AuthID ($AUID)

A Skewed Return Distribution with Huge Upside in a Growing Market

Overview:

When was the last time you went a month without hearing about a huge technology breach? We've seen identities stolen when usernames and passwords were posted to disreputable corners of the internet. We've seen hospitals shut down by hackers who demand payment to return patient records, or to turn on medical equipment they've disabled. When was the last time you went a month without having a problem logging into a site or app you frequently use because you couldn't remember the password? As you read this, do you know the password for your work and personal email addresses? If you had to change them, do you know where to log in to do so? When was the last time you went a month without getting locked out of an account because the system couldn't authenticate you? The process of calling the company, waiting on hold, and explaining the situation to customer service could take an hour if all goes well.

Companies are hacked and breached every day. Individuals have their data and identities stolen every day. Passwords, which are either impossible to remember or insecure, are a daily source of friction in our lives.

Even the constantly touted two factor authentication (2FA) has an incredible flaw. Imagine that someone steals your phone and tries to access your bank account. The thieves don't have your password, so they request a password reset. Because the bank is using "best practices", they will probably send at least two of the following: an email, a text message, and/or a code to an authentication app. The problem with all of that is if someone has your phone, they also have access to your email, text messages, and your authenticator app. Even in situations where

someone doesn't steal your phone, cloning a SIM card (the little chip in your phone which identifies your phone number and information) is far too easy.

I've done many expert calls in the authentication and security space, and there is near-universal agreement that the next step in securing your accounts is biometrics. Fingerprints are better than passwords but can be copied. Voiceprint was highly accurate until inexpensive AI made it easy for thieves to copy your voice and match any required voice prompt. Retina scanning is very accurate, but difficult to perform with a high-end cell phone and impossible with an older one. Active selfie where you put your phone in front of your face and then perform acts like turning your head or sticking out your tongue is an accurate method of authenticating identity but take a lot of time creating friction and frustration for end users and customers.

In almost every call I made, experts thought the next wave of security improvements would be passive face identification with liveness detection. That means you'd put your phone in front of your face, and the authentication process would match your face to the image on a government ID you provided when you set up the account. The system checks to ensure that the image is of a live person instead of a photo of a photo. There is also a back-end check to ensure you are using the phone's camera instead of using an AI image and replacing the data stream (called an insertion attack). AuthID can authenticate your image, do a liveness check, and scan for an insertion attack in just over half a second.

Biometric security is going to be a huge market, and right now, AuthID has one of the fastest solutions available. That's the opportunity. **This stock could be up 10x in the next 5-6 years. There's also meaningful risk, and I intend to cover them in detail in this report. Please read the risk section before committing capital.**

Security is a Tradeoff and Buyers Have Made Their Choice:

I travel frequently. The last time I entered the US, I presented myself to immigration and gave the agent my passport. He checked my identification and then used a basic webcam to take a

photo of my face. While I didn't have access to his side of the computer monitor, it's a reasonable assumption that he was ensuring my passport was valid, and that I was the person who matched both the passport and whatever identifying information the government has for me. In just one to two minutes, he authenticated me and invited me to officially re-enter the US. I was at baggage claim long before my bag was. Under the circumstances, that's a great experience. Last time I visited Thailand, they took my fingerprints, but still got me through immigration before my bag arrived. Again, that's a win. Because I present myself in person, there's no need to do a liveness detection or check for an AI insertion attack.

I suspect almost all of you would agree that getting through immigration before your bag arrives is great. Now, imagine it took you one to two minutes to unlock your cell phone. Imagine it took a minute to open your banking app or your work email. In that situation, we'd either throw the phone against a wall, or stop using it. Speed and a user-friendly interface are crucial for adoption in the consumer hand-held market. AuthID authenticating accurately in under a second meets that standard.

When I started researching the biometric security space, I thought purchase decisions would be made based on accuracy. Whoever had the best, most accurate technology would win. It turns out that's not the case. The people who purchase biometric authentication systems are more concerned about losing customers and providers than they are about accuracy. I've heard of cases where 10% - 20% of initial account setups fail. Many of them fail because people have difficulty taking a photo of their identification or are using an older cell phone and the image quality is too low.

