LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Announcements:

The Lansing ACFE Winter Conference is **February 20th** and will be offered in-person in East Lansing and virtually! See details in *Upcoming Events*.

Don't forget to renew your LACFE membership! Remember that only paid members receive the discount for LACFE trainings. Find the membership form at: Membership | (lansingacfe.com)

Did you know that LACFE offers a scholarship for CFE certification? The Board is looking to reach out to additional colleges to reach more potential scholarship applicants. Do you have a contact within a college or college group that may have students interested in this scholarship? Please send those contacts to Jennifer Edmonds at treasurer@lansingacfe.com

In This Issue

Fraud Talk Podcast

Adapting Fraud Detection for Latin America - Marta Cadavid - Fraud Talk - Episode 149

In this episode of Fraud Talk, Mason Wilder sits down with Marta Cadavid, founder of NoFraud Latam, to explore the unique challenges of detecting and preventing fraud in Latin America. Cadavid shares her journey, including the creation of a Latin American-specific fraud tree, and how cultural nuances shape the approach to fraud communication. They discuss the vital role of artificial intelligence in analyzing human behavior and predicting fraudulent actions.

https://acfe.podbean.com/e/adapting-fraud-detection-for-latin-america-marta-cadavid-fraud-talk-episode-149/

UPCOMING EVENTS

LOCAL:

MICPA Tax Season Update with Steve Dilley
Multiple dates and locations:
January 14th, 16th, 23rd, February 5th
Grand Rapids, Livonia, Online, Online
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=157462&return=1~1

SAAABA/AGA Annual Tax Update
Constitution Hall, South Atrium Level, 525 West Allegan, Lansing MI, 48933
January 15, 2025
11:45 am – 12:45 pm
Learn more: https://www.saaaba.org/events3/

ACFE South Florida Presents: Winter Fraud Forum A Virtual Seminar on Fraud Trends and Prevention (includes a Healthcare Fraud Panel and Case Study)
Virtual
January 24, 2025
9:00 am - 12:00 pm
Learn more: https://acfesouthflorida.org/event-5996502

ACFE Southwest Ohio Chapter – Ignorance is Blitz (Case Study)
In-Person or Virtual
February 13, 2025
12:00 pm - 1:30 pm
Learn more: https://swohacfe.org/event-5852166

Lansing ACFE Winter Fraud Conference
In-Person (East Lansing) or Virtual
February 20, 2025
More details coming soon! See the poster below.

NATIONAL:

ACFE Adapting Anti-Fraud Practices in the Generative AI Age
On-Demand Webinar – *FREE to CFEs in good standing*
Learn more: Product Detail Page

ACFE Women's Summit
In-Person or Virtual
March 7, 2025
(early registration ends January 21st)
Learn more: 2025 ACFE Women's Summit

Help me create your newsletter! If you have an event that you would like posted or if you wish to share an article, please contact Jennifer Ostwald at jenny1661@hotmail.com

The Lansing Chapter of the Association of Certified Fraud Examiners

Winter Fraud Conference

February 20, 2025

Theft of $450,000 – A Nickle at a Time

Polygraph Information and Ethics

Fraud Statistics, Detection, Prevention, and Advanced Excel Data Analytics

Plante Moran • 1111 Michigan Ave. East Lansing, MI 48823

CONFERENCE DETAILS	
Conference Fee:	$250 chapter members, $285 non-members
Registration:	Through Friday, February 14, 2025
CPE Credit:	8 Hours
Dress:	Business Casual*
Format:	In-Person or Virtual

** This conference is being offered in-person or virtually, via Zoom.*

Holiday Scams to Watch Out for in 2024

November 11, 2024
Dustin Eaton, CAMS
https://www.acamstoday.org/holiday-scams-to-watch-out-for-in-2024/

The holiday season, with its surge in shopping, travel and festive activities, is also a peak period for scammers who seek to exploit the spirit of generosity and the flurry of financial transactions. In 2024, as digital technology becomes more integrated into daily life, new and evolving scams pose significant threats to consumers and financial institutions alike. Understanding these scams and employing strategies to guard against them is vital for both consumers and bank employees who are at the front line of detecting fraudulent activity. Below are six of the most prominent scams likely to be at the forefront of the holiday season.

