EPISODE 369

[INTRODUCTION]

[0:00:00.8] JM: A cryptocurrency exchange faces a uniquely difficult fraud problem. A hacker who steals my credentials can initiate a transfer of all of my bit coin to another wallet and it's a nonreversible, nonidentifiable payment. It is really important to prevent those kinds of fraudulent transactions. At the third Software Engineering Daily meetup, Coinbase director of data science soups Ran Jan explained how a Coinbase stays ahead of fraudsters and he describes some of the cutting edge social engineering attacks that are being used to try to steal crypto currency.

Including cellphone take over attacks which are particularly chilling. Next week, we will be airing three shows that I did on site at Coinbase, these are going to be interviews with engineers from three different teams. You can check out those shows for a deep dive into crypto currency uses, the fraud challenges that Coinbase is tackling and the infrastructure and security of Coinbase. Coinbase is a really exciting company and it was a lot of fun getting a panorama for how several parts of the organization function.

Now, this episode today was recorded at the meetup and it's a presentation from Soups who I also interviewed in the upcoming interviews that I did that are going to be aired in the coming week. Since this is a bonus episode that we're airing on the weekend, there's no adds, you can just think of it as a preview for some of the topics that I go into more deeply with Soups in the interview next week.

By the way, the next Software Engineering Daily meetup will be in New York, we don't know when it will be yet but you can sign up to follow the podcast meetup at softwareengineeringdaily.com/meetup and we'll be sure to let you know anything ahead of time, as soon as we know, you will know when the meetup is and I hope to see you three.

I hope you like this episode and I'm particularly excited about the upcoming episodes around Coinbase that will air next week.

[INTERVIEW]

[0:02:09.6] SR: All right guys, my name is Soups, I am the director of science and risk congealing at Coinbase. How many of you guys have heard of Coinbase or use Coinbase? Okay, quite a few, awesome. For those who don't know what Coinbase is one of the largest digital currency exchanges in the world.

The digital currencies that support are bit coins, Ethereum and actually starting today, light coins. I'm here to talk about preventing payment fraud and account take overs in digital currency. Our mission at Coinbase is to create an open financial system for the world, bit coin is essentially powered by a public ledger system called a block chain which essentially allows multiple parties to prove that whether someone who says they own this much money really are the true owners of the money.

They can actually enter into an agreement too you know? Send money to each other et cetera. Very efficiently. Now, you know, there's been other versions of lock chain which are far more efficient like Ethereum, et cetera, I'll be come on, people to write smart contracts such as you know, the event X happens then the person A should send money to person B and all of that can happen in code right?

That's a real quick, high level introduction to the world of digital currencies. Now, our mission at Coinbase is we want to be the gateway to a lot of people to purchase bit coins, light coins, Ethereum using the fiat currencies as in US dollars, Euro, Pound, Singaporean dollars, those are the full fiat currencies we support on our platform.

So far we have had six million users in 33 countries, exchanged about six billion dollars in and out of digital currency, what are some of the common use cases? Cross board remittance is a popular one so I could for instance send money to my parents in India at a far cheaper remittance rate. Much cheaper than transfer wires et cetera.

All that my dad in India needs to do is he needs to have a bit coin exchange account in India and I'm just going to send him bit coins to bit coins, that will go instantly right? In the public blocktion of bit coins, every transaction on average gets noted down in 10 minutes right? We are working towards speeding it up and make it even faster but that's what where it as right now.

The second big use cases, merchants they can accept bit coins with no charge back risk right? The important point to note here is that the bit coins right? It's essentially just a private keep, 64 bit private keep. That's what is you know, that's where your funds are locked up right?

Whoever knows that private key has access to your funds right? Unless somebody were to actually physically coerce that private key out of you right? If you have the private key, you have it, you are the true owner of the funds behind it right? Turns out, it's not really the case in fiat currency right? Somebody could steal my credit card much more easily right? Somebody could steal my online bank using email password much more easily and pretend to be me or pretend to be the person who is the owner of the bank account or the credit card.

That's a very important distinction to remember here which is why we say that merchants can accept bitcoins with no charge back risk. Coinbase has a merchant platform as well, you know, V power, the likes of Kayak, Expedia, Dell, et cetera, you can purchase products using bit coins.

