Title: I did the Plaid Share Verification because I liked what this ape had to say, and I am relatively sure the number of verified shares are ALREADY more than the true float. If I am wrong, then so be it. I was probably doxxed a long time ago, anyhow. ■
Author: disoriented_llama
Created 2021-08-04 01:55:43 UTC
Permalink: /r/TheGloryHodl/comments/oxiddx/i_did_the_plaid_share_verification_because_i/
Url: /r/amcstock/comments/oxgnfj/a_cyber_security_professionals_input_on_say/

Linked Post Content:
TL;DR at the bottom

DD has now been covered on Randall Cornett's channel on YouTube
[link](https://youtu.be/W1T_pf0Gd30)

Good afternoon, Apes

Something very important is currently going on with $AMC that, if you aren't aware, could have a substantial effect on the MOASS, and we can all have a direct impact.

If you have not heard, u/einfachman pointed out in [this post](https://www.reddit.com/r/amcstock/comments/owgqec/adam_aaron_is_a_beautiful_genius_do_you_realize/) that Adam Aron's recent decision to announce a public Q&A; presents us with an opportunity to **publicly count our shares**.

This is made possible through "[Say Technologies](https://www.saytechnologies.com)", a company that facilitates retail investor Q&A; sessions during earnings calls for small cap companies. Typically, it has not been feasible or necessary for large companies like AMC to host a Q&A; for retail investors; however, due to the massive interest from retail investors in AMC, it would seem they found a reason.

Why are we even taking a vote twice? Why does it matter?

Many apes do not realize that "Proxyvoting" services like through DF King & Co., are not allowed to make public statements regarding overvoting, which would otherwise be legal proof of naked shorting. This is due to SEC rulings and laws surrounding insider trading and making unsubstantiated claims of fraud which could land AMC and its executive staff in hot water with the law--especially if those figures are subject to an ongoing investigation by the SEC.

As a result, even though there may absolutely be naked shorts, and even though Adam Aron and his staff may know that the number of votes they received during the shareholder meeting were sketchy as hell, they are legally bound to keep their mouths shut. In my opinion, this only further cements the fraudulence of our markets, but nevertheless, there is a loophole.

If AMC investors connected through a **legitimate organization** (such as Say Technologies) which was capable of verifying legitimate shares of the company, and the following applies ...

1. This company does not materially benefit nor does it possess any conflict of interest in regards to the number of votes collected
2. The company does not receive nor disseminate substantial, non-public information through its services
3. The company publicly provided the number of shares/votes cast to discuss any non-specific issue regardless of outcome
4. The company does not hold any stake or incentives for disseminating or publishing that vote count

... then that organization is not obligated by law to withhold the vote count for any reason.

Say Technologies is a legitimate company that legally do this with no repercussions to either AMC, AMC's staff, AMC's investors, or itself.

This is another vote count, and this time, we get to know the **real** numbers as they come in.

So what's the problem? FUD... lots of it

Since this vote service came out, I have seen literally hundreds of comments and tweets claiming that this is a trap. That AA is trying to scam us somehow. That somehow by signing up for this vote service will result in shares being stolen. That this is will hurt the squeeze.

Comments like [this](https://www.reddit.com/r/amcstock/comments/ox0ie3/the_ceo_gave_you_the_tools_to_trigger_the_short/h7km3mw/?context=3), which cite legitimate privacy concerns...

Baseless [fear-mongering](https://www.reddit.com/r/Superstonk/comments/ox2lip/looks_like_steve_is_on_an_evil_mission_of/?utm_source=share&utm;_medium=ios_app&utm;_name=iossmf) like this, which attempt to incite terror and prevent apes from getting their shares counted by convincing them of a ploy to steal their shares...