1. Phishing and Smishing Attacks

Phishing, where attackers impersonate legitimate organizations to obtain sensitive information, remains a top threat.[1] In 2024, scammers have improved their tactics, using advanced technology to craft convincing emails and text messages. Smishing, or phishing via SMS, is particularly popular as more consumers rely on their smartphones for online shopping and financial transactions.[2]

Example scenario: A consumer receives a text message purportedly from their bank or a popular retailer, warning them of a suspicious transaction and prompting them to click a link to "secure" their account. Clicking this link can lead to a fraudulent site designed to steal login credentials or prompt the installation of malware.

Recommendation for Consumers:

- Verify the sender's authenticity by directly contacting the institution or retailer using verified phone numbers or websites.
- Avoid clicking on links in unsolicited emails or texts, even if they seem urgent.

Advice for Bank Employees:

- Be alert for customer accounts that show unusual activity immediately after a suspicious message has been reported.
- Educate customers about the bank's communication methods, emphasizing that legitimate organizations never ask for passwords or sensitive information via email or text.

2. Fake E-commerce Sites and Social Media Ads

As online shopping grows, fake e-commerce sites have become more sophisticated. In 2024, scammers are leveraging social media ads to attract consumers to well-designed but fraudulent websites that offer deals too good to be true.

Example scenario: A shopper finds an ad on social media for luxury or popular goods at an unbelievable discount. Clicking the ad takes them to a website that looks legitimate but is a scam. Payment results in sharing card details and other sensitive personal data, a potential loss of funds, and often the product never arrives.[3]

Recommendation for Consumers:

- Research online retailers thoroughly, checking reviews and verifying the website's URL for signs of authenticity (e.g., HTTPS and legitimate domain names).
- Use secure payment methods, like credit cards or services that offer fraud protection.

Advice for Bank Employees:

- Monitor accounts for sudden, high-value online purchases from lesser-known sites, which could be indicative of fraudulent activity.
- Assist customers in disputing fraudulent charges swiftly and guide them on steps to protect their accounts.

3. Charity Scams

Scammers often take advantage of the season's charitable spirit. In 2024, these scams have become more targeted, using email campaigns that appear to be from real nonprofits or mimicking well-known charity organizations[4] with slight name changes.[5]

Example scenario: Consumers receive emails or social media messages asking for donations to disaster relief funds or community initiatives. These messages may link to cloned websites where donations go straight to scammers.

Recommendation for Consumers:

- Always donate through well-known, established charity websites or platforms and verify the legitimacy of new charities through services like the Better Business Bureau's Wise Giving Alliance.
- Be cautious of unsolicited requests for donations and verify their authenticity before contributing.

Advice for Bank Employees:

- Be vigilant about sudden, repeated donations to unfamiliar organizations.
- Educate customers about safe giving practices, emphasizing how to spot fraudulent charitable solicitations.

4. Gift Card Scams

Gift cards are popular holiday gifts, but they are also frequently used by scammers as an untraceable form of payment.[6] In 2024, scammers continue to impersonate tech support agents, government officials, or even friends and family members, demanding payment in the form of gift cards.

Example scenario: A scammer poses as a representative from the Internal Revenue Service or a utility company, threatening immediate legal action unless payment is made through gift cards. Once the victim provides the card information, the funds are quickly depleted.

Recommendation for Consumers:

- Be skeptical of anyone requesting gift card payments, as legitimate companies or agencies never accept them as a form of payment.
- Report any suspicious calls or messages to local authorities or consumer protection agencies.