Lastly you know? Bit coins and other digital currencies, they have spurred this new wave of alternative investment. You know, there are lots of folks who are really big believers into this new ecosystem of applications which are going to be powered on top of these digital currencies right? They are basically going to — they are all betting on the fact that in the near future, you know, the Europe banks would be over, there will be an open financial system and there would be apps which allow you to do anything that you do with respect to traditional banking right now.

Be it you know, peer to peer lending, be it some of the examples like remittances or smart contracts et cetera right? There are lots of people who are buying bit coins, digital currencies et cetera as an investment. As I just said, huge day for us today, we added support for light coin which is our third crypto currency and now I am going to focus on the bad actors.

Before I move on to the bad actors, I want to add a very important caveat. Majority of the activity on our platform is good. Majority of the users are using bit coins for purposes they really believe in right?

It's these few bad actors which spoil it for us or in some sense make it interesting for me you know? Because I get to go fight them right? Now, the same reasons which make bit coins so popular with users right? That is the instant, you can instantly transfer bit coins and they're nonreversible right? If I send it to you right? I can never get it out from you, I can never get it back from you right?

It's like cash right? Unless I physically coerce it out of you right? The same reasons that make bit coin so popular for good users make it very popular for bad users as well which is why you know, I firmly believe that all the bit coin exchanges in the world and Coinbase being the biggest one.

We have the hardest payment fraud and user security problem in the world right now. Harder than PayPal ever did 10, 15 years ago, I'm a huge fan of how Paypal built its fraud team right? There's lots of lessons to be learned but everything that they had to do at that time fails in comparison to what we have to do because what we are selling is 64 bit digital key which can store millions of dollars right?

If I have access to let's say thousands of trade cards, I can go buy like stolen credit cards. The best thing I can buy is bit coins using it. Because I can buy bit coins, I can move it out instantly right? To a private wallet that only I know the private key for, it's not hosted out in exchange and no one can come and get it out of me.

That makes it super attractive for fraudsters. Likewise, if I'm a fraudster, if I miss camber, you know, going after a Coinbase or any of the digital currency exchange users wallet is a super high target because once I get that money out of there, I can move it in suddenly to a wallet only I control right?

You know, no one can get it back from me, right? The distinction here, all of that is true with PayPals of the world as well, on the fiat side. However, on the fiat side, you can track money right? All this banks, they have built a way by which they can actually – essentially you know, in some means or the other, call each other up and figure out where did the money go right?

There is yet to be anything built off that sort in the bitcoin, or any of the digital currency world and that is why it's a lot harder. Now, I'm going to focus on just those bad actors which make this problem really fascinating to solve and I'll talk to you about how we are solving it.

That would be I'll talk about payment fraud, I'll talk about account take overs, what do we do for detecting and preventing fraud and a few case studies. Payment fraud. First of all, this is our signup flow. In order to create an account on Coinbase, you have to provide us with your email address and then we send you an email, there's a link that you have to click and then you have to provide your phone number, you get an SMS to that phone number, you have to verify that SMS.

[0:09:48.3] Then you add your bank account or credit card right? If you add your bank account, then there's two ways of doing it and it's important to know this now. One is that you know, there's a list of banks where we directly support you know, for you to just enter your username and password and then your bank would be verified.

We don't store the usernames and passwords. We use a third party service which has all the clearances and the highest grades of privacy, economist leader for storing usernames and password. Now, the advantage for us is that once you actually give us the username and password, we know that it is you, the true owner of the bank account because we can pull the name and address behind it right? There's an alternative there which cameras love.

Also privacy conscious users love which is you could actually do the micro deposit method, you could actually, you would basically make two micro deposits less than a dollar each into your bank account, you go in to your bank account log in there, look at what those amounts are.

Come back to Coinbase and enter it and then we know that you control that bank account right? Scammers. Say that again? Yeah. Scammers loves it right? Because they know that once they verify a stolen bank account using micro deposits, we can't get the name behind the bank account right?

This whole thing about getting the name and the address behind the bank account, there's of course privacy reasons right? In fact, it's impossible to even call up a bank and you know, as a fraud agent and tell them “Hey, we have a customer of your bank who has created an account on Coinbase can you tell me, if the account number and name and address they match,” they won’t do that right?

The US patriot law I think is one of the laws over here, it has made it so hard that you know, even to fight fraud, money services businesses can’t make use of the information that I think should really be readily available because you know, at the end of the day, we’re going to help customers right?

