sixgill

SIXGILL REPORT

TERMS AND CONDITIONS APPLY

Refund Fraud on the Dark Web

NOVEMBER 24, 2020

Terms and Conditions Apply: Refund Fraud on the Dark Web

EXECUTIVE SUMMARY

- As e-commerce sees growth during the COVID-19 pandemic, the fraud phenomenon of refunding - seeking undeserved refunds from e-commerce vendors - has similarly boomed. Underground mentions of the phenomenon reached record highs in July 2020.
- Refunding leverages an understanding of the technical weaknesses of customer support and courier services, as well as social engineering.
- Loosened shipping protocols as a result of hygiene concerns and social distancing have piqued social engineers' interest in refunding.
- Similarly, the fears, uncertainties and sympathies aroused by the COVID-19 pandemic have lent themselves to effective social engineering.
- Some refunding methods such as "boxing" and "false tracking ID" (FTID) are frequently outsourced to a growing service sector of such fraud advertising on the dark web and instant messaging.
- Discourse on the deep and dark web, as well as manuals circulating on paste and file-sharing sites, reveal evolving threat actor best-practices for refunding, including targeted vulnerabilities.
- Amazon, Apple and Walmart are the top three e-commerce vendors targeted by fraudster refunders.

INTRODUCTION

The COVID-19 pandemic has been a boon to e-commerce with Amazon's Q3 financials revealing 37% year-on-year sales growth worldwide and 39% in North America. With the holiday season approaching and no end to the pandemic in sight, consumers are deterred from brick-and-mortar shopping and keen to turn to online shopping to stock up their holiday gift baskets.[1]

On the cyber underground, threat actors seek to fraudulently profit from the e-commerce boom. In particular, a tactic called refunding is growing in popularity. Refunding, which involves defrauding e-commerce vendors by claiming undeserved refunds, exploits both couriers and retailers, seizing on technical loopholes in delivery and customer support services while leveraging emotionally manipulative social engineering. This phenomenon witnessed a peak in underground mentions in July 2020.

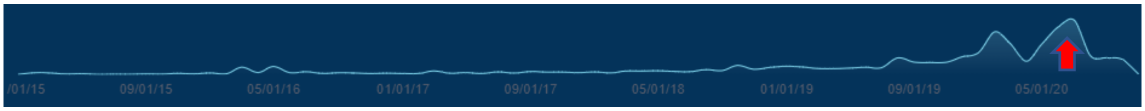


Figure 1: References to refunding scams reach a daily peak in underground mentions (1,752) In July 2020.

This report examines underground discourse of "refunding" trends, tactics and procedures (TTPs), providing an overview of the most common refunding methods deployed by threat actors. The report then drills down into threat actor discourse to identify both the traits and habits that characterize effective social engineering of this sort, and the vulnerabilities that put certain e-commerce vendors more frequently in the crosshairs of threat actors.

Finally, we will examine how COVID-19 has made refunding fraud both easier and more difficult for threat actors. As retailers and "refunders" adapt to the new reality, threat actors' TTPs continue evolving, yet reveal certain perennial truths about social engineering.