Advice for Bank Employees:

- Watch for unusual gift card purchases or withdrawals that are atypical for a customer's spending behavior.
- Inform customers that banks and legitimate companies never ask for payment in gift cards.

5. Travel Scams

The holiday season also brings an increase in travel, which scammers exploit with fake travel deals, bogus accommodation listings and fraudulent ticket sales.[7] In 2024, scammers have begun using cloned websites of reputable travel agencies and online booking platforms to defraud travelers.

Example scenario: A traveler books a holiday rental from a site that looks identical to a trusted platform but is, in fact, a scam. After making a payment, they discover that the rental does not exist or is not affiliated with the platform they thought they were using.

Recommendation for Consumers:

- Use well-known booking sites and verify the website's URL carefully before making any payments.
- Be cautious of deals that are significantly cheaper than the market rate and ask for independent verification of listings.

Advice for Bank Employees:

- Pay attention to large, international transactions tied to travel agencies that are not commonly seen in a customer's history.
- Collaborate with fraud teams to trace suspicious travel payments quickly and advise customers on reclaiming lost funds when fraud is detected.

6. Package Delivery Scams

With the increase in online shopping, scammers are capitalizing on package delivery notifications.[8] In 2024, fraudulent delivery notices, sent via email or SMS, prompt users to click a link to reschedule a delivery or pay a delivery fee.[9]

Example scenario: A consumer receives a message stating that a package could not be delivered and must click a link to reschedule. The link leads to a page that asks for personal details or payment, leading to identity theft or financial loss.

Recommendation for Consumers:

- Contact the delivery service directly through their official website or customer service to verify any delivery issues.
- Avoid clicking on links from unknown senders claiming to be delivery services.

Advice for Bank Employees:

- Be alert to instances where customers report suspicious charges related to small, unknown delivery companies.
- Implement educational initiatives about these scams, encouraging customers to double-check unsolicited notifications.

Conclusion

The holiday season should be a time for joy and celebration, not for becoming a victim of scams. By staying informed about the latest threats and practicing caution, consumers can safeguard their personal information and finances. Bank employees play a critical role in identifying and mitigating these risks, protecting both their institutions and their customers. By fostering awareness and collaboration, 2024 can be a safer year for all.

How Internal Audit Powers Fraud Investigations and Protects Organizations from Within

November 12, 2024
By Rihonna Scoggins
https://www.acfe.com/acfe-insights-blog/blog-detail?s=internal-audit-powers-fraud-investigations-protects-organizations

Fraud is a costly and complex threat to organizations, demanding strategic and well-executed defenses. Among the most valuable assets in an organization's fraud prevention toolkit is its internal audit team. Internal auditors have the advantage of an insider's view of an organization's controls, making them uniquely positioned to help identify fraud risks and support investigations.

The Strategic Position of Internal Audit in Detecting Fraud

Internal auditors are embedded within the organization, with access to systems, controls and transactions. They do not just understand the organization's policies; they understand the gaps and weak points where fraud can creep in. By examining irregular patterns, flagging unusual transactions and assessing where internal controls may falter, they serve as an early warning system.

Rather than waiting for a whistleblower or a suspicious transaction to trigger an investigation, internal auditors can spot the signs of fraud as part of their regular risk assessments. This proactive approach is especially valuable in industries prone to complex schemes—such as those involving procurement, payroll or regulatory reporting.

Internal Audit's Key Role in Investigations

When fraud is suspected, internal auditors can support or even lead the initial fact-finding phase. Their investigative role varies by organization, but it typically includes:

- **Data Gathering and Analysis:** Internal auditors have access to high volumes of operational data and understand its nuances, allowing them to dive into the numbers with a critical eye. This skillset is essential for identifying trends or anomalies that signal fraud, such as unexplained spikes in spending or suspicious vendor activity.
- **Uncovering Internal Control Failures:** A key strength of internal audit lies in its capacity to examine whether controls are functioning as intended. If a control weakness is uncovered, internal audit can explore how it might have enabled fraud—and recommend changes to strengthen defenses moving forward.