[0:11:51.1] Now, what does product Coinbase look like? If I miss camber, I’m going to basically create a mish mash of identities. What I’m going to do is I’m going to steal Alice’s bank account or credit card number, Bob’s identity which is driver’s license numbers, driver’s license card as well as social security number and I’ll steal a third person’s card’s mobile phone number, remember I said that you have to have you know, a phone number to verify an account on Coinbase right?

Then I will steal money from Alice’s bank account by bit coins and move it out of Coinbase to a private address that only I control right? Alice will – a couple of months later, look at her bank statement and be surprised alarmed, aghast that your what is this row in my statement, it says Coinbase, she should call up her bank eventually will then call up our correspondent bank and in most cases, if you haven’t done a few set of requirements then they may have to return the money back to Alice right?

Those cameras are away with the bit coins, Alice gets her money back, Coinbase is left holding the bag right? Therefore, it all comes down to if you don’t solve this problem well then you know, our margins will be really low. This is what is also one of our USP’s which distinguishes us from most of the other bit coin exchanges in the world that we manage to keep fraud low.

Account takeovers. The second thing that scammers love is account takeovers. They want to go after Coinbase accounts. Now, you know, brief primer on two factor authentication right? Two factor authentication means that you should have something you know which is a strong password and something you only have which is a physical device right?

Every time you get an SMS right? When you are logging in anywhere to your phone, it’s actually meant to really verify it as you, the person because there are two factors that they are very fine right? That only you should have. However, I’m going to take you down like very quickly down one of the most prevalent account take over methods at Coinbase.

[0:14:08.5] Basically what mistake was made was that this something you always have which is a physical device, it was equated to a phone number right? The whole security industry said okay, let’s just send a text to the user’s phone number and then we’ll be able to validate that the user has control of the phone because otherwise why will he actually be getting the SMS and be able to enter the SMS back on this website right?

Turns out it’s actually far easier to steal phone numbers than to steal physical devices right? Far easier. First of all, you know, there are methods by which I can actually read SMS online. How many of you guys have Verizon phones over here? Awesome, there’s only two people. Love it, cool.

Please come talk to me after this. Because if you have a Verizon phone, you can actually read all of your SMS online. Every SMS that goes to your phone, you know, if I’m an attacker, all I need to know is your Verizon username and password, that’s it.

You know, if you have it set like a very weak password, it’s probably already dead and all the password dumps order. I can easily read all the SMS that you’ve been getting there. In fact, I can probably also read all the SMS tokens that you get from variety of companies in the world.

[0:15:29.3] Therefore you know, the fact that if I’m trying to really prove that you know, Jeff controls his device by saying that okay, the SMS that I sent to his phone number, only he could have seen it, it’s totally untrue because I as an attacker could have logged on to Jeff’s Verizon account and seen the SMS to codes, he was getting and therefore without even stealing his phone, I have now you know, passed the two factors.

Please stop me at this point and ask any question. Take a question there.

[0:15:59.4] MALE: [INAUDIBLE]

[0:16:03.0] SR: I will walk you through all of that, however, quick answer is, our 2FA is opt in right? We can't force people to only use a particular two method right? In some countries, SMS is the only method they want to use and some places they're not you know, tech savvy enough that they will default to using an app and the second answer to that is we've closed that loop hole already. You can't Coinbase SMS 2FA tokens, you cannot see them on Verizon online portals right?

The second methods are yeah, just SMS hijacking. There's lots – yeah. The third one is basically sim swap or phone porting which we have seen increase in prevalence starting Christmas of last year. This is how phone porting attacks work.

Phone porting attacks are basically number one scammer finds a list of targets, in this case, we find people who may hold lots of digital currency. And then, what they do is, they then try to find all the phone numbers of those individuals, that's relatively easy, you can go to Facebook, LinkedIn et cetera if you have it public.

In fact, there's another far easier method if you have Gmail then all they got to do is I got to just go in and you know, sorry, this was the next step. Once I find your phone number, how do I find your email address right? I have to just go to Google and pretend that I have lost access to my email address and this is my phone number, Google will tell me all the email addresses behind the phone number.

Then, I can basically go in and reset any email right? Google, Yahoo, et cetera. Because most of them default to for a contrary purposes, the default we're just sending a text to that phone number right? Now that I have access to user's phone number as well as email address right? I can do anything. There's lots of sites out there which are you know, password managers as well as you know, 2FA apps which try to store your 2FA tokens online right?