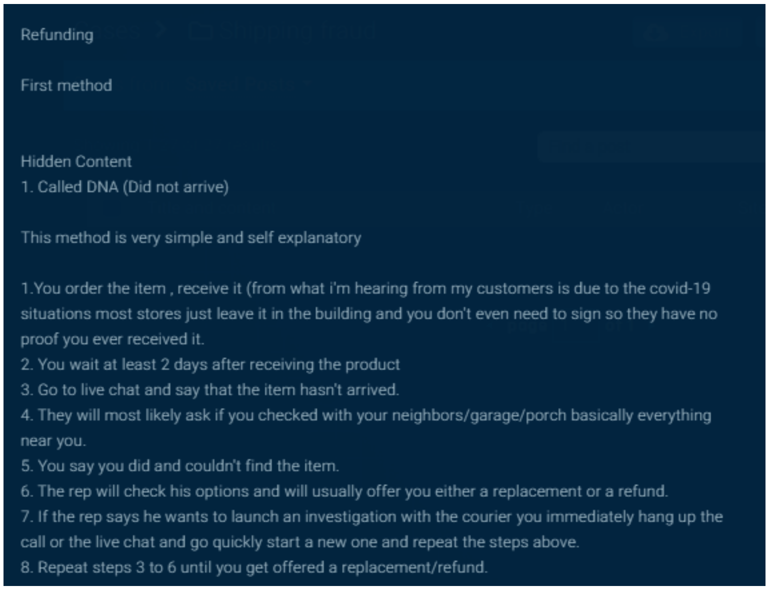
COMMON REFUNDING METHODS

The underground is rife with guides and manuals on refunding methods - some for sale, but many published freely and often anonymously.

[1] https://econsultancy.com/stats-roundup-coronavirus-impact-on-marketing-ecommerce-advertising/

This section gives a brief overview of the most common methods employed by threat-actors and laid out in their "how to" guides.

"Did Not Arrive"/"DNA" – The simplest method of refund fraud involves simply claiming that the package has not arrived. Underground manuals suggest that customer support will likely press you on whether "you checked with your neighbors/garage/porch," but that after enough strenuous denial they will offer you a replacement or refund. An anonymous guide recommends that if the customer service representative says they want to launch an investigation with the courier service, simply hang up and try again.



Refunding

First method

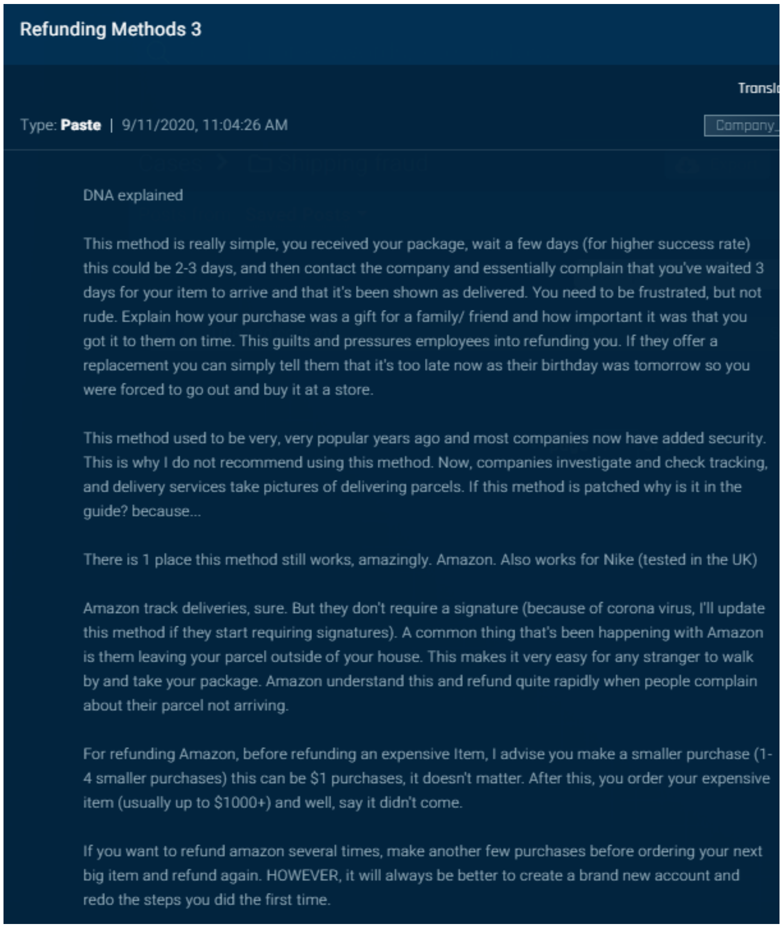
Hidden Content
1. Called DNA (Did not arrive)

This method is very simple and self explanatory

1.You order the item , receive it (from what i'm hearing from my customers is due to the covid-19 situations most stores just leave it in the building and you don't even need to sign so they have no proof you ever received it.
2. You wait at least 2 days after receiving the product
3. Go to live chat and say that the item hasn't arrived.
4. They will most likely ask if you checked with your neighbors/garage/porch basically everything near you.
5. You say you did and couldn't find the item.
6. The rep will check his options and will usually offer you either a replacement or a refund.
7. If the rep says he wants to launch an investigation with the courier you immediately hang up the call or the live chat and go quickly start a new one and repeat the steps above.
8. Repeat steps 3 to 6 until you get offered a replacement/refund.