Navigating Challenges and Conflicts

Internal auditors face challenges that may constrain their involvement in fraud detection. There is often a fine line between their roles in audit and investigation, and they must maintain objectivity, especially if the suspected fraud involves senior leadership. Additionally, resource constraints or limited forensic training can present hurdles. Yet, these challenges underscore the importance of collaboration between internal audit, compliance, legal and dedicated fraud investigators.

Building a Resilient Anti-Fraud Culture

Beyond detecting and investigating fraud, internal audit teams are instrumental in cultivating a culture that discourages fraudulent behavior. After each investigation, they assess the findings to improve internal controls and advise on how to reduce fraud vulnerabilities in the future. This is where the internal audit function's true value shines: by embedding fraud prevention into daily operations, they help create an organization more resilient to fraud risks.

The Path Forward for Internal Audit

While internal auditors are essential to fraud detection, they often face challenges like limited forensic training, resource constraints and the need to balance investigative and auditing roles. Investing in continuous education can help auditors stay ahead of emerging fraud risks and hone their skills in identifying red flags.

For those seeking to deepen their expertise, the ACFE's *Auditing CPE Bundle* offers in-depth courses focused on core principles of fraud prevention and detection, making it a valuable resource for expanding knowledge and maintaining a proactive approach to fraud risks.

The role of internal audit is evolving as fraud schemes grow more sophisticated. Organizations that empower internal auditors to play an active part in fraud investigations not only improve their detection capabilities but also foster a culture of accountability and transparency. In this sense, internal audit does not just monitor compliance; it safeguards the organization's integrity, one audit at a time.

Video of the Month

Holiday fraud (and a new year), how can we prepare?

As the holiday season kicks into high gear, it's not just shoppers and families preparing for festivities—fraudsters are ramping up their efforts too. In the latest episode of Good Question, we sit down with fraud prevention experts Dustin Eaton, a financial crimes professional at Seis who recently published an article with ACAMS titled "Holiday Scams to Watch Out for in 2024," and Daragh McMeel, risk operations manager at Inscribe AI, to discuss seasonal fraud trends, scams to watch out for, and how businesses and consumers can protect themselves.

Fraudify Wrapped 2024: The Year in Fraud Trends

December 10, 2024
By Abbie Staiger
https://www.acfe.com/acfe-insights-blog/blog-detail?s=fraudify-wrapped-2024

Welcome to Fraudify Wrapped 2024! This year, fraud examiners tracked the top scams reshaping industries, the most impacted sectors and the tools fraudsters wielded with alarming innovation. Drawing from industry trends, news stories and expert insights, we have compiled a recap of the biggest fraud developments of the year.

The Top Frauds of 2024

These schemes dominated the fraud landscape, posing challenges for individuals and organizations alike:

1. Pig Butchering

Fraudsters lured victims into fake investment schemes by posing as romantic interests or long-lost friends. Once trust was established, they manipulated victims into transferring large sums to fraudulent cryptocurrency and digital asset investment platforms. The twist? Many scammers used artificial intelligence (AI) to maintain convincing interactions. Pig butchering scams reached a new level of sophistication, with fraudsters deploying professional-looking websites, social media profiles and even customer service representatives to make their operations appear legitimate. Meta released a statement on going after criminal organizations behind pig butchering schemes, stating, “This year alone, we’ve taken down over two million accounts linked to scam centers in Myanmar, Laos, Cambodia, the United Arab Emirates and the Philippines.” These scams were not only devastating financially but emotionally, as victims invested their savings and time into building relationships with scammers who had no intention of ever returning their funds. Global losses from these schemes skyrocketed, with a surge in targeted regions such as Southeast Asia and North America.