As a hypothetical example, imagine you wanted to rent an AirBnB for an upcoming trip. If they required biometric authentication and you had enough difficulty getting the system to process your ID, you might just book a hotel or go to Vrbo. If you wanted to drive for Uber, and there was too much friction getting your account authenticated, you might just decide to drive for

Lyft instead. Losing 10% of your potential customers or vendors is a non-starter for most companies. They'd rather take the risk of getting hacked.

The winners in this space will have a fast frictionless user experience and a fantastic sales team. Right now, $AUID is focused on being the fastest solution using facial identification. As of today, that's the best solution when considering accuracy and speed while limiting user annoyance caused by asking them to perform acts for the camera.

Total Addressable Market (TAM):

Someone recently asked me what the total addressable market is for biometric security. I asked him to look at his cell phone and pick out how many apps he'd pay $.50 to secure. The easy answer was email, banking, brokerage, LinkedIn, and other social media used for work. Now, multiply that by the number of cell phones. The decision to use higher-level security and to pay for it will come from the companies involved, and won't be made on an individual level, but it's a helpful exercise to determine an appropriate level of interest.

Uber and Lyft should be using biometric authentication for both their drivers and riders. AirBnB should be using it for both hosts and guests, especially when there is shared space. Dating apps which facilitate moving people from online conversations to meeting in person **should definitely be using** authentication for personal security.

Any company that allows off-site work should be using biometric authorization. Imagine paying a programmer to complete a task. That creative programmer could potentially find an inexpensive outsourced programmer to do the task for him. In order for the outsourced programmer to do the work, the lazy employee needs to provide his login information. Now, the non-employee programmer has access to the data and systems of the company. That's a massive security problem due to malfeasance that passwords can't solve. Biometrics would solve it by ensuring that the person with access is the actual person who is supposed to have access.

Hospitals and hotels have been hacked, and the hack almost always comes from authenticating a user who shouldn't have had access. Shutting down a hotel can ruin a brand. Shutting down a hospital can ruin lives. A stolen username and password can sometimes be enough to provide a bad actor access to internal data and systems.

Every one of the above categories of potential customers is ideal for AuthID's fast user-friendly solution. Spend five minutes on this, and you'll think of five more relevant use cases.

The Short Case:

I intend to go over the risks involved in investing in AuthID, but let's start with the most successful detractors of the company. $AUID is a micro-cap company with 9.5MM shares outstanding and a current market capitalization of just under $70MM as I write this. About 75% of the shares are owned by people who have financed the company in both the early years and in last year's capital raises. Those investors have no interest in selling at anything near the current $7 stock price. That means the active float for the company is around $20MM. This is a tiny amount and any buying or selling has an outsized impact on the stock price. The short interest was 263k shares as of the end of March, and I suspect is higher right now. Criticism from short sellers combined with a sizeable short interest relative to typical trading volume means they have influence.

Many people despise short sellers and complain that engaging in the practice is immoral. I disagree. I've shorted stocks for decades, and don't particularly care if someone buys then sells, or sells then buys. The $AUID short sellers have every right to take a position and explain in public their reasons for doing so.

Further, let's give these people additional credit. They've been right! The company has been public for years and in 2021, the stock price was around $120. Last year, AuthID had to raise capital three times to avoid bankruptcy and had to do a reverse stock split to avoid being

delisted. Over the past few years, the short sellers have nailed this situation and made a lot of money in the process. Short selling is hard, and I compliment them on their success.

Because I take them seriously, I'm going to try to explain their case against the company. If you are a short seller in $AUID, and you believe I've missed something, misunderstood something, or misstated your case, my email address is IR@DeepKnowledgeInvesting.com. I'll read whatever you send, and in the event that I've misstated your position in any way, will be happy to revise.

A History of Failure:

This is the area where the short sellers nailed their case. AuthID was incorporated in 2011, has had a string of ineffective CEOs, and last year, had $200k in revenue. Prior management has been terrible, and one former CEO wanted to go to dog parks to sign up people walking their dogs. Leaving aside the questionable case for dog walker biometric security, that's not a scalable business model, nor is it one that recognizes the massive TAM of the field.

Here's what changed: Last year, AuthID brought in Rhon Daguro as the new CEO. Rhon was the Chief Revenue Officer of competitor, Socure, where he grew revenue from a few million to over $100MM and signed 1,200 customers. Rhon is building and training a new sales force which is his area of expertise. I agree with the short sellers that prior management was horrible. I don't agree that this criticism applies to current management.

