia and Hawaii (two states under US NRC jurisdiction). To accomplish this work, he needed a radiography camera and an NRC license. He allegedly filed an application claiming he had a qualified Radiation Safety Officer with other false information about training and qualifications. The NRC issued the license based on the individual's false representations. After receiving the license, he ordered and signed for a radiography camera containing radioactive material. The NRC opened an investigation after concerns were raised about information in the license application.

In January 2019, while employed by his original company, the individual allegedly misappropriated one of its radiography cameras containing ^{192}Ir and depleted uranium radioactive source material. He had his side company employees use the camera for industrial radiography without recording the transfer of the radioactive sources, as required by law. Around the same time, the individual applied to a Hawaiian bank on behalf of one of his side companies for a revolving line of credit; he provided bank loan officers false information, including his side company assets.

In 2021, a federal grand jury returned an indictment charging the individual with violating the Atomic Energy Act (AEA), making false statements to the Nuclear Regulatory Commission, obstruction of NRC proceedings, and bank fraud; if convicted, he faces 42 years in prison (US DOJ 2021).

Process vulnerabilities exposed include the absence of original source verification, the apparent absence of a random audit process, and the failure to confirm operations.

COMMONALITIES

Based on a synopsis of the cases described here, a set of recurrent process vulnerabilities are revealed:

- An apparent presumption that if something appears official, it must be legitimate;
- An apparent presumption that someone else has previously verified all claims;
- Failure to verify claims with original sources—i.e., not a secondary report of a degree, but actual contact with the college or university to confirm (similarly with certification boards, licensing agencies, regulatory agencies);
- Failure to contact reliable professional references;
- Failure to meet in person or physically visit the facility; and
- Absence of some routine audit of a sampling of records, submissions.

Through increased awareness of these vulnerabilities, the radiation safety community can take immediate steps to improve the fidelity of the entire process.

PREVENTING FRAUD

Armed with the information described above, there are some simple steps the profession can consider to reduce or eliminate cases of fraud:

- Increase awareness and index of suspicion across the entire radiation protection profession to ensure all are collectively aware of the extent of the problem. We should ask ourselves: does what is being requested or confirmed even sound right?
- The radiation safety community is a relatively small world, so we should also ask ourselves: is the person or service being purported even known?
- Keep in mind that even if you know the person, their status or situation may have changed.
- Seek customer/client feedback, but remember some customers may be satisfied but don't know the person or group is practicing fraudulently. For example, are the prices too low to be true?
- Contact regulatory agencies independently, and verify specifics. For example, what exactly is the purported permit holder permitted to do or possess?
- Contact universities and professional organizations directly for confirmation. Verify licenses via agency web listings. Also, ensure currency to determine if there had been an expiration or termination.
- Consider an electronic field data collection inspection system that automatically data logs the date, time, and geolocation of the assessments being performed.
- Consider enlisting the services of a third-party verification firm.
- Actually visit with the person or visit the place.

SUMMARY

Practices of fraud are rampant in society, especially so in our digitally dependent economy. Actual fraud involving radiation sources has occurred and has been documented in the open literature. A review of selected cases reveals a set of exploitation commonalities; but armed with the knowledge of these vulnerabilities, some simple steps can be taken across the radiation protection continuum to thwart these practices.

REFERENCES

Black's Law Dictionary. Oxford languages [online]. 2023. Available at https://languages.oup.com/google-dictionary-en/. Accessed 6 July 2023.

Buffalo News. Man indited in purchase of radioactive material [lqb] [online]. 1997. Available at https://buffalonews.com/news/man-indicted-in-purchase-of-radioactive-material/article_cb2d8a76-3856-5ce4-97aa-

2787241a2064.html. Accessed 12 July 2023.
Clayton RM. The rise of insurance fraud: preventive steps for OSH professionals. Prof Saf 67:32–33; 2023.
Ferguson CD, Lubenau JO. Securing US radioactive sources. Issues Sci Technol 20:67–73; 2003.
Hall J. Inspector was not what he claimed [online]. The Free Lance-Star. October 14, 2007. Available at https://fredericksburg.com/image_f6f5a605-9d75-574d-858f-467c67027671.html. Accessed 24 July 2023.
Investopedia. The most common types of consumer fraud [online]. Available at https://www.investopedia.com/financial-edge/0512/the-most-common-types-of-consumer-fraud.aspx. Accessed 1 July 2023.
National Public Radio. GAO sting uncovers unclear security shortcomings [online]. 2007. Available at https://www.npr.org/2007/07/12/11907450/gao-sting-uncovers-nuclear-security-shortcomings NPR. Accessed 14 July 2023.
Silverstein K. The radioactive boy scout: the true story of a boy and his backyard nuclear reactor. New York: Random House Press; 2004.
US Department of Justice. Press release—September 15, 2014 [online]. 2014. Available at https://www.justice.gov/usao-md/pr/owner-alpha-diagnostics-indicted-75-million-health-care-fraud-scheme. Accessed 14 July 2023.
US Department of Justice. Press release—November 5, 2021 [online]. 2021. Available at https://www.justice.gov/opa/pr/hawaii-man-indicted-violating-atomic-energy-act-obstruction-agency-proceedings-making-false. Accessed 14 July 2023.
US Government Accountability Office Report. Preventing a dirty bomb: vulnerabilities persist in NRC's controls for purchases of high-risk radioactive materials [online]. 2022. Available at https://www.gao.gov/products/gao-22-103441. Accessed 15 July 2023.
Van Akkeren J. Fraud triangle: Cressey's fraud triangle and alternative fraud theories. In: Poff D, Michalos A, eds. Encyclopedia of business and professional ethics. Springer, Cham; 2018. Available at https://doi.org/10.1007/978-3-319-23514-1_216-1. Accessed 3 July 2023.