Figure 2: Anonymously authored refunding guide gives instructions for DNA method, September 11, 2020.

One guide suggests that most e-commerce have caught on to this simple fraud method and have updated their security procedures accordingly. According to the anonymous author of this guide, the method remains relevant for e-commerce giant Amazon.



Refunding Methods 3

Type: **Paste** | 9/11/2020, 11:04:26 AM

DNA explained

This method is really simple, you received your package, wait a few days (for higher success rate) this could be 2-3 days, and then contact the company and essentially complain that you've waited 3 days for your item to arrive and that it's been shown as delivered. You need to be frustrated, but not rude. Explain how your purchase was a gift for a family/ friend and how important it was that you got it to them on time. This guilts and pressures employees into refunding you. If they offer a replacement you can simply tell them that it's too late now as their birthday was tomorrow so you were forced to go out and buy it at a store.

This method used to be very, very popular years ago and most companies now have added security. This is why I do not recommend using this method. Now, companies investigate and check tracking, and delivery services take pictures of delivering parcels. If this method is patched why is it in the guide? because...

There is 1 place this method still works, amazingly. Amazon. Also works for Nike (tested in the UK)

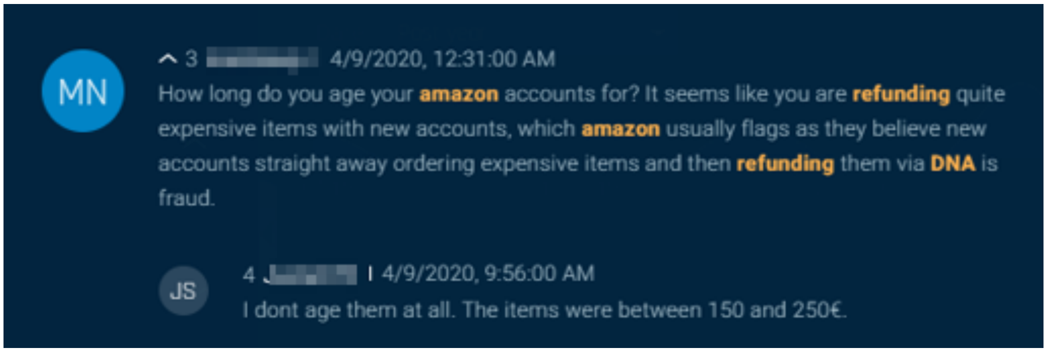
Amazon track deliveries, sure. But they don't require a signature (because of corona virus, I'll update this method if they start requiring signatures). A common thing that's been happening with Amazon is them leaving your parcel outside of your house. This makes it very easy for any stranger to walk by and take your package. Amazon understand this and refund quite rapidly when people complain about their parcel not arriving.

For refunding Amazon, before refunding an expensive Item, I advise you make a smaller purchase (1-4 smaller purchases) this can be $1 purchases, it doesn't matter. After this, you order your expensive item (usually up to $1000+) and well, say it didn't come.

If you want to refund amazon several times, make another few purchases before ordering your next big item and refund again. HOWEVER, it will always be better to create a brand new account and redo the steps you did the first time.

Figure 3: Anonymously authored manual explains relevance of DNA method to Amazon, September 11, 2020.

In order to pull this method off on Amazon, threat actors often recommend using "aged" Amazon accounts; that is, attempting the method with a brand-new account is more likely to raise red-flags, whereas veteran accounts are more likely to receive the trust of customer support representatives.



^ 3 [redacted] 4/9/2020, 12:31:00 AM

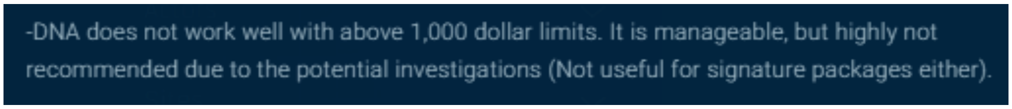
How long do you age your **amazon** accounts for? It seems like you are **refunding** quite expensive items with new accounts, which **amazon** usually flags as they believe new accounts straight away ordering expensive items and then **refunding** them via **DNA** is fraud.