2. Account Takeovers and New Account Fraud

This trend saw cybercriminals exploiting stolen credentials to hijack accounts or create fraudulent ones. Account takeovers have reached alarming rates over the past few years, with a notable uptick in attacks on online banking platforms and e-commerce websites. Fraudsters often used information obtained from data breaches or social engineering tactics to gain access to financial accounts and make unauthorized withdrawals. On the other hand, new account fraud flourished, as criminals used synthetic identities to open new accounts and secure loans, often escaping detection due to advancements in AI technology. These schemes were most prevalent in the financial services industry, where fraudsters circumvented financial institutions' automated fraud detection systems to carry out large-scale money laundering operations.

3. Synthetic Identity Fraud

By merging real and fabricated data, criminals created synthetic identities that slipped through detection systems. This type of fraud has become even more sophisticated, with fraudsters combining legitimate personal information with fabricated elements to create entirely new identities. These synthetic identities were then used to secure credit lines, loans and even

government benefits. Financial institutions and other service providers found it increasingly difficult to spot these fraudsters, as the synthetic profiles often appeared to have established histories, complete with credit reports and verifiable employment records. Synthetic identity fraud continued to plague the financial services and retail sectors, with fraudsters leveraging these fake identities for criminal activities such as money laundering, credit card fraud and loan defaults.

4. Deepfake Business Email Compromise (BEC)

BEC scams continued evolving in sophistication through the increased incorporation of deepfake technology. Fraudsters created hyper-realistic AI-generated video and audio to impersonate executives, convincing employees to authorize large payments. Deepfake BEC became one of the most sophisticated scams, with cybercriminals using AI to simulate the voices and faces of company CEOs, CFOs and even government officials. These deepfakes were used to deceive employees into transferring funds, altering contracts or divulging sensitive information. In some cases, the fraudsters even used deepfake technology to impersonate high-level employees in virtual meetings. The success of these scams relied on how convincing the deepfakes were and the industry saw a rise in software developed specifically to detect these fraudulent media manipulations.

5. Government Impersonation

Scammers posed as government officials, targeting individuals and businesses with fake IRS calls, counterfeit permits and fraudulent grant offers. The frequency of these scams is increasing, with fraudsters impersonating government agencies to defraud citizens out of tax payments, welfare checks or social security benefits. Some scammers even went so far as to create fake websites that mirrored official government portals, convincing victims to input personal information or make payments to fake accounts. Government impersonation also affected businesses, with fraudsters submitting fraudulent applications for government contracts and grants. These schemes disrupted operations, drained financial resources and damaged reputations.

Top Industries Affected by Fraud

Fraud spared no sector, but these industries faced the brunt of attacks:

1. Healthcare

Fraudulent claims, fake suppliers and billing scams surged, exploiting weaknesses in a stressed sector. Healthcare institutions, particularly hospitals, have been hit hard with fraudulent billing schemes. Fraudsters submitted fake invoices or overstated charges for medical procedures and equipment. In some cases, they even posed as medical suppliers to sell counterfeit or substandard medications. This type of fraud not only resulted in financial losses but also put patients' health and safety at risk. Additionally, healthcare providers continued to be prime targets for cybercriminals, who used stolen personal health information to launch identity theft and insurance fraud schemes.

2. Government

Impersonation scams and fraudulent applications for grants and benefits highlighted vulnerabilities in public systems. The government sector saw a significant rise in fraud schemes in recent years, particularly targeting COVID-19 relief funds, unemployment benefits and other social services. Scammers exploited government programs designed to provide

financial relief during the pandemic by submitting false claims and using stolen identities. These scams not only hurt the financial integrity of governments but also eroded public trust in their ability to protect citizens. Additionally, since governments have an enormous amount of obligations for which they depend on private sector companies, contract and procurement fraud continues to be a major concern for government agencies.