Poor/Misleading Communication About Financial Metrics:

The short sellers have complained about the company's use of the words "bookings" and "sales". Much of this relates to a term AuthID has used in prior press releases called bARR which stans for Booked Annual Recurring Revenue. The problem with bARR is it includes both booked, or contractual revenue owed by customers, and also includes estimates of future revenue from those customers. When you include "booked" and "estimated" in the same term, it's going to

cause confusion. In fairness to the short sellers, I had the same reaction when I saw the definition of bARR.

Fortunately, I've had the opportunity to spend hours talking with new CEO, Rhon Daguro, and CFO, Ed Sellitto. About half of bARR consists of contractual obligations from customers, and about half is an estimate of future usage above the contractual minimum. I will provide clarity on how this works later in this report and break out contractual obligations and estimated additional usage in the model included below. I will show you how these numbers are calculated one component at a time.

I believe this issue was created by imprecise communication rather than a lack of integrity and honesty from the management team. The good news is the company now understands why bARR should no longer be used, and I expect them to start reporting component data. AuthID will not be changing their financial metrics and accounting; but rather, will start providing additional disclosure to make it explicitly clear how they are arriving at revenue guidance.

Bad and dishonest management teams "solve" problems by aggregating data and obfuscation. Good and honorable management teams solve problems with more detail, more disclosure, and more clear communication. Both the short sellers and I will be watching closely how Rhon and Ed handle this in the future.

<u>No Use Case:</u>

A recent report by a short seller indicates they believe "selfie identification will never be the second factor of authentication". They think that behavioral analysis will be what's used. My research turned up several experts who think behavioral analysis like the angle you hold your phone, how fast you type, and way you walk will be a piece of what's used to authenticate people. They believe, and I agree, that behavioral analysis will be a potential second factor. The most likely next scenario is one where you use a live selfie to authenticate yourself and gain access while behavioral analysis monitors you. If you gain access, but your actions differ from

your typical baseline by a large enough margin, the system will flag your account and issue a challenge. You might be asked to re-authenticate using a selfie, to put in a password, or to call someone at your company who could assist in either authorizing your continued access or cut off the access of someone committing fraud.

I think the idea that there will be no use case for biometric authentication is not credible; especially face ID which is the current best option for accuracy and ease of use. In the introduction and total addressable market sections of this report, I listed many different use cases. At a minimum, users in health care, hospitals, and hospitality tend to have a limited number of fixed workstations that are shared among several members of the staff. There's no behavioral analysis possible in that situation that would allow authentication. Currently, most of those systems use either a password or a keycard. If you've ever seen a spy thriller, part of the plot always involves stealing someone's key card to gain access. With no possible behavioral analysis at a shared workstation or entry to a secure facility, wouldn't a half-second selfie be a better solution?

Just like I invited the short sellers to contact me if I got something wrong, I'm going to invite you to do something. Read the rest of this report. Then read what the shorts have written. Be open to both sides and see what makes the most sense to you.

Risks:

AuthID was close to bankruptcy a year ago. It's effectively a publicly-traded venture capital company. These are high-risk situations that are often part of a larger VC portfolio. If I could find 100 companies just like AuthID, I'd invest in all of them, accept that some will go to zero, and make a ton of money from that portfolio. Let's take a close look at what could go wrong here.

AuthID Needs Financing:

AuthID needed three rounds of financing last year to avoid bankruptcy. The company started 2024 with just over $10MM in cash on the balance sheet and burned over $8MM in free cash flow last year. They're currently building out the sales force and to do that means putting people on the payroll before they're productive. They'll run out of money in about six months, and it appears that they need to raise a total of $20MM to get to the point where they'll be self-financing. My model confirms this is a reasonable estimate.

Normally, the need for financing within a short time would be a huge concern. However, I've spoken with a number of shareholders who participated in last year's capital raises. They all understood that without another $20MM to come after the almost $20MM (before expenses) raised in 2023, the company would run out of cash and the value of their investment would be zero. When they put the money in, they knew that without doing a follow-on raise, their investment would be worthless. They've spent the money putting the new management team in place and funding the new sales force. The probability that they mark last year's investment down to zero and walk away is close to zero.

The reason the company has been raising money often and in small amounts is because as they put the pieces in place to succeed, the stock price has risen. By funding $AUID a little at a time in 2023, they've been able to do so at increasing prices and have reduced dilution. My model on the company assumes a higher share count due to additional equity offerings.