False information based on lack of understanding of how Say Technologies/Plaid manages data...

https://preview.redd.it/03824uahr7f71.png?width=300&format;=png&auto;=webp&s;=006ffcb372a039eb2afadc317b6c89c1a033c350

All of these examples do not take into account for the absolute mountain of legal and financial regulations that ensure such things to not take place.

Whether it is legitimate fear, or FUD being spread, I am here to settle those fears and squash the FUD.

For once, I am actually an ape that knows what he is talking about, whose entire career revolves around the topic of data privacy, security, and risk management.

I'm not a financial advisor, but I am an infosec professional

This may perhaps be the only thing I can actually say I am qualified to speak on as an Ape. I am an information security consultant. It is my job to assist my clients in securing their data, applications, networks, and computers systems. Specifically, I am a penetration tester. I test the security of applications, networks, and systems by actually hacking them.

Part of my job requires me to be extremely familiar with and be able to interpret the regulations which companies are subject to, especially when their apps, networks, and systems handle bank or credit card data. For that reason, I am certified and qualified to test and advise my clients on how to secure applications and APIs, just like Plaid, which is what Say Technologies uses.

What is Say Technologies?

Say Technologies is, in the simpliest terms, a proxy-vote service.

They operate very similarly to companies like D.F. King & Co., who are tasked with taking shareholder votes in order to allow shareholders to vote during shareholder meetings for companies in which they own stock.

Unlike D.F. King & Co., however, Say Technologies exclusively provides the service of giving retail investors a platform to submit questions for earnings calls to ask their clients' whose companies retail investors own stock. Their entire business model revolves around the task of collecting shareholder votes by verifying their stock holdings through their respective brokerages. Therefore, it is important for them to support as many brokerage firms as possible.

How did Say get started? Who are they?

Say Technologies was started by a gentlemen by the name of Alexander Lebow and his Co-Founders, Julio Fredes, Zach Hascoe, and Jeffrey Crutenden (who also co-founded Acorns). Here is their LinkedIn [company page](https://www.linkedin.com/company/saytechnologies/) and [employees page](https://www.l

inkedin.com/search/results/people/?currentCompany=%5B%2211540073%22%5D&origin;=COMPANY_PAGE_CANNED_SEARCH), so you can connect with them and look into their backgrounds and career experience.

You can actually learn everything you want to know about them from a fantastic [podcast interview](https://medium.com/wharton-fintech/podcast-with-alexander-lebow-co-founder-of-say-eb9fbe829a0e) with Alex Lebow on Medium.com. Alex Lebow used to be a Mergers & Acquisitions Lawyer before he and his co-founders realized that there was a problem with the democratic process of corporate governance, in that retail investors *rarely* get the opportunity to vote on how companies they invest in do business.

[Sorry, this is a screenshot. I ran out of characters ■](https://preview.redd.it/0yn1gsaq7ef71.png?width=486&format;=png&auto;=webp&s;=86382cf67b5e775b27168392801225660 3b21c93)

What data does Say get and what do they do with it?

Here is the [privacy policy and disclosure](https://saytechnologies.com/privacy) page on their services site, but I will draw your attention to specific areas of what information is collected. I would encourage you to read this disclosure in full detail so that you can fully understand what you are agreeing to provide when signing up.

[Information you provide to Say Technologies](https://preview.redd.it/sbj2njhjv7f71.png?width=646&format;=png&auto;=webp&s;=b89bd6d84c58853981c8041b7bfc227ff1015e40)

This is specifically what you agree to divulge to Say Tech directly. Say Tech asks for contact information, questions you wish to ask companies in which you hold stock during earnings calls, and votes which you are submitting using the voting power of your shares.

[\(Shareholder\) Information that Third Parties \(Plaid\) retrieves on behalf of Partners](https://preview.redd.it/4tewbow5w7f71.png?width=644&format;=png&auto;=webp&s;=d47092e46d4fc60406b67aa01f4180a3c3a847df)

The above is what is collected by a service called [Plaid](https://plaid.com/), which is a Web Application Programming Interface (API), that allows banks and financial institutions to authorize direct communications on behalf of account holders. This includes your share details, trade history, account fund/share balance, and the contact information which you used to sign up with your broker. This is for the purpose of counting and verifying your shares to determine voting power, and additionally to supply contact information which can be used to reach you in relation to the shareholder voting services.