They all are vulnerable because the economy process for all of them relies on you know, making sure that no one has access to two things which is phone number and email. If I as an attacker have access to those two things, even the most secure online cloud backed 2FA method is insecure because security is basically the weakest link right? This method, by this attack, all of our fancy cloud backed apps are actually at the hands of the Telco call operator.

Yeah, this number two step is actually just social engineering, all they're doing is they're calling all the telco guys and they're saying "hey, I lost access to my phone number, to my iPhone, can you just port my phone number from this iPhone to this other iPhone right?" And they will do it right? Sometimes they have phone line which is open with the telco's like 24/7.

There's a big ring out there which is just doing this 24/7. We have lots of information about them and we are you know, going after them but yeah, once you have those two factors, you can do anything and then they try to steal bitcoins.

Of course If I have alarmed you and you feel like you should not invest in this currency, none of these are, all these loopholes have been fixed on Coinbase. You know, you just have to follow a few basic steps. Number one, to prevent any of those account take overs right? All you have to do is use a strong password manager, you know, don't use weak passwords which are you know your name or your kid's name, et cetera.

You know, just use a TOTP app like Google authenticator, Microsoft authenticator, these TOTP apps, they work as follows. What happens here is that you know, like if you guys have used Google authenticator, you remember scanning a QR code right? That thing, what is really happening is that you know, it's really just a secret key that is not being shared between the Google authenticator app on your phone and the website, who's page he was scanning, in this case, Coinbase right?

[0:20:17.7] Nothing traveled on the Ether right? it was just you know, the fact that you took a picture, there's no man in the middle here right? Nothing traveled in the Ether. After that, now that both parties, Coinbase and your phone have this shared secret key, you know, they have an algorithm which basically generates a secret code every 30 seconds a new code is generated and the algorithm just looks like, you know, it's just a function of current time and the secret code right? that's it.

Therefore, you know, the code that you see on your app, your internet, Coinbase will basically use the same algorithm based on the secret key and the current time of the day and generate the code and try to match what you entered with what your phone generated.

[0:20:58.8] MALE: Are there attacks that Google authenticator is particularly vulnerable to or is it pretty bullet proof?

[0:21:03.8] SJ: There are some attacks that it's vulnerable to but I don't have details of them off the top of my head. Yeah. Going back to one question that we got from the audience, they're still – our 2FA policies opt in right? There's lots of people who will, even if you tell them please do this, they won't do it right?

There's lots of people who won't to move to Google authenticator even though they may be storing millions of dollars with us but we still have to protect them. Now you know, the same thing that happens in the trade card industry where you know, you all of a sudden are traveling and credit card companies puts a ban on your card right?

Similar logic right? What we are doing now is basically we would detect that you are making a withdrawal from your account, you know, which looks very suspicious and under those conditions where we verified as suspicious, we will just delay it by 48 hours right?

In the mean time we'll just you know, email and SMS blast the user, making sure that they really did it. However, there's always going to be false positives right? This algorithm that we use or we rely on, it's a rules based algorithm, it will have some false positives and we don't want to annoy the people who will really legitimately trying to move the money out right?

In those cases we allow them an option to say "okay, it was really me trying to do it" so they can actually just click that button that says, I still want to accelerate my withdrawal right? All that they will have to do then is to upload a picture of their ID, front and the back and take a picture of themselves, the selfie.

Then, we will match the name on the ID with a legal name on the account. It serves two purposes, the selfie and the picture on the ID need to match proving that it is you in true position of your ID, the name on the ID and the legal name on the account need to match proving that it is indeed you who did it right? Questions?

[0:23:04.8] MALE: Does that take away some of the value of anonymity of bitcoin watching?

[0:23:09.8] SJ: Yeah, we get asked that question quite a lot so we consider ourselves as the gateway to between finance 1.0 and finance 2.0 which is the finance 2.0 being bitcoin, additional currencies based and finance fund point on the email of the traditional banking right?

In order for us to be the bridge and in order for us to be the white knight in the space where we are still following all the regulatory requirements, we do have to collect ID's from our users right? Now you know, like the victim of the account take over, would receive an SMS or an email and there's a new thing we've done. Because you know, victims would typically just write to us all the time, they were emailing us left and right to support at Coinbase saying. "I am hacked, do something," right?