Unclear Disclosure:

I mentioned this above in the short-seller section. The company needs to stop using bARR as a metric. I've joked that they need to use Kosher reporting practices and not mix contractual obligations with estimates. I believe this was miscommunication due to a lack of experience dealing with public shareholders. I further believe management will start providing additional disclosure showing investors exactly what is contractual and what is an estimate.

Competition:

There are many companies doing facial recognition authentication. Most are small and private unlike AuthID which is small and public. Technically, Apple and Google could start to do this kind of authentication, but I think that's unlikely because they'd have to make their technology available on all platforms for it to have value to companies that have a wide range of customers.

Typically, these kinds of industries consolidate to 2-4 winners, and the experts I've spoken with agree. I expect about a third of the industry to become huge winners where the shareholders make 10x their investment or more. The next third will gain some scale, but when it becomes apparent they aren't going to win, will likely be bought by larger companies for a multiple of current valuations. The bottom third will likely fail and be worth zero.

Alternative Technologies:

Almost 100% of people in the cybersecurity industry believe we need to move past usernames and passwords. Right now, it looks like face ID with liveness detection is the best compromise between accuracy and ease of use. However, the technology market moves fast, and fingerprints, voiceprint, video selfie or active selfie, retinal scan, and behavioral analysis are all possible competitors. Even if the winners of the current round of biometric authentication are the face ID players, there's no guarantee that new technology won't supplant it in the future. In technology, there's no permanent lead.

Everything is Hackable:

Everyone claims their solution has incredible accuracy and can't be beaten or hacked. Based on a high volume of expert calls, I disagree. Everything is hackable. Everything can be beaten. The name of the game here is to make your system so much work to hack that the bad guys go pick on someone else. It's one of the reasons I have motion detector lights on my property. While no home security system is unbeatable, having lights go on when someone approaches at night is a good way to communicate to hopeful thieves that they'll be better off trying to break into someone else's home.

The most interesting expert call I did was with someone who told me that currently voiceprint is easily hackable using AI, and that face ID would be difficult to hack using an insertion attack. That plays right into AuthID's strengths. The same expert further said that he thought detection of fake voiceprint would improve and that hackers would eventually figure out how to use insertion attacks without detection. Should that happen, at that point, voiceprint would potentially be more secure than face ID.

In the end, hackers and cybersecurity and biometric security experts are playing a cat and mouse game with no end. As criminals make use of increasingly sophisticated technology to attack systems more effectively, the guardians of those systems come up with new more secure methods to safeguard our data. Again, there are no permanent leads in this business.

Everyone Gets Hacked:

This is similar to the previous point. If all systems are hackable, then all system operators will be hacked at some point. Industry security leaders like Okta and Microsoft have been hacked multiple times and will almost certainly be successfully hacked again. No matter how good you are, there will come a day when the newspaper article about today's successful intrusion has your company name in it. The bad news is it's unavoidable. The good news is customers seem to understand that no system is perfect.

A subset of this problem is that a hack can happen due to carelessness. It's not always a technology problem. One expert I spoke with told me that one of the Okta hacks happened because a third-party vendor put an excel spreadsheet in the cloud that had all authorized usernames and passwords. That doesn't indicate a problem with Okta's technology, but they got the blame for the security failure.

Illiquid Stock with Very Wide Bid/Offer Spread:

AuthID has a small float and trades around 26k shares a day. That means small amounts of buying or selling regularly move the stock a huge amount on a percentage basis. At times, the bid/offer spread has been around 10%. That means that buying or selling one share could move the stock 10% as the price shifts from the bid to the offer or back. The stock will be volatile so if that creates concern for your risk control model, size the position accordingly.

The Model:

AuthID ($AUID)

($MM)

