PERSPECTIVES

AI FRAUD DETECTION AND FORENSIC ACCOUNTING:
Embracing Innovation to Combat Financial Crime

JS|HELD

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

Copyright © 2025 J.S. Held LLC, All rights reserved.

Introduction

In today's rapidly evolving digital landscape, fraud and financial crime have become increasingly complex and create pervasive issues for organizations of all sizes and specialties. As a result, advanced technology and artificial intelligence (AI) have emerged as invaluable tools in the fight against such issues. By leveraging sophisticated algorithms, data analytics, and machine learning capabilities, combined with traditional forensic accounting principles, these technological advancements empower investigators and compliance professionals to enhance their investigative processes, identify patterns and anomalies in vast amounts of data, and proactively detect unusual activities. The integration of advanced technology and AI not only accelerates these types of investigations but also supports compliance with regulatory standards, ultimately leading to more robust and effective fraud prevention and detection strategies.

While the technology itself demonstrates impressive capabilities, its innovation is fully realized through its use by professionals. For example, forensic accountants and investigations specialists interpret transaction analyses and perform due diligence on suspicious individuals and entities. Investigations benefit from combining deep subject matter expertise with an analytical approach, deriving actionable intelligence from advanced technology, forensic accounting, and other fact-finding disciplines.

This article focuses on how advances in AI and machine learning can aid forensic investigation procedures and further bring the detection of fraud and other financial crimes into the digital age.

The Evolution of Fraud and Financial Crime

Fraud and financial crime, including money laundering, digital currency schemes, and sanctions violations, have challenged organizations for years. Consequently, companies continue to focus more time and money on preventing and combating these activities. A Juniper Research report on online payment fraud found that merchants and financial service organizations will spend $9.3 billion annually on fraud prevention.[1] Simultaneously, corporations and professional services firms work to improve their processes as well. That said, fraudsters continue developing tactics to bypass new preventative measures. However, AI and technological advancements have the potential to revolutionize financial crime detection and anti-fraud processes, making them more efficient and effective than before.

Leveraging Artificial Intelligence and Machine Learning to Detect Fraud Faster

AI-powered systems can analyze vast volumes of data in real-time, swiftly identifying suspicious patterns, trends, and anomalies that may indicate fraudulent activities. Machine learning algorithms can continuously learn and adapt to evolving fraud techniques and a litany of changing rules and regulations, enhancing detection capabilities and reducing false positives. The ability to constantly improve procedures is incredibly powerful, as these algorithms can make changes to processes that previously took significant amounts of time to identify and implement under an organization's framework. Additionally, advanced technology enables the automation of time-consuming and repetitive tasks, such as data entry and document verification. This allows investigators to focus on higher-value activities such as complex analysis and strategic planning.

While these technological advancements are powerful, their potential can be inhibited by the traditional organizational structure of an investigation. Financial crime and anti-fraud efforts are typically separated into two distinct areas: compliance and security. Segregating activities in this manner can lead to inefficiencies in resource allocation. Although each field has its own unique skill sets, investigative efforts often track the same suspicious individuals and even use the same technology. Companies can take advantage of potential overlap by combining efforts from both sides. This collaboration is especially useful in the application of machine learning. Machine learning models operate most effectively when given as much data and training across myriad scenarios. This dual approach enables the identification of fraudulent behavior while simultaneously ensuring adherence to legal and compliance frameworks.

Calculating Damages from an Embezzlement Scheme

A high school for at-risk youth discovered that the head of finance was embezzling funds. When the high school filed an insurance claim, the insurance company retained us to investigate and calculate the extent of the damages. We utilized AI-enabled software to analyze:

» All transactions, including transfers and checks. This included 20,000 transactions across 10 accounts over a five-year period. The transactions were automatically matched in just hours, instantly revealing transfers the suspect made into his personal bank and brokerage accounts.

» Full payor details for over 1,000 checks – including those that were handwritten – that were then ready to be analyzed in just a few days.

» The damages were quickly calculated to be more than $7 million in funds potentially embezzled.

Every transaction was then linked back to the original banking evidence, making it simple to prepare a report for the insurance company that would withstand the scrutiny of the courtroom.