Now, what we do is, all the victims, they get an email and there's a link which says you know, if you did not initiate this withdrawal, you can click this link and you can lock your account until somebody unlocks it for you or by yourself. So without requiring a support agent, they can actually lock their own account. If they feel that the withdrawal was made from their account but not by them. So yeah, the second part of the talk is fraud detection prevention. As I was telling you this problem of people using stolen credit cards, stolen bank accounts to buy bitcoins right?

Hurts on margin so you can't tell this problem using just machine learning alone or using human analyst alone. You have to use both of them in cohesion and I try to motivate that through the rest of this talk. Essentially what happens is human actions, they train the machine learning algorithm. So we have in my team eight engineers and seven analysts. The analyst's job is to just review the account and if they see anything suspicious, they use their six sense to ban that account.

Whatever the actions that the analyst took gets fed into the machine learning algorithm which basically extrapolates it and then learns a new algorithm which we apply on the rest of the users going forward. So it happens in a close feedback loop on and on and each of them help each other. We call our internal machine learning system as Peacock and it's a supervised machine learning algorithm. How many of you folks are here into machine learning?

A quick show of hands, okay cool, quite a few. So yeah, supervised machine learning, bandwidth classifier, there's two labels, fraud and non-fraud. The fraud label comes from two sources. One is our analyst, they are using their six sense. Second is when Alice calls up her bank and sees this charge was unauthorized right? Charge backs and then as a user is actually doing any activity on a platform. We collect lots of singles. We collect information about their device, process finger prints about the location and based on the email, phone number, ID, SSN or bank account behind all of them, we extract the name and the address from all of them and we bring the names and services from all these data sources and we do mismanage deduction right?

So now why does machine learning work to detect fraud? First of all as I said we are bringing the names and addresses behind the phone number, behind the bank account etcetera.

First of all, let's set one thing, establish one thing here, in order to be the system where I am doing like a name mismatch protection across all data sources, I have to be a real expert scammer because I have to not only – I am going to have pick on Jeff again, I have to not only steal Jeff's bank account. I have to steal Jeff's identity, I have to register a phone under Jeff's name. I have to create fake Facebook, LinkedIn, etcetera profiles which have the names and addresses matching Jeff's.

So doable, really doable if I really want to go after one particular user but at that point the ROI for fraud should be high enough that they don't do it. That's our intent right? So okay, machine learning why it works is because – or rather why do you even need it? If I were to just collect names and addresses from all these data sources, I could just say, "Okay I'll use a rule based system" that says if names and addresses don't match across any tool or resources ban the user.

But that will catch lots of false positives because as you know we have different names or aliases on different places. Jonathan became John Ken, right? So that's why machine learning is important because you want to still have a high enough detection accuracy by eliminating the false positives. So therefore a common trait that we do is that we take the two names, we do some transforms like your card similarity but we take the number of categories which are common between the two names.

[0:27:53.0] In the numerator and the denominator is the number of characters which are in the union set of the two names right? The second reason why machine learning works to detect fraud is because of the book and window theory. So these scammers they are constantly talking to each other. They are exchanging information on online forums, etcetera and if they discover one method of committing fraud, all of them will come rushing through the flood gates right?

So case and point, there was a point where we saw this pretty close screen resolution, 13-64 by 7-68. It's probably the off occurrence in real life is less than 0.1% but our agents, they were banning them at the rate of 55% right and it turns out that all these scammers they are actually using remote desktop protocol from Windows to pretend to be coming from a particular device type and Windows IBP protocol, thanks to Windows it has a bug.

The pixel appears to be off by one pixel on each side. So that screen resolution does not exist in reality, it should be taking 66 by 7-68. Praise be to Windows for not fixing it, please don't fix it. Cool, so how do we use the risk score? We use the machine learned risk score to do the following thing: Previously, we used to say anyone above a particular value of risk score we would ban them. That just means that if you were a false positive to whom we give a high risk score, you can never prove yourself innocent again.

You're just banned for life. So therefore now what we do is we just based on the risk score, we give you particular purchase power. So even the scummiest of the scammers in some cases they will get a second purchase power, colored dollar five per day. We will observe them over a period of time and if you don't see any charge backs over that period of time then they have proven themselves innocent if they were a false positive otherwise we just reduce our exposure and in a lot of ways we're just learning, paying to learn right? Paying to train our machine any moral.