3. Financial Services

Account takeovers and synthetic identity fraud led to significant monetary losses and damaged trust. The financial services sector has remained a top target for fraudsters, with account takeovers affecting banks, investment firms and e-commerce platforms. Fraudsters also used synthetic identities to gain access to loans, credit lines and even open new accounts, leaving financial institutions with massive losses. Financial services companies struggled to keep up with the sophisticated tactics used by criminals, who often leveraged stolen data from previous breaches or used AI tools to manipulate fraud detection systems. The rising cost of fraud in the financial sector has led many institutions to invest heavily in new technologies, such as AI-powered fraud prevention systems, to detect and mitigate these risks.

4. Manufacturing

Supply chain scams, including fake vendor schemes, created logistical nightmares. The manufacturing industry found itself increasingly targeted by fraudsters who posed as suppliers or vendors to intercept payments or deliver counterfeit goods. Scammers often exploited the industry's reliance on complex supply chains and global networks, tricking companies into paying for goods that were never delivered or for substandard materials. As manufacturers grappled with disrupted supply chains, the financial impact of these frauds grew, with some companies losing millions of dollars in fake orders and payments.

5. Construction

Fraudsters exploited payment systems and posed as contractors to swindle businesses. The construction industry has faced a surge in fraud schemes, with criminals posing as contractors, subcontractors or suppliers to receive payments for non-existent work or materials. These scams were often facilitated by forged documents and fake invoices that appeared legitimate at first glance. The construction industry’s vulnerability to fraud grew as digital payment systems became more prevalent, making it easier for fraudsters to manipulate payment approvals or alter financial records. Additionally, the high costs associated with many construction projects tend to lead to large losses when fraud does occur.

Fraud Genre of the Year: AI-Powered Fraud

Artificial intelligence was the headline act in 2024’s fraud trends, as evident throughout this blog. Fraudsters deployed AI to craft realistic phishing emails, automate social engineering and create networks of fake identities. Deepfakes, synthetic data and automated scam operations blurred the line between human and machine-led fraud. AI-powered fraud tools grew exponentially this year, making it harder for traditional fraud detection methods to keep pace.

In a recent Public Service Announcement (PSA) released by the Federal Bureau of Investigation (FBI), the FBI warned the public that “criminals exploit generative artificial intelligence (AI) to commit fraud on a larger scale which increases the believability of their schemes.” Additionally, they pointed out that “Generative AI reduces the time and effort criminals must expend to deceive their targets,” making it easier and faster for criminals to

generate convincing fake identities or manipulate large datasets in a fraction of the time it took human fraudsters.

"Fraudify" Highlights

Here are fraud highlights that stood out to us throughout 2024:

Tactic of the Year:
Social engineering continued to dominate, with fraudsters leveraging human trust to power most schemes.

Comeback Scheme:

Phishing emails made a strong return, enhanced by generative AI to target victims at scale.

Looking Ahead to 2025

The battle against fraud is far from over. As scams grow more sophisticated, collaboration, innovation and proactive measures will be essential to mitigating risks. Let Fraudify Wrapped serve as a reminder: understanding the trends is the first step to combating them.

What fraud trends will shape the year ahead? Stay tuned for our Fraud Trends of 2025 blog coming this January, where we'll explore the emerging threats and opportunities to stay one step ahead.

Quote of the Month

"When criminals can perfectly imitate your CEO's voice and writing style for less than $400, traditional fraud prevention becomes obsolete."