	Year							
	0	1	2	3	4	5	Run Rate	Run Rate - Higher Expenses
Estimated Revenue Signings (bARR)	$ 3.0	$ 9.0	$ 18.0	$ 36.0	$ 63.0	$ 94.5		
% Growth		200%	100%	100%	75%	50%		
RPO from Year 0		1.5	1.5	1.5				
RPO from Year 1			4.5	4.5	4.5			
RPO from Year 2				9.0	9.0	9.0		
RPO from Year 3					18.0	18.0	18.0	
RPO from Year 4						31.5	31.5	
RPO from Year 5							47.3	
UAC from Year 1		-	0.8	1.5				
UAC from Year 2			-	2.3	4.5			
UAC from Year 3				-	4.5	9.0		
UAC from Year 4					-	9.0	18.0	
UAC from Year 5						-	15.8	
Revenue		$ 1.5	$ 6.8	$ 18.8	$ 40.5	$ 76.5	$ 130.5	$ 130.5
% Growth			350%	178%	116%	89%	71%	
Revenue		$ 1.5	$ 6.8	$ 18.8	$ 40.5	$ 76.5	$ 130.5	$ 130.5
COGS		0.9	2.7	5.6	12.2	19.1	26.1	
Gross Profit		0.6	4.1	13.1	28.4	57.4	104.4	104.4
Gross Margin		40%	60%	70%	70%	75%	80%	
G&A		5.0	6.0	7.0	8.0	9.0	10.0	26.0
% of Revenue		333%	89%	37%	20%	12%	8%	20%
R&D		4.0	4.5	5.0	5.5	6.0	6.5	13.0
% of Revenue		267%	67%	27%	14%	8%	5%	10%
EBITDA		(8.4)	(6.5)	1.1	14.9	42.4	87.9	65.4
% Margin		-560%	-96%	6%	37%	55%	67%	50%
D&A		0.3	0.3	0.3	0.3	0.3	0.3	0.3
EBIT		(8.7)	(6.7)	0.9	14.6	42.1	87.7	65.2
% Margin		-577%	-99%	5%	36%	55%	67%	50%
Interest Expense		0.1	0.1	0.1	0.1	0.1	0.1	0.1
Pre-Tax Income		(8.7)	(6.8)	0.8	14.5	42.1	87.6	65.1
Taxes		-	-	-	-	-	21.9	16.3
Tax Rate							25%	25%
Net Income		$ (8.7)	$ (6.8)	$ 0.8	$ 14.5	$ 42.1	$ 65.7	$ 48.8
EPS		$ (0.92)	$ (0.71)	$ 0.08	$ 1.53	$ 4.42	$ 6.90	$ 5.13
EPS Assuming 20% Dillution		$ (0.76)	$ (0.59)	$ 0.07	$ 1.27	$ 3.36	$ 5.20	$ 3.87
FD Shares		9.5	9.5	9.5	9.5	9.5	9.5	9.5
FD Shares Post Offering(s)		11.4	11.4	11.4	11.4	12.5	12.6	12.6
Projected Stock Price						**$ 67**	**$ 104**	**$ 77**

Year 1 vs 2025:

The reason I have the model organized as year 1, year 2, etc. instead of using calendar years is because I don't know at what point of the year the company will sign contracts. In a normal year, we'd expect the average contract to be signed in the middle of the year and then take about three months to go live and start earning revenue. For simplicity, I assume all contracts go live Jan 1 of a particular year. In 2024, the company has said that contract signing will be back-end weighted. If we push everything back a year, due to late signings and a three-month onboarding process, you could think about year 1 as 2025. In other words, if AuthID starts signing $9MM of bARR in 2H of 2024, they'll start collecting most of that revenue in early 2025. Viewing year 1 as 2024 would be aggressive and unrealistic. Viewing year 1 in my model as 2025 would be slightly conservative.

bARR:

The most important thing to understand about the model is how bARR (the non-GAAP term that should never be mentioned again) works. I highlighted the numbers related to the $9MM of year 1 bARR in yellow. RPO stands for Remaining Performance Obligation. That is the minimum contract amount for a customer. Contracts are for three years, and about half of the bARR amount would be contractual (RPO) and paid each year. That's why for the $9MM of bARR in year 1, you see $4.5MM of RPO paid in years 2, 3, and 4.

The rest of bARR is usage above commitment (UAC) and consists of estimated revenue above contractual minimums. It should take about 18 months for companies to ramp up usage to these higher levels at which point, they start to produce about as much revenue as the RPO. If you look at the row labeled UAC from year 2 (in yellow), you see no revenue for the first 18 months. Then you get the full $4.5MM in UAC for the last 18 months of the contract.

To sum up:

- $9MM of bARR results in $13.5MM of contractual revenue (RPO) over the next three years.
- $9MM of bARR results in $6.8MM of usage above commitment (UAC) over the next three years.
- Total amounts paid over the three years is $20.3MM consisting of $4.5MM in year one, $6.8MM in year two, and $9.0MM in year three.