Data Analytics: High Tech Tool or Industry Disruption?

Robotics and automation are expected to see continued growth due to the world's increasing reliance on technology. In the past few years, especially, AI has been making headlines as its use and development provide opportunities for automation in numerous industries. Recent articles have warned of the dangers of available AI technologies, focusing on the potential disruption of the job market. While these concerns are not unfounded (the World Economic Forum predicts that by 2030, approximately 30% of all jobs will be at risk of AI automation[2]), a "robot takeover" is far from the anticipated outcome.

AI can be used to complete time-intensive or repetitive tasks, but it is not equipped to replace humans in tasks that require critical or expert thinking. Like other technological advancements, humans have learned how to use AI to make workflows more efficient, and companies have been recognizing this potential. This shift is noticeable in the information technology field, for example, where 53% of information technology professionals say they have accelerated AI adoption over the last two years.[3]

Similarly, AI has been making waves in investigative data analytics, where analysts are often ingesting a plethora of data that can include financial transactions, as well as vendor, customer, and employee information. The processes to standardize these data points into a unified framework are time-consuming and repetitive. Project timelines can be lengthy, driving up costs for clients. It is the responsibility of analysts to stay apprised of new and emerging tools and apply these technologies to increase our efficiency for our clients. In recent years, there have

Untangling a Lapping Scheme

Following the acquisition of a smaller company, the acquiring firm- a healthcare staffing agency – began to suspect irregularities in the accounts receivables.

We were retained by the chief financial officer to complete a recalculation of the accounts receivables balance. We discovered the general ledger had not been properly maintained, and there were more than 25,000 checks to evaluate. Because "lapping" was suspected – when payments from one customer are applied to a different customer's account – check analysis was critical. Using AI-enabled software, we uncovered:

» Full payor details for over 25,000 checks – including those with poor image quality – were ready to be analyzed in just a few days.

» Checks were automatically matched to bank transactions, with missing or ncomplete data flagged, helping to increase the speed of the analysis.

» The lapping scheme was revealed to be material, with more than $30 million in potential misapplied payments identified.

We met the deadline, helping our healthcare staffing agency client make an informed decision about its insurance claim.

been several developments in AI and machine learning that allow professionals to speed up and automate analyses.

Machine Learning for Forensic Accounting and Financial Investigations

Skilled consultants use cloud-based technology to automate the processes used to collect, validate, and analyze structured (e.g., databases, transactions) and unstructured (e.g., Email, chats) data sources and investigative algorithms. Prior to these technological advancements, data collection and validation took a substantial amount of budget – sometimes as high as 50%. Utilizing machine learning and artificial intelligence allows for increased automation of these once time-intensive processes and allows the experts to focus more on analyzing the data, deriving insights from results.

Machine learning and AI additionally enable analytics and behavior algorithms that support customized testing and flexible reporting. For example, a company suspects that an employee is creating false vendor invoices and misappropriating funds. Equipped with the right tools, investigators can bring the company's vendor lists, invoices, accounts payable, and other relevant data into an online platform to perform fraud detection analyses. They can swiftly identify vendors that might share a phone number, address, or bank account number with an employee and perform other tests for conflicts of interest. Investigators can also set up a system to perform active monitoring alongside existing internal controls. This information is available with a built-in visualization tool, decreasing the time required to build analytical dashboards.

Another advancement in AI provides a quick and efficient way to transform PDF data sources (e.g., bank statements, check images) into usable structured data using **Optimal Character Recognition**, or **OCR**. This technology detects and converts text from digital files into a searchable and copyable format. Unfortunately, OCR tools within many PDF editors prove to be unreliable, especially in cases where text is difficult to read or pages contain formatting inconsistencies. Using enhanced OCR tools that harness AI, investigators can process bank statements, checks, brokerage statements, and other financial documents into exportable and analyzable data to support investigative efforts. As part of a test for accuracy, these new tools compare beginning and ending balances of statements with the extracted transaction details. Any mismatches are flagged and returned to the user to ensure accuracy.