Who is Plaid, what do they do?

Plaid is the organization which facilitates bank-to-bank exchanges of information to customer accounts through the use of its API.

The purpose of Plaid is to make it easier for financial institutions to act in the interests of their customers who possess multiple accounts between them. Many financial applications like Robinhood, CashApp, Venmo, or Mint, for example, use Plaid in order to connect brokerage/individual accounts to a primary bank account, which allows customers to do things like view statements, check account balances, review transaction history, and transfer money between accounts.

Why does Plaid use my bank credentials?

As mentioned in this [FAQ response](https://my.plaid.com/help/360043065354-does-plaid-have-access-to-my-credentials) as well as in Plaid's [End-user privacy policy](https://plaid.com/legal/#how-we-use-your-information), Plaid provides

an API which sometimes collects your bank/broker credentials for the express purpose of proving account ownership and authorization for information access.

Before you panic, it's important to recognize that, in accordance with an incalculable amount of legal paperwork, **your credentials cannot and will never be divulged to anyone**.

As an information security professional, I can confidently say, Apes who are afraid to share their credentials are wise to be skeptical. You should only ever share credentials with organizations you trust. Therefore, let us first determine whether or not Plaid is trustworthy.

Plaid does not store credentials permanently. In most cases, especially with partnered organizations and financial institutions such as J.P. Morgan Chase, Key Bank, Bank of America, and many other financial institutions, Plaid works directly with the institution to provide a direct API with which Plaid can engage in customer banking on behalf of the customer through their application services.

[Plaid's official statement on the access & storage of user\/customer credentials](https://preview.redd.it/8qbujfdd88f71.png?width=942&format;=png&auto;=webp&s;=475bb2ccd393ad157dd684834ef179ec700798c9)

How does this work. How is it secure?

[Sorry. Another screenshot cuz out of room for text](https://preview.redd.it/uf01xs948ef71.png?width=483&format;=png&auto;=webp&s;=7708a97ea39f6c34043625261c04c91687c157a5)

If Plaid must store your credentials permanently... it is done in such as way that it uses a special form of storing them called "[password hashing](https://auth0.com/blog/hashing-passwords-one-way-road-to-security/)." This is a special way of converting your password, such as "password1" into an irreversible string of garbage, like this example SHA256 hash of "password1":

`0b14d501a594442a01c6859541bcb3e8164d183d32937b851835442f69d5c94e`

The only way Plaid can check your password is by asking you first. Then, it uses the same conversion on the password you sent, compares that to the hash Plaid has stored in its database, and finally permits access to the institution in question.

>Note: This is not an exact description of how Plaid itself works, but more a general description about how secure password storage works. I am not privy to such information, since such knowledge would be considered classified and highly privileged. In addition, Plaid most likely uses additional protections such as database encryption, hash salting, and other techniques that cyber-security aficionados like myself could talk about for days, so we won't go into more detail than that.

In all remaining cases where the institution does not support Plaid at all, plaid simply does not support them. There must be cooperation, or else it doesn't function at all. There are no compromises here.

Lastly, Plaid takes things a step further by securing your account with two-factor authentication. This is when you try to log into a bank or something, and Plaid sends you a text message with a temporary code to your cell phone to prove you are who you claim to be.

Even in situations where someone gets your password, they also must have you phone, and so adds more difficulty for someone who is looking to steal from you. Not an easy thing to do.

Without both passwords and the SMS/2FA authorization, Plaid's API simply does not work for the entity requesting access, and any such access can be revoked at any time by the customer--You.

Why do they do it this way?