[0:30:01.0] Now in our case here, this is a pretty interesting modeling problem. How do you decide people's limits? There are several factors which are baked into it. One of course is how much is your purchase volume. So the more you purchase, the higher limits will go. How aged are your funds as in how long have you seen you being continued purchasing use on a platform without seeing charge backs. That means that it can give you higher purchase power going forward.

Thirdly, have you passed certain verifications, have you uploaded your ID, etcetera right? And of course there's all the other things like machined learned score. As we observe the user we constantly learn more and more of them and your machine learn score also changes. So based on all of them your risk, your purchase power keeps evolving. One of the things that is quite interesting is that how do you take a look at metrics in a system like this right?

So much of learning metrics are hitting under the curve or log lost, that's what you trained your model to optimize for. However the business metric we are interested in is basically fraud rate which is basically dollar lost by purchase volume. That is actually our goal and this is how we've been doing it. It has been around our goal for the last 10 months. There was a time where that was really high and I'll talk more on those scary times.

But now there are lots of many designs of machinery and systems. There's lot of other things that can go wrong like when you deploy a new machine learning model this is what happens. Somebody read it and was freaking out, what happened to our limits? People really love to watch the limits on point of this. They hold it very sacred. The lesson in this case for us was that we can't deploy a new machine learned model without actually doing a few things.

Which is whenever there's a new model that we need to deploy, call it the challenge model we need to make sure that the challenge model is deployed in shadow mode and the observed scores of all the users as produced by the challenge of model as well as the production model and then you plug the distributions of what does it look like for both the good users and the bad users right? And then if it looks all right, then only do we bump up the challenge model to production.

That another thing we have to do and we have to be really careful about which is our wheels, our high value users. We don't to basically suddenly because we just deployed a new machine learning model, changed the scores on them overnight. So this is an extra step we have to go through which is there will be false positives. Just accept that right? But as long as it's a handful of false positive, we then provide those false positives to our analyst.

Who will then go through them and just lock the scores for those user. I wanted to provide a theory for this because are going deep into how machine learning is done but instead to talk about how do you use machine learning in a business context because I feel like this is the kind of stuff that gets less frequently spoken about. So the next one is where does the supervised machine learning fail? First of all the charge back Window is large.

They could be getting charge backs up to 60 days for ECH, that is banks as well as up to six months for cards right? If you need it for that long in order to really look at labels for all the machine learning algorithm that will be too late. Fraud is highly dynamic. So you have to extrapolate what our analysts are seeing very quickly and therefore you need some unsupervised approaches like anomaly detection, related users modeling and rules engine.

[0:33:38.2] Anomaly detection is basically what we do is we baseline traffic. For every signal we baseline traffic on a monthly basis. Let's say I want to track how many people are signing up on Coinbase using Wells Fargo cards on a monthly basis. What fraction is that user population compared to the current population? That's the blue line and then all of a sudden the weekly line for the particular week jumps up then I know something is wrong right?

There is a scam rate. Somebody purchased a whole bunch of Wells Fargo cards online somewhere so then we present those accounts through our analyst who can quickly zoom in and analyze those users. Remember, this is unsupervised. We hadn't gotten any labels from anywhere and we are trying to zoom in and identify unusual patterns. The second thing we try to do is related users deduction which is if I ban an account then I will quickly ban other accounts which are related by some strong attributes.

Like social security number, bank account number, etcetera because then they are likely controlled by the same individual. There is a probabilistic sense to it as well where you can't act or we don't act automatically. We just basically say every user in an end dimensional feature space is this point and we compute the core science similarity between two points and whenever we ban an account, an analyst is presented with list of other users.

Strongly related to this user in this core science similarity space and then the analyst can choose to drill down and take a look at those other users and choose to ban them or not. The third one is a custom rules engine. Our analyst are constantly using the sixth sense or they are using some of the other tools to identify what sorts of behavior is happening on the platform and then they quickly create rules. They create rules and they delete rules as quickly as well because you don’t want to hold that in the system.

[0:35:34.3] So the rules could be okay, if I see JP Morgan Chase cards which are using Verizon phones and from these states then I’m going to freeze the risk score to this level which will reduce my risk exposure to that level or it could be in some kind of conditions like I want to require an ID from those users. The Holy Grail for us would be if we can combine all of this and use anomaly detection to power creation of new rules automatically so we are working on that next.