— Nicolas Thomas, Inkan.link's founder and 25-year enterprise technology veteran

Reindeer Games Solutions

Dickens' *A Christmas Carol* - SOLUTION

```
. . . . . Y . . . . . . . . . . . . . . E . .
. . . . . T . . . . . J A C O B M A R L E Y .
. . . . . R . . . . . . . M . . . . . . R . .
. T N E S E R P S A M T S I R H C F O T S O H G .
. . . G V L . . . . S . S . . . . . I . P . T . .
. . . O . L . . . . . E . . . G . N . . I . Y . .
. . P O . E . . . . R . L . I . Y . . . R . T . .
. . . R . B . . . . . . . F . T . . . . I . R B .
E M O C O T T E Y S A M T S I R H C F O T S O H G
G H O S T O F C H R I S T M A S P A S T S B F E U
. . . R . . . . . . . . . . . . H . . . C . N . B
. S N E K C I D S E L R A H C . . . . R . E E . M
. . . Z . . . . . . . . . . . . . . A G R E E D U
. . . E . . . . . . . . . . . . . . T . O . . T . H
. . . N . . . . . . . . . . . . . C . S . . . H . H
. . . E . . . D N A L G N E T H G I R F . . G . A
. . . B . . . . . . . . . . I . T . . . . . I . B
. . . E . . . . . . . . . T . Y . . . . . . E . .
. . . . . . . . . . . . . . . . . . . . . . . . .
```

Charles Dickens	poverty	Ghost of Christmas Past
Ebenezer Scrooge	spirits	
selfish	frighten	Ghost of Christmas
miser	generosity	Present
Bah! Humbug!	England	
Jacob Marley	gifts	Ghost of Christmas
Bob Cratchit	greed	Yet to Come
Tiny Tim		

To find the answer to the trivia question, look for a word or phrase that is hidden in the puzzle, but not in the word list.

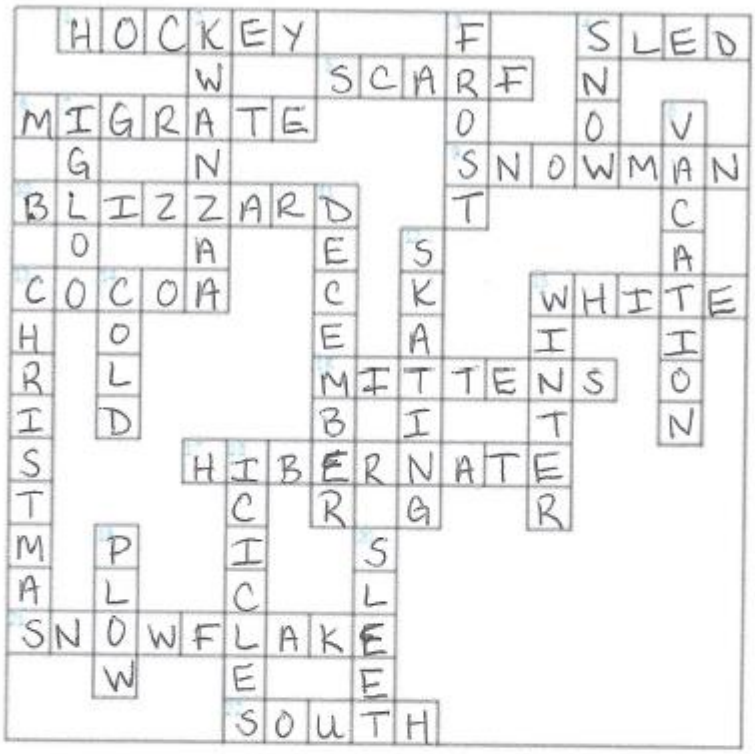
Trivia 1: **In what year was Dicken's novella, *A Christmas Carol,* first published?**

Trivia 2: **In the story, Scrooge lost the true love of his life because of his greed and love for money. What was the first name of his "true love"?**

Answer 1 : 1843

Answer 2: Belle

Winter



Across

1 Ice sport played with a puck
4 Fun ride down a snowy hill
5 Neck warmer
6 Change habitat seasonally
9 Sometimes has a carrot nose
10 Snowstorm
13 Hot sweet drink
15 The color of snow
16 Keeps your hands warm
17 Sleep through the winter
21 A unique crystal of ice
22 Direction birds fly for the Winter

Down

2 African American holiday
3 Jack _____
4 Frozen rain
7 House made of ice
8 Time off from school or work
11 Christmas month
12 Gliding on ice
13 Holiday of giving
14 Opposite of hot
15 The coldest season
18 Frozen spikes
19 Vehicle that clears snow from streets
20 Mix of snow and rain