The reason Plaid does things this way is because storing banking information is something the Payment Card Industry Data Security Standard ([PCI DSS](https://www.pcisecuritystandards.org/pci_security/)) regards as a cardinal sin. **Storing credentials in plaintext (not encrypted) is an extreme security "no-no" which puts it in the crosshairs of one of the most powerful entities of the financial world--Credit Card issuers**. Specifically, these companies are Visa, Mastercard, Discover, JCB, and American Express. And if your company/organization falls under PCI compliance, and you violate that compliance, then they will fine the absolute living shit out of you until you get back in compliance. This is not negotiable.

Specifically, Plaid falls under a specific piece of the PCI DSS called PCI-PA (Payment Application) certification.

Any organization that wishes to get this certification this must undergo a regulatory gauntlet of audits and security testing, unleashing guys like myself who break into the organization and steal data from it in any way possible. If we find anything wrong, auditors mark the organization as "failed" on their "Report of Compliance". To fail a report on compliance puts you on the issuing banks' shit list and prevents you from executing your services on behalf of your customers, lest you face fines and lawsuites.

The five credit card issuers can force any organization under PCI to pay massive fines for violating the PCI DSS regulations in a way that results in the mishandling, misuse, or unauthorized disclosure of **any** banking or credit card data. As such, there is a specific regulation that applies to Applications and programming APIs like Plaid which are used by FinTech to access banking systems.

As an added bonus, any company that uses Plaid's API is *also* forced to comply with PCI in order to do business, which means they *also* are forced into a position of not pissing off the issuing banks, lest they face fines and litigation because they did something that caused them to implement Plaid in an insecure way... and that doesn't account for situations where those at fault would be forced to pay damages for anyone who lost money as a result of their negligence.

This industry, despite how corrupt we might think it is, is scrutinized more than any other because of just how deeply self-regulated it is by banking institutions. Anyone caught violating banks trust, especially if it results in a loss of data privacy, or worse a financial loss due to a security breach or negligence, the ramifications are instantaneous and severe.

What happens if Plaid is compromised?

In addition to being regulated by PCI DSS, Plaid is subject to all laws and regulations that apply to the [FDIC](https://www.fdic.gov/resources/regulations/), the [Bank Service Company Act](https://www.aba.com/banking-topics/compliance/acts/bank-service-company-act), and [all of the federal statutes and all supplemental laws that fall under it](https://www.rivialsecurity.com/blog/bank-pci-compliance). This is because Plaid is technically considered a financial institution that provides banking services.

In addition to that, any company that uses Plaid is subject to the same laws and regulations **in addition to local/international laws if they are outside the United States**. So if you are in the EU, for example, and you were upset that your data was being misused by Plaid, you could file a General Data Privacy Regulation (GDPR) compliant, which states that all companies that service EU-nationals are duty-bound to irrevocably destroy any and all data associated with that individual.

Violators of these laws that result in a failure of compliance are subject to **massive fines** in the millions to billions of dollars, proportionate to the losses and damages sustained by organizations and their customers who use the service. Plaid is trusted by FDIC insured institutions all over the world, and if something were to happen to Plaid where it resulted in a monetary loss, those losses would be covered by the FDIC insured institutions and guaranteed for up to $500,000 per account.

Meanwhile, Plaid themselves would be sued out of existence by every affected bank and institution as a result.

It is not an exaggeration to say that, if the worst should happen, and Plaid was not only compromised but also if **its millions of customers had their banking credentials stolen** as a result of their negligence, then **they would cease to exist as a company** because of the resulting damage.

Can Plaid send my credentials or shares to a hedgie?

In short, no, **absolutely not**.

Sharing of banking information between financial institutions without the express consent of their customers is regarded as a violation of fiduciary responsibility, *numerous* federal laws, and would permanently destroy their reputation and business beyond repair. At such a level of trust violation, the FBI becomes involved instantly, and anyone involved in this magnitude of fraud against numerous banking institutions and their customers would land everyone in prison for a minimum of 20 years.