In the future, I expect the company to stop using bARR which is confusing due to the mixing of contractual obligations and estimates. The better way to present this information is to provide contractual obligations and estimates separately. So, instead of providing the $9MM bARR on the first row of the model, AuthID should show you RPO and UAC separately. When you add those two together at the end of the contract, they equal the soon-to-be-retired metric, bARR.

Margins:

Gross margins are currently low because AuthID licenses certain software items. Currently, the company doesn't do enough volume to meet its contractual minimums. That will be fixed by the time revenue approaches $20MM. The company has said that G&A will increase by about $1MM per year and that R&D will increase by about $.5MM per year. Right now, $AUID has net operating losses (NOLs) so won't be a taxpayer for several years. For the purpose of valuing the company, I'm assuming they'll start paying taxes by the time we're using earnings to come up with a price target. For the share count, I'm assuming 20% dilution from coming equity offerings. In the out-years, I'm imputing a projected stock price for the purpose of determining dilution from options are warrants that are currently out-of-the-money. That's why the fully diluted share count post offerings is 12.6MM instead of the current 9.5MM number.

Valuation:

I assume the company continues signing contracts for the next five years, and then determine a revenue run-rate. That's the $130.5MM number in the "Run Rate" column. Think of that as a revenue target in 5-6 years. That gets us to fully diluted earnings per share of $5.20. **A 20x**

multiple on that would be very conservative for a company growing revenue and earnings at this rate, and would translate to a stock price of $104; about 15x the current stock price.

The one place in the model where I thought some conservative criticism would be reasonable was my margin assumptions in the out year. That's why I added a "Run Rate – Higher Expenses" column. For that calculation, I assume that G&A is 20% of revenue, or more than double the amount suggested by the company. I also double R&D from $6.5MM to $13.0MM. With those more conservative assumptions, **I get to earnings of $3.87/share. Assuming the same conservative 20x multiple on earnings, we get a stock price of $77; about 11x the current stock price.**

The risk section above is long because this is a risky situation. The reason to invest is the skewed return distribution. Essentially, you're risking $1 to make $10 - $15.

I'm not including the cash flow model here as this report is already heading for 20 pages. Because AuthID doesn't need to keep a lot of inventory around or build construction plants, incremental cash flow used to grow revenue isn't very high. The primary drag on free cash flow is increasing accounts receivable related to higher contractual revenue. I have free cash flow running at 90% - 94% of earnings in the later years which is a great ratio for a company growing this quickly.

The Bar Isn't High to Succeed:

AuthID is focusing on signing contracts with two key groups of future customers. The first is the Fast 100; a group of smaller companies where they could move quickly, but with smaller contract amounts. The other is the FAT 100; a group of larger companies where the sales cycle is around 18 months and would have larger contract amounts. I asked management what kind of revenue they could expect from the median company in the FAT 100. They responded $3MM - $6MM of bARR.

They provided an example of a current customer with 500,000 users requiring onboarding with identity verification. All of them require authentication. This existing customer started to test AuthID at 500 users a month and has now moved up to 5,000 per month. Over time, they'll move to the full 500,000 users plus additional users that they may add every month. This is a perfect example of how revenues ramp up at a new customer and how $AUID gets from contractual minimums to higher usage levels above the minimum which add up to the bARR calculation explained in the previous section.

Based on this example, we can model a typical hypothetical FAT 100 customer which would pay AuthID about $1.00 per user per year (about $.50 per user to initialize the account plus a monthly fee). After a ramp-up period, they could reach 3MM users. When fully deployed, this comes to $3MM per year. To achieve this year's $9MM of bARR signings, the AuthID team needs to sign 3 new customers at or around this level.

To get to next year's $18MM of signings I've put in my model, they need to sign 6 new customers, or one every two months. New CEO, Rhon Daguro, was hired specifically because he has a track record of building and training sales teams, and achieved this kind of revenue ramp while at competitor, Socure. This is the one most important factor to determine $AUID's future stock price**. If Rhon and the new sales team can get to the point where they're making 1-2 meaningful new sales a quarter, then we'll see the kind of growth outlined in the above model, and a much higher stock price.** If they can't do this, then there's nothing that will help the stock.

In my opinion, 1-2 sales a quarter is a reasonable and low bar to clear. This is especially true given the importance companies are now placing on cybersecurity. Not having a plan to keep the bad guys out of your system is no longer an option for businesses that serve large numbers of customers.