Cool, so a case study we call the Verizon debit card ring. I am picking on Verizon here, I hope there is no one here who works at Verizon. So Verizon ring what they did is first of all no PII here, these are stolen, these are photo shopped ID’s. All the attacker did was that he just changed the driver license number. He was using stolen debit cards and he was using stolen Verizon phones to verify that con. Remember I told you that you don’t need physical device to receive SMS?

So of course there’s websites where you can go, recievesmsonline.net. You’ll get a phone number, you enter that phone number on Facebook, you get the 2FA of that token on their website, you enter that token back on Facebook, you are in, easy. The other method is as I have describe earlier, I steal someone’s Verizon username and password. I can see the 2FA tokens over there right? This is our agent, this is a screenshot from that time.

Our agent, our analyst he discovered this and he was like, “whoa!” and then we fixed it. The fix was basically we had to find SMS to a paper wider who knows how to send SMS such that it can never be read online. The solution existed however this whole bureaucracy of Telco’s etcetera, it took us a while to find it and the existing 2FA provided that we are using, we told them as well that this is how you fix it so that we benefit via then the whole industry gets benefited.

It took them six months to figure that out and all it needed is a six digit code change from what I'm told but a huge bureaucracy to figure out how to do it. So how we did enter this ring, we did via anomaly detection. The scammer wasn't far. They basically left something wanting which is the user's same screen resolution and that's how we nailed it and the risk engine it's automatically scoring and rescoring users after every action.

The scammer reused a card that we had already blacklisted and then automatically we reduced the exposure from $60 a day to 10. So there we have the whole system anomaly direction, automatic rescoring, machined learned risk score, all of them came together to reduce the risk exposure in this case. I just wanted to in the last section just show you a few ID's and talk to you about how do you go about establishing identity online.

So first of all, like all ID verification methods where you are asked to open the front and the back of your ID are flawed because I have on my phone, ID's of people I have had car accidents with, legitimately obtained. I could upload them and I could pass ID verification but I am not that person. Of course it would be illegal for me to do that as well. Now one of the biggest learnings for us, one of the biggest scam rings was that that's what the scammer did.

He just uploaded the front and back of someone else's stolen ID. So what we do now is basically we require a selfie where you not only have to upload your front but also your selfie and then we can truly establish you are in control of your ID. In some cases even that is not sufficient. In some cases our agents have the capability to use a new tool that we've built which is we even send a postcard in the mail to an address that we only want to send it to right?

So I suppose you uploaded this ID and we were still not convinced then we will extract the address in the ID and send a postcard in the mail to that ID and you get that six digit code. You come back and trade on Coinbase and then you can validate that yes, you actually lived there too. Of course some cases it works and some cases it doesn't work. So of course, you would think that selfies will only work with 20 year old's.

No, there are people on our platform that are far older who are able to use selfie. However, in some cases you know, there is other attacks that became across. We don't require ID verification or the lowest risk tier users where the rest score is defined, is learned from machine learning right?

Also, we don't require CDV, we do require CVV for most of them but CDV for card verification where you again do the micro deposits, we don't require that either for certain low risk tier users. Also, address verification, we don't require that for certain risk, low risk tier users so yeah.

We're constantly playing with that. I really wish we had a central repository of you know, retinal scans as well as you know, thumb prints which any of us could access right? Unfortunately the US doesn't have anything just like that yet. However in India is actually leap frogging the rest of the world there. They're storing like 10 fingerprints and retinal scans of a billion people.

It's built by a nonprofit and the Indian government released an app January of this year, and even can call the database to truly verify who that person is. Question?

[0:41:14.6] JM: A lot of this stuff is predicated on the fact as you said that these scammers will share stuff so readily with each other? Why is that, why are they so willing to share the different mechanisms whenever somebody discovers a new route into scanning the system, they just share it with everybody else?

[0:41:33.0] SR: It's then somebody will build a tool and sell that tool, that's one method.

[0:41:39.2] JM: The dark web and use the passwords along it? GPUS to attack on some forms?

[0:41:45.0] SR: There's dark net forums right? Where they're discussing all of this.

[0:41:51.1] MALE: They buy it as a service, the passwords to certain people and you could buy them and compute too.