If something like this were allowed to happen, it would annihilate all faith in the United States banking system. Plaid operates under a fiduciary responsibility in the sense that they are obligated to protect all of their customers' banking information from any and all unauthorized access, except with the express consent of the customer or by a legal warrant or subpoena by U.S. courts pursuant to a criminal investigation and legal proceedings.

Further to this point, Plaid does not have the power to authorize transfers of shares to begin with. Only the financial institution itself has the ability to do so, which must be authorized by both the sending and receiving bank via ACH or wire transfers. In the event of such a transfer, it is highly likely you would be notified before it took place, and have every opportunity to notify your bank/broker that the transfer was not authorized, prompting a fraud investigation.

You'd be surprised to find that you probably already use Plaid

Plaid and it's API is used by hundreds of financial institutions, including many brokerages and banks. If you have ever "linked accounts" with any of the following institutions, then you have trusted plaid with your data before:

* Chime (banking/budgeting app)
* M1 Finance (banking/budgeting app)
* Mint (banking/budgeting app)
* Simple (banking/budgeting app)
* Varo (banking/budgeting app)
* Acorns (finance/investments)
* Credit Karma (finance/investments)
* Digit (finance/investments)
* Ellevest (finance/investments)
* Qapital (finance/investments)
* Venmo (ACH/fund transfers)
* PayPal (ACH/fund transfers)
* Wise (ACH/fund transfers)
* Metal(ACH/fund transfers)
* SoFi (loans)
* Figure (loans)
* Avant (loans)
* Petal (loans)

If any of these ring a bell, and you've authorized a log-in through their services to connect one of your bank accounts, then you've used Plaid.

Can I revoke Plaid's access?

Yes. The easiest way to do this is to simply change your password for the financial institution you allowed

Plaid to access.

You can also register an account with Plaid to check which applications you used to sign up with your phone. You can create an account with your phone that you used to set up any past connections with Plaid.

In fact, this is actually a **more secure** thing to do, because if you do not create a plaid account, then someone with access to your phone could technically create an account on your behalf to gain access to your Plaid account information. Not that there is anything there to take, since Plaid doesn't store any private information in your Plaid account other than a list of the applications which you have authorized.

Point72 / Stevie Cohen's investment in Say

Virtually all of the FUD surrounding Say hinges on the argument that Point72 Ventures, a venture capital-focused hedge fund owned by Steve Cohen's Point72 Investments, [made a seed investment](https://www.barrons.com/articles/point72-backed-start-up-to-rock-the-proxy-vote-1523363755) of an undisclosed amount but no greater than $8M back in 2018 during Say's start-up funding period.

While you can believe what you want to believe, that all things are connected and that because Steve Cohen is involved in investing in the company that somehow this means this is a trap, carefully orchestrated by Adam Aron to betray all retail investors... that is one paranoid delusion that goes a bit too far.

Point72 invested in Say. Ergo, they own private equity in the firm. Yes, that is true. They invest more than 20% of their investment portfolios in the FinTech industry, including start-ups. It's not surprising.

This does not mean that Point72 has the ability to access privileged information that is protected by federal banking and privacy law by default. They, in fact, probably have little to no material interest in the data itself, since they have far greater access to market analytics and privileged information than what we could hope to imagine.

As an investor that is part of this movement, I can sympathize with the feeling that the entire market is stacked against us--and it is, but in cases such as this, access to someone's banking data is so highly privileged and guarded that the banks themselves, not to mention the Consumer Financial Protection Bureau (CFPB) and US DOJ, would drive a crusade of massive litigation designed to crush the violators, halt the data leaks, and put the company's responsible staff in prison for wiretap fraud, data theft, and bank fraud.

