Highlights

Four Brothers Accused of Scamming Amazon for $19M

Four brothers, ages 24-32, are accused of running a fraud scheme out of their parent's basement using their Amazon vendor accounts to manipulate invoice and billing procedures. For example, the complaint indicates they agreed to ship a case of disinfectant spray for $94 but, instead, shipped 7k toothbrushes for $94 each, and billed Amazon $658k. In another instance, a vendor bought one bottle of perfume for $290. They sent 927 units of a plastic beard trimming tool for $290 each, and billed Amazon for nearly $270k. They are charged with attempting to defraud Amazon out of $32M, having received $19M at the time of their arrest.

There are two ways independent vendors sell products through Amazon. They can use Seller Central and/or Vendor Central. Seller Central provides a platform for sellers to direct sell to customers. Vendor Central provides a wholesale arrangement where vendors sell products to Amazon and Amazon resells them to customers. Products are assigned an ASIN, Amazon Standard Identification Number, a string of numbers that serves as a unique product identifier. Using Vendor Central, the brothers swapped ASINs for items Amazon ordered to send thousands of units of items in cases where less than 100 had been ordered. Vendors have access to ASINs in order to make sure product descriptions are accurate.

Even after their accounts were disabled, the brothers tried to create new accounts using fake names and emails addresses and virtual private servers to hide their physical location. They are charged with conspiracy to commit wire fraud, wire fraud, and money laundering.

Amazon created a Counterfeit Crimes Unit to prevent these scams going forward. The group includes former federal prosecutors, data analysts, and investigators. Amazon spent over $500M to counter these schemes in 2019. They are using machine learning to identify anomalies on applications and in-person and video meetings to verify a vendor's identity.

Reddit versus Robinhood

reddit

ROBINHOOD

Digital activism hit Wall Street trading hard with droves of Reddit users slamming hedge funds who were banking on short selling stocks for beleaguered retail companies. The most noteworthy trading revolved around GameStop, though AMC, BB, and NOK were targeted too. Robinhood, touting a reputation of serving the little guy, shut down trading, other platforms increased margin requirements, and basically the system went a bit haywire while social media buzz played an aggressive role in directing users what to buy and to hold tight to drive prices as high as possible. And, even more ironic, Robinhood's response to the crisis, with efforts in direct contrast to their branding, only served to further exasperate the chaos.

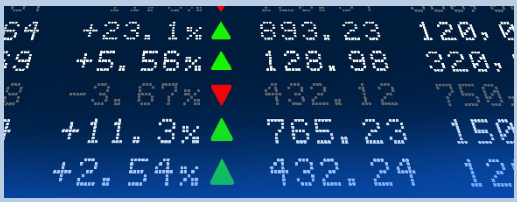
Five Robinhood user experience fails that contributed to the GameStop frenzy:

1) Robinhood wanted to stop users from purchasing GameStop shares, so they removed "GameStop" and "GME" from search results.This created confusion and additional chaos.

2) Robinhood disabled the buy function on the GME stock page and posted a comment – “You can close out your position in this stock, but you cannot purchase additional shares.” Without more information, or the fact this halt would be temporary, users went to social media to vent and banded together in even more aggressive attempts to purchase from them and other trading platforms.
3) Robinhood stopped allowing the purchase of fractional shares, something Robinhood is know for allowing. At some point, Robinhood lifted the ban on purchasing shares but prevented the purchase of fractional shares and limited the number of whole shares that could be purchased.
4) It is not clear whether or not the following happened (there are mixed accounts of what happened) – Users claim that Robinhood created sell orders and were not allowing users to cancel them. The Terms & Conditions do allow this practice, but it is not clear under what circumstances this would apply. Robinhood claims they did not sell shares outside of their standard margin-related sellouts or options assignment procedures.
5) Users wishing to move to another trading platform say they needed a “Statement of Portfolio” to switch but the ability to download the form was disabled. When users attempted to download the statement they received an error message indicating they could email for assistance, with expected responses times of 3-4 working days.

Reddit does not limit discussions regarding stocks. Investors have aggressively utilized social media for years. And, anonymous posts have been directly linked to trading swings. But, the Reddit situation, with digital activism versus a “new” investor is driving a discussion around the “short squeeze”, market manipulation, and whether there is a need for controls.

AI & Stock Trading



"Artificial intelligence is to trading what fire was to the cavemen." An industry player.

High frequency and algorithm trading has moved from 60-70% of trading in 2010 to 90% in 2017. Aidiya, a Hong Kong company, has a hedge fund that performs all operations transactions solely through artificial intelligence. Equity Trading Fund is 100% AI-powered and utilizes Watson's continual learning capabilities to continue to make more accurate predictions.