Forensic Accountants Need to Innovate

Technology has played a pivotal role in shaping the field of forensic accounting throughout history, revolutionizing the way financial investigations are conducted and uncovering fraudulent activities. Not too long ago, the field of forensic accounting was a foreign concept to many. Most historical research and publications were focused on showcasing the extent of existing fraud and convincing organizations of the importance of implementing anti-fraud and detection efforts, as well as the significant cost savings forensic accountants provided.

However, technological advancements and investment by organizations have provided forensic accountants with powerful tools and techniques to analyze complex financial data, detect irregularities, and deliver more accurate results. Looking ahead, forensic accountants must continuously search for innovation to

further transform their investigative role. The ongoing development of advanced data analytics, machine learning algorithms, and blockchain technology will enable forensic accountants to tackle emerging challenges in an increasingly complex digital landscape. These innovations will bolster the ability to detect and prevent fraud but will require forensic accountants to adapt to a fast-changing environment.

Conclusion

Fraud detection and investigative data analytics are two of many areas in the legal and regulatory space that are being transformed by AI and machine learning tools. By embracing these tools rather than rejecting them, investigators can reclaim time previously spent on repetitive, less complex work and instead focus on tasks that require deeper analysis or critical thinking.

AI and advanced technological tools are transforming the fraud landscape. Fraud and money laundering continue to threaten organizations across the globe, and their prevalence will persist as fraudsters constantly develop new methods and weaponize the same technology that organizations can use to improve their fraud prevention. However, with proper application of these emerging technologies for both fraud prevention and internal investigations, organizations can significantly improve the efficiency and effectiveness of their anti-fraud response to match an ever-changing landscape.

Acknowledgments

We would like to thank Ken Feinstein, Matthew Cordell, and F. Dean Driskell III for providing insights and expertise that greatly assisted this research.

More About J.S. Held's Contributors

Ken Feinstein is a Senior Managing Director in the Digital Investigations and Discovery Service Line within the Global Investigations practice at J.S. Held. He specializes in investigative data analytics and provides investigations, regulatory risk, and litigation support solutions spanning multiple sectors, including retail and consumer products, life sciences, technology, financial services, industrial products, and government agencies. His clients include law firms and Fortune 500 legal and compliance teams for whom he delivers large-scale, complex investigations, regulatory response matters, proactive anti-fraud efforts, and compliance programs. He is a member of the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners.

Ken can be reached at ken.feinstein@jsheld.com or +1 917 277 7868.

Matthew Cordell is a Senior Director in the Digital Investigations and Discovery Service Line within the Global Investigations practice at J.S. Held. He helps analyze structured and unstructured data along with other forensic accounting and investigative methods to help clients achieve their goals in reducing fraud and regulatory risk. His work includes data modeling and analysis, database management, programming, and implementing finance software spanning multiple industries, including financial services, technology, industrials, life sciences, and retail. His clients include law firms and Fortune 500 multinational companies. He is a member of the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners.

Matthew can be reached at
matthew.cordell@jsheld.com or
+1 214 216 4960.

F. Dean Driskell III is an Executive Vice President in J.S. Held's Economic Damages & Valuations practice. He specializes in performing consulting services for clients involved in various types of accounting, economic, and commercial disputes, as well as fraud and forensic accounting matters. With more than 30 years of experience in financial analysis, accounting, reporting, and financial management, Dean has served clients and their counsel in both private and public sectors, providing technical analyses, accounting / restatement assistance, valuation services, and litigation support across a variety of industries, and as an expert witness in litigation.

Dean can be reached at
DDriskell@jsheld.com or
+ 1 404 876 5220.

[1] https://www.businesswire.com/news/home/20170725005147/en/Juniper-Research-Online-Payment-Fraud-Detection-Spend
[2] https://www.weforum.org/agenda/2020/10/dont-fear-ai-it-will-lead-to-long-term-job-growth/
[3] https://www.ibm.com/downloads/cas/GVAGA3JP

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal, or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation, or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.

J.S. Held, its affiliates and subsidiaries are not certified public accounting firm(s) and do not provide audit, attest, or any other public accounting services. J.S. Held is not a law firm and does not provide legal advice. Securities offered through PM Securities, LLC, d/b/a Phoenix IB or Ocean Tomo Investments, a part of J.S. Held, member FINRA/SIPC. All rights reserved.