Further to this end, there have been completely unsubstantiated rumors that this would allow hedge funds to somehow steal shares or enable lending programs without customer consent. Violations and crimes against banking data, customer accounts, and the US financial banking and treasury system are some of the most guarded and vehemently litigated in the world. Violators rarely get away with it. Additionally, in accordance with the [FDIC](https://www.fdic.gov/consumers/privacy/yourrights/index.html) and the [Gramm-Leach-Bliley Act](https://www.sapling.com/5679388/access-bank-account-information), customers are entitled to full disclosure of where and how their data moves through any companies that handle their bank information. That data doesn't move anywhere without someone knowing exactly where it is or who has access to it.

Here are just a few cases where such actions on customer accounts, led to federal probes and prosecution, law suits and jail time:

* https://www.sec.gov/news/press-release/2020-158
* https://en.wikipedia.org/wiki/Wells_Fargo_account_fraud_scandal
* https://money.cnn.com/2005/05/23/news/fortune500/bank_info/index.htm

The events of these scandals have a dramatic effect on the banks they effect, often resulting in millions and billions in losses, less so from the litigation itself, and more because of the damage to their reputation

and loss of customer trust.

Individuals, banks and investment firms that find themselves on the wrong end of a data fraud investigation seldom survive. Wells Fargo was the exception here. Nevertheless, regardless of whether Point72 and Say were somehow in cahoots to siphon all this data for some unknown market advantage, it probably wouldn't matter anyway because...

The unfortunate reality is that your data is already very accessible anyway

As a professional in the infosec industry, it saddens me to tell you that your data is probably already out there regardless. It is highly unlikely that Say is selling your brokerage information, given their responsibility to all the aforementioned data privacy laws and regulations. However, it doesn't really matter because banking data is openly traded on the dark web regardless for pennies on the dollar.

Your personal information and bank account is probably already easily accessible via darknet database dumps that have either leaked or sold your bank account and routing number long ago, and that includes brokerage accounts.

In fact, your bank account can be queried at any time using [SWIFT](https://www.paiementor.com/swift-mt940-customer-statement-detailed-analysis/) without needing your login username or password. This is because SWIFT is a system used internally by banks for direct bank-to-bank account queries, balance and transaction history, and even direct transfers. Even hedge funds have access to SWIFT for the purpose of handling their customer's investment accounts and completing deposits and withdrawals on behalf of their clients.

Despite its legitimacy and long-standing use in the industry, SWIFT is a very old system held up by bandaids and toothpicks. [It has been around since the origins of digital banking in the early 70s](https://www.swift.com/about-us/history), and now it is so widespread it is accessible and broadly used by the entire financial world across the globe.

Access to it is trivial for a legitimate financial institution, and it is largely untested by the infosec world. It is a mystery ladened by countless Non-Disclosure Agreements and threats of litigation for anyone that talks about it in terms of security for fear that such disclosures might lead to a breakdown of the security of the system.

We in the industry call this "Security through Obscurity" and it rarely plays out well, and unfortunately, [access to SWIFT is both trivial and totally insecure](https://www.accellion.com/secure-file-transfer/swift-security-vulnerabilities-bank-data-breaches-are-the-future-of-bank-robberies/). The worst part is SWIFT isn't the only method that is used, and most of the other methods aren't really any better, SWIFT just happens to be the most well-known that you have probably heard of at one point or another.

So what I'm saying is... **even if somehow our brokerage/share information and the bank accounts we link with SayTechnologies was relevant to evil hedgefund's magical strategy to rob us blind, it doesn't really matter because it's accessible with or without them.**

The financial world is mired in a litany of horrendous insecurity, and the sad fact is that Plaid is probably a hundred times more secure than SWIFT because:

1. It actually requires legitimate credentials. SWIFT's credentials are the bank ID you are sending the message from...there is no other validation.
2. Every action requires an authorization token for each time an institution wishes to access another's account. SWIFT doesn't do that...
3. Plaid supplies the security of its framework and is financially responsible for any negligence or loss of data that occurs through the use of their platform. SWIFT isn't responsible in any way. They say "it's the banks' responsibility to secure their SWIFT system"
4. Plaid has multi-factor authorization on all user accounts and allows full user/customer control and visibility of what institutions have access to their accounts. SWIFT don't give a fuq who accesses shit cuz it ain't their problem... bitch.