In a report by the FSB, using AI in the market can also lead to some problems that include decision transparency (when money is lost, who is the responsible party?), systematic risk (volatility leads to more volatility in an AI model), market concentration (vulnerabilities in one area of specialty can impact the system), greater diversity (new volatility without ability to pinpoint cause), and historical data (limited data in a catastrophe may require human intervention to address outliers).

A suggestion is that the optimal scenario is to have AI Systems work with humans side by side to create "Super Money Managers" who pay attention to client's needs as well as understanding both the advantages and the limitations of using AI Systems. Some of the ways companies are using AI in trading is here.

However, while AI is being largely utilized, the proof seems far into the future (don't we need a recession or major market correction to test the stock trading models?), so the links are there for you to browse but we won't go into specific company approaches in depth at this point. Of course, at the pace AI is being integrated into all aspects of our lives, perhaps a deep dive will be appropriate by the next newsletter. It is definitely worth noting the role and extent to which we are already relying on these models.

AI Stocks

NVIDIA

C3.ai

Alphabet

*** Public interest story; not financial advice.

Companies use both machine learning and artificial intelligence to improve products, provide strategic analysis, for training, and to understand processes. There are few pure artificial intelligence companies. C3.ai sells AI software for the enterprise market. Netflix, Intel, Google, and Microsoft have made the largest investments in AI startups. Nvidia, the leading provider of AI chips for cloud computing and other applications, will purchase Arm Holdings, the leading technology provider of processor IP, for $40B. Graphcore, which created the IPU processor for AI compute, raised $222M at a $2.77B valuation and may IPO this year. Intel acquired Habana Labs for $2B. Amazon will offer those chips to its customers. Additionally, AWS has a new machine learning training chip, Trainium.

On the software side, Workday, Coupa, ServiceNow, Five9, and DocuSign have a strong presence in the AI space. Salesforce's Einstein tools improve sales forecasts and for financial services. Its platform delivers over 80 billion AI-powered preditions daily. Alphabet, Microsoft, Facebook, and Amazon are investing heavily in AI. Match, Square, and Trade Desk use AI to drive decision making. Forecasts show AI chipsets and accelerators for edge applications will grow from $7.7B in 2019 to $51.9B by 2025.

"Nvidia will extend its architectures and offer artificial intelligence or 'acceleration in a box' for all ARM-based chips," explains RBC Capital analyst Mitch Steves. "Instead of looking at ARM as potential CPU play along, we think the bigger picture is that 22 billion-plus ARM chips can be accelerated with AI."

John Devine, US News and World Report, recommends the following 10 AI stocks:

1) Nvidia (NVDA): Nvidia plans to build an AI lab in England featuring an AI supercomputer. Nvidia's graphics processing units (GPUs) will also be used to power "Leonardo," the world's

fastest AI supercomputer. Nvidia, high-end chipmaker, provided specialized semiconductors that power some of the more exciting areas in AI, from high-performance gaming to AVs.

2) Alphabet (GOOG, GOOGL): Alphabet uses AI daily to improve its operations, from voice search, digital ad pricing, and relevant search results. Google has been developing self-driving car technology since 2009. Alphabet's autonomous vehicle unit, Waymo, was valued at $30B in its last funding round.

3) Salesforce (CRM): Salesforce's Einstein software uses AI to identify trends, prioritize sales leads, and predict superior marketing copy.

4) Amazon (AMZN): Amazon's Alexa devices have led consumer-facing speech recognition. Search relevancy is very important to the AMZN business, and artificial intelligence helps constantly iterate and improve search results. Amazon Web Services, the leading cloud computing platform, offers machine learning services to customers. Last quarter, AWS operating income accounted for more than 57% of Amazon's overall operating income.

5) Microsoft (MSFT): Microsoft's Azure, is home to AI-driven tools for medicine, language, robotics, and medical. Elon Musk invested $1B in 2019 and founded OpenAI which aims to produce artificial general intelligence (AGI) – technology that can do anything human intelligence can. Recently, it produced a neural network called DALL-E that produces custom images from text. Microsoft will become OpenAI's preferred partner for commercialization.

6) Twilio (TWLO): Twilio makes cloud-based application programming interfaces (APIs) allowing developers to build voice, video and messaging features into their apps.

7) IBM (IBM): IBM is investing profits back into the cloud, data and artificial intelligence and the company has been working with partners including JPMorgan Chase & Co. (JPM) and Daimler AG to discover various practical applications for its efforts in quantum computing in their industries. IBM's Watson technology, famous for dominating "Jeopardy!", is also being put to use in health care, infrastructure, finance and other areas.

8) Facebook (FB): Facebook’s commitment to machine intelligence includes hiring Jerome Pesenti, who led IBM's Watson division, for its AI Research team. Automating self-teaching algorithms to improve Facebook's News Feed algorithm is central to FB's success. Facebook is developing tools like COVID-19 forecasting. It built AI chatbots that unexpectedly began communicating in their own invented language in 2017, forcing the company to pull the plug.