Conclusion:

AuthID is a publicly traded micro-cap venture capital company without meaningful revenue right now. This is a high-risk situation…**but one with a skewed return distribution**. I think the company has a bad history with management that didn't know what to do with its technology. I believe that hiring a CEO with a successful history of systematically building and training an effective sales force was the right move for the company. Rhon Daguro is the person I'd put in place to give the company the best opportunity to succeed.

One place Rhon is currently having an impact is in attracting other impressive people to join AuthID. He recently convinced Kunal Mehta to join the $AUID Board. Kunal is a Partner at Bain & Company. Previously, he was an Operating Principal at TCV where he invested in a long list of well-known high-growth technology companies. Kunal is one of those guys with a gold-plated 5-star resume. People who have achieved that level of consistent success don't join companies like AuthID thinking they'll go bankrupt in the next year or two. Separately, I've spoken with him. In addition to being as intellectually impressive as you'd expect, he's also a very nice engaging person. Fantastic addition to AuthID and a great pickup by Rhon.

Given that the company is coming from a sales base that's close to zero, I think there's a one-third probability that the company fails. I believe there's a one-third probability that AuthID starts to sign new customers but doesn't become one of the top 2-4 companies in the industry. In that scenario, the company would probably be bought by a larger competitor at a multiple of the current stock price. **That leaves a one-third probability that the company becomes a leader in the biometric authorization space with a conservative target price of $77 - $104 or 11x – 15x the current stock price.**

The "problem" with AuthID isn't that it's a higher-risk situation than most other investments I make. It's that I don't have another 99 companies exactly like it to put into a huge profitable portfolio. It's rare to find a return distribution this skewed where all the pieces are in place to

succeed in the next huge growth area in cybersecurity. I'm comfortable risking $1 to make $10 - $15.

From a portfolio management perspective, the way to manage the risk is position size. I've sized my $AUID position so that if the stock went to zero, I'd be able to manage the loss – AND – sized it large enough that if the new management team executes, the stock will be a meaningful contributor to my net worth. I think it's worth committing capital, and caution you to size your position with an eye on the risk and potential losses.

Disclaimers:

At the time of writing this report, I personally own $AUID stock. Any future updates on the company, changes in opinion, changes in target price, or changes in my personal shareholdings will be communicated to paid premium subscribers of Deep Knowledge Investing. If you are not a Deep Knowledge Investing subscriber, please don't count on me to keep you updated.

I was not paid to write this report. **I do not have a financial relationship with the company and they did not offer me compensation.** Had they done so, I would have declined.

DKI is conflict-free and our only aspiration is to attempt to help our subscribers make better returns in the stock market.

Disclosure:

This idea was first posted to the Deep Knowledge Investing blog on April 13th, 2024. The closing price the prior trading day was $7.50.

Information contained in this report, and in each of its reports, is believed by Deep Knowledge Investing ("DKI") to be accurate and/or derived from sources which it believes to be reliable; however, such information is presented without warranty of any kind, whether express or implied. DKI makes no representation as to the completeness, timeliness, accuracy or soundness of the information and opinions contained therein or regarding any results that may be obtained from their use. The information and opinions contained in this report and in each of our reports and all other DKI Services shall not obligate DKI to provide updated or similar information in the future, except to the extent it is required by law to do so.

The information we provide in this and in each of our reports, is publicly available. This report and each of our reports are neither an offer nor a solicitation to buy or sell securities. All expressions of opinion in this and in each of our reports are precisely that. Our opinions are subject to change, which DKI may not convey. DKI, affiliates of DKI or its principal or others associated with DKI may have, taken or sold, or may in the future take or sell positions in securities of companies about which we write, without disclosing any such transactions.

None of the information we provide or the opinions we express, including those in this report, or in any of our reports, are advice of any kind, including, without limitation, advice that investment in a company's securities is prudent or suitable for any r investor. In making any investment decision, each investor should consult with and rely on his or its own investigation, due diligence and the recommendations of investment professionals whom the investor has engaged for that purpose.

In no event shall DKI be liable, based on this or any of its reports, or on any information or opinions DKI expresses or provides for any losses or damages of any kind or nature including, without limitation, costs, liabilities, trading losses, expenses (including, without limitation, attorneys' fees), direct, indirect, punitive, incidental, special or consequential damages.