So ultimately, if a hedgefund wanted to access your brokerage information, violate all these laws, and commit financial and legal suicide by maliciously accessing millions of apes' accounts without authorization just to count how many shares they have... they can already do it. They don't need your permission. They can pay someone to give them access some other way, and we would never know about it.

It's an insecure world out there. The sooner we accept that, the sooner we can start doing something about it.

Can I really trust SayTechnologies, Plaid, or AA for this vote?

Honestly, you have to decide that for yourself. **I trust them, and I'm paranoid to unhealthy levels**. I don't like signing up for anything. I don't like sharing my information with anyone. But I also accept that my information may as well be catalogued at a public library, because anyone who wants it can get it from somewhere, and it wouldn't even be that hard. The networks and control systems of our financial markets are terribly fragile and insecure. I know ... I've tested some of them. You don't know how bad it can really get or how easy it is...

The simple fact is Plaid is about as trustworthy as any bank. If you don't trust banks, then you must have your money stored in a mattress, which I would say certainly protects your privacy, but exposes you to many more severe and likely risks.

You should read Plaid's disclosures yourself, and do your DD as you have done before.

However, please consider this...

>**Casting your shares in a vote to get a REAL share count is probably the only thing we as retail investors can do to prove that naked shorting and synthetic shares exist.**
>
>**Unless the SEC publishes the results of an investigation that may not even currently be happening, then we will never know--and maybe not even then.**
>
>**This is something we can do right now to prove that naked shorting has been happening, but it will only work if we do it together.**

TL;DR

SayTechnologies uses a well-known, trusted, and widely utilized API called Plaid to access your brokerage accounts securely. This is only done as a means to count your shares so that they can be used to cast a vote on SayTech's website.

It cannot be used to steal shares. If something like that were to happen, it would quite literally destroy confidence in all the banks partnering with Plaid, and their reputation as banking institutions.

I can attest to Plaids security because I work in the Information Security industry, and I have personally experience in testing applications which in my work as a penetration tester to prove that it keeps customer's data secure. I understand how it works, and I have examined applications which use Plaid to transmit credentials and bank information. I am deeply familiar with the regulations and laws which force organizations to prioritize security and privacy of customers' banking information.

I am willing to accept this small risk of logging into Plaid's service and to [cast a vote](https://app.saytechnologies.com/amc-2021-q2/) on saytechnologies.com to add my shares so that we can see how many shares **really** exist in the hands of retail investors.

This is something that we can do to help the squeeze, but only if we do it together.

Apes together strong.

P.S. / Q&A;

Feel free to ask me anything about any of the above. I am happy to talk about cyber security, PCI DSS, and any of the laws as they relate to information security. I live and breathe this stuff. It's my career, my hobby, and my passion. There are no dumb questions. Feel free to reach me on twitter too, [@TRUExDEMON](https://www.twitter.com/TRUExDEMON)

Edits / Corrections:

>8/4/2021
>
>I made the statement that Visa merged with Plaid. Unfortunately, this was inaccurate as of January 2021, due to an anti-trust action by the US Department of Justice which halted the merger pending litigation that began in November 2020. Visa and Plaid decided it wasn't worth the hassle to face the DoJ in court and abandoned the merger in January 2021. I have removed this claim as a result. Thanks to u/69deok69, who was the first to point this out to me.
>
>Addressed the Point72 information
>
>Included sources/facts that your bank information may as well be on fucking Google, because anyone who wants it can get it anyway. Sorry... but it's true...