9) Tencent (TCEHY): Tencent uses AI to improve its content, social media and gaming experiences and hopes to sell its AI solutions to the health care, agriculture, industrial and manufacturing sectors. WeChat, an app with over 1 billion daily users, is used in China for messaging, payments, ride-hailing, social media, and mail providing a wealth of data for analysis. TCEHY has recruited top AI experts from rivals including Microsoft and Baidu (BIDU).

10) DocuSign (DOCU): DocuSign uses natural language processing and machine learning to uncover risks in contracts and to accelerates deal flow by cutting down on legal work. In 2020, DOCU bought Seal Software, an AI company focused on contract analytics, for $188M.

How to Secure Your WiFi Router

Keep your WiFi router secure:

1) Use WPA2 security to guard access to your router- it requires every new device to submit a password to connect. Use WPA3, which automatically encrypts your WiFie connection, if your router and devises support it;
2) Change the Wi-Fi password;
3) Change the default name of your WiFi network (SSID)
4) Change the password to access the router settings;
5) Keep firmware up to date – make sure to activate the automatic update feature;
6) Disable remote access, UPnP, and WPS – sometimes these are enabled by default
7) Use a guest network;
8) Keep all devices up to date with the latest software;
9) Be picky about what apps you install;
10) If a device does not need WiFi access, disable it;
11) Enhance protection for the devices most frequently connected to your home network with updated software, security patches, and anitviris security software;
12) Of course, choose strong passwords with numbers, letters, and symbols.

How to Check Your Devices for Stalkerware

Stalkerware is designed for keylogging, location monitoring, internet monitoring, recording audio/video, and taking screenshots. Some clues your device is compromised - reduced battery life, keyboard lag, your phone gets hot even when you are not using it; long shut down or start-

up times, unusually high data useage, sudden pop-ups, active sessions you did not authorize, unauthorized webcam permissions are on for applications.

MSNGroup provides the following steps for detecting and resolving stalkerware issues on your devices:

1) Check your apps list for apps you don't recognize. Of course, the name of the stalkerware is not going to be "stalkerware" – it could be listed as "System Update Service" or something comparable;
2) For Apple devices (iOS) it may also show up as a malicious profile. Go to Settings > General > Profiles & Device Management. If you don't see the last option, it means there's not a mobile device management profile installed on your phone (good news). If you do see it, investigate by clicking "More Details." There should be a "Remove Management" option in the settings. If you find something, it could also be a Mobile Device Management program if your device is owned by your employer, or you use your personal device for work purposes.
3) For iOS, open iCloud drive, click on your username and then iCloud settings and Sign Out of All Browsers
4) Erase and reset your device to remove stalkerware- after you back up your data.

Computer-based spy programs contain keystroke loggers. Third-party security applications like Bitdefender or AVG can be used to spot spyware and stalkerware. For Windows, open up Task Manager and on an Apple machine check out Activity Monitor to see everything that is running. Look for apps using a lot of disk space. Run a web search for any unfamiliar applications.

Prevent stalkerware by using malware software, change passwords, use strong passwords, monitor activity, block installation of third party applications, and enable two-factor authorization.

G2M Research Multi-Vendor Webinar Series

Our 2021 webinar schedule is ready! Click on any of the topics to get more information about that specific webinar. Interested in Sponsoring a webinar? Contact **G2M** for a prospectus.

Our January webinar "Can Your Server Handle the Size of Your SSDs" was sponsored by Kioxia (Matt Hallberg), Lightbits (Josh Goldenhar), and Intel (JonMichael Hands). View the recording and/or download a PDF of the slides.

G2M RESEARCH

Feb 23:	Storage Architectures to Maximize the Performance of HPC Clusters
March 23:	One Year after COVID-19: How Did Storage Architectures Perform for Biotech AI Modeling & What Can We Learn From This?
April 20:	The Race to be Relevant in Autonomous Vehicle Data Storage (both On-Vehicle and Off-Vehicle)
May 18:	Responsive and Efficient Storage Architectures for Social Media
June 15:	It's 2021 - Where Has NVMe-oF™ Progressed To?
July 13:	Computational Storage vs Virtualized Computation/Storage in the Datacenter: "And The Winner Is"?
Aug 17:	AI/ML Storage - Distributed vs Centralized Architectures
Sept 14:	Composable Infrastructure vs Hyper-Converged Infrastructure for Business Intelligence
Oct 12:	Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
Nov 9:	The Radiometry Data Explosion: Can Storage Keep Pace?
Dec 14:	2021 Enterprise Storage Wrap-up Panel Discussion