[0:42:00.3] SR: I think Jeff is leaning towards the methods, right?

[0:42:03.5] JM: I'm just was wondering why these people are willing to share –

[0:42:05.9] SR: The methods?

[0:42:06.5] JM: To share the methods, yes.

[0:42:07.9] SR: I don't think they're explicitly sharing for charity purposes, they probably are charging people by telling them you know, "hey, I have this proof, look at my screenshot of Coinbase, I stole this money. You pay me $10 and I'll tell you how I did it."

[0:42:22.0] MALE: They're using product ties into all that? Literally they build a tool for it, you read the tool, if you din't know how to get the login and password, you can buy I did it. Then if you need compute to attack like block chain or other by GPUS. And they read it as a cloud available that's incredible while you're trying other places, we just paper use it.

[0:42:45.3] SR: Yeah, question over there?

[0:42:46.7] MALE: Yeah, I love your question, once you use a tool enough times it becomes detectable and therefore it's like kind of you got your worth out of it and then you would want to sell that to other people, so you're kind of milking the cow.

[0:42:57.3] SR: Yeah. And during the gold rush, the people who made the money were the ones making the shovels, right?

[0:43:04.7] MALE: And Wells Fargo protecting it.

[0:43:07.4] SR: Yeah. Cool, I wanted to say one thing. I have two more slides and then I can take all the questions at the end of it right? One very interesting thing is, you know, you see that guy holding the phone right? There's a new kind of attack that I didn't even tell you about, it's a socially engineered text scam attack.

Elderly people are called and they're told that you know, "hey, you got a virus on your computer, I can remove it if you pay me in bit coins. In order for you to pay me with bit coins, you know, you have to go to coinbase.com or some other district exchange, clear the site, you know, upload your ID," hence that ID right? Hence that ID. The only way we can detect it one way is basically there's always a phone behind the ID right?

They are on the phone, the guy creating the accent, the victim is on the phone with the attacker right? Another application of computer vision, deep learning that we would love to explore, we've started taking a stab at it which is identifying objects inside dimensions right?

Then, you know, sometimes when you ask people to give us their selfies right? They go to great lengths, sometimes you can of course fake selfies right? You can take a high resolution printed image and put it in front of the webcam right? This is what someone did. This is a scrape from social media, we asked this attacker to upload three fingers and write the date and Coinbase, expertly photoshoped over there right? Our agents though, found the identity made on social media.

Yeah, sometimes they do the pretty chubby job right? that's a photoshop, happened a week ago. Yeah, I don't know what they were thinking. Yeah, I covered a variety of topics you know about how do you secure yourself, how do you protect yourself et cetera. There's one last thing I want to tell you which is PSA. Public service on one's announcement.

If you're on Coinbase, then you're all set. I can't take over somebody about it, please create a Coinbase, trade freely, buy you a digital currency, we will protect you but there are lots of sites out there who still support the service based to a fee who are not as you know, advanced or don't take security as seriously.

We like to think of ourselves as a security first company which just happens to be selling digital currency right? To protect yourself, please call up your Telco's, put a sim lock, tell them you're already hacked and no one should be able to port your phone number to a new device right? Unless you walk into a store and show your ID right?

That's the only way to protect yourself. If you are an android user or like android, move to Google Fi which is basically Google's phone service because there's more call centers, no social endangering right? You prevent that phone porting attack vector.

Second thing, but if you do end up being a Google customer, you are signing your life over to Google which is if you're using Gmail as well as you know, Google Fi, then your two factor have one right? Because if somebody now has access to your Google password right? You know, someone manages to get access to still port – they can still port your phone number from Google to another carrier right?

If they have access to your phone number, your Google password. The most secure form of online production that we can think of is of course UB keys right? As the second factor, if not that then use Google Fi but secure your Google account with Google authenticator right?

Because if you secure your Google account with Google authenticator then they have to physically steal your device which has the Google authenticator accounts.

[0:46:53.3] MALE: What's UB Keys?

[0:46:54.3] SR: UB keys are these micro USB keys which will generate the six digit codes right? But you have them with you physically. It's what to a favor's meant to be. Something you have right?

Cool, so last slide, this is our day time risk team, 15 people, eight engineers, seven analysts, we're looking for machine learning engineers, data engineers and data analyst, that's my email address soups@coinbase.com. Some information about what I talked is on blog.coinbase.com.

[END]