4 [redacted] | 4/9/2020, 9:56:00 AM

I dont age them at all. The items were between 150 and 250€.

Figure 4: Threat actor asks how long to age Amazon accounts for DNA method, April 9, 2020.

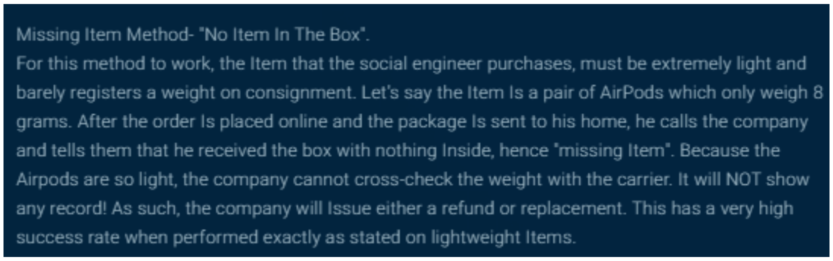
One refunding guide recommends this method for items below $1000. More expensive items are likely to trigger investigations by FedEx or UPS, which, being a drain on resources, are likely to be prioritized for more expensive shipments. More expensive shipments are also more likely to require signature upon delivery.



-DNA does not work well with above 1,000 dollar limits. It is manageable, but highly not recommended due to the potential investigations (Not useful for signature packages either).

Figure 5: Anonymous threat actor cautions keeping DNA method to price limit of $1000, July 26, 2020.

"Empty Box" – This method simply entails claiming that the shipment arrived empty. It is most successful with lightweight items – guides frequently mention Apple AirPods as a choice item – so that the weight cannot be cross-checked with the courier. Seasoned threat actors also recommend indicating to customer support that the box came in excellent condition, lest you trigger an investigation if the retailer senses they can offload the responsibility onto the courier.

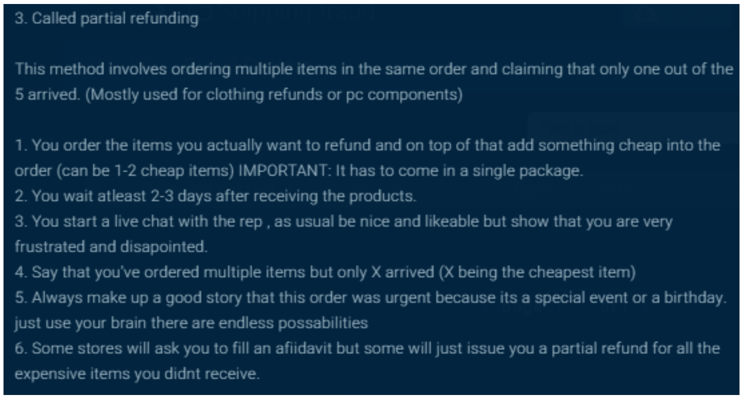


Missing Item Method- "No Item In The Box".

For this method to work, the Item that the social engineer purchases, must be extremely light and barely registers a weight on consignment. Let's say the Item Is a pair of AirPods which only weigh 8 grams. After the order Is placed online and the package Is sent to his home, he calls the company and tells them that he received the box with nothing Inside, hence "missing Item". Because the Airpods are so light, the company cannot cross-check the weight with the carrier. It will NOT show any record! As such, the company will Issue either a refund or replacement. This has a very high success rate when performed exactly as stated on lightweight Items.

Figure 6: Threat actor recommends "empty box" method with Apple AirPods, October 5, 2020.

Partial Refund – This method claims a high success rate and is recommended for large orders. It entails ordering multiple items and claiming only some of them (the cheaper ones) arrived in the box. As with other methods, its success hinges on the social engineer's acting skills. "Always make up a good story that this order was urgent because it's a special event or a birthday," urges the anonymous author of one refunding guide.The same guide recommends using this method on clothing orders with items worth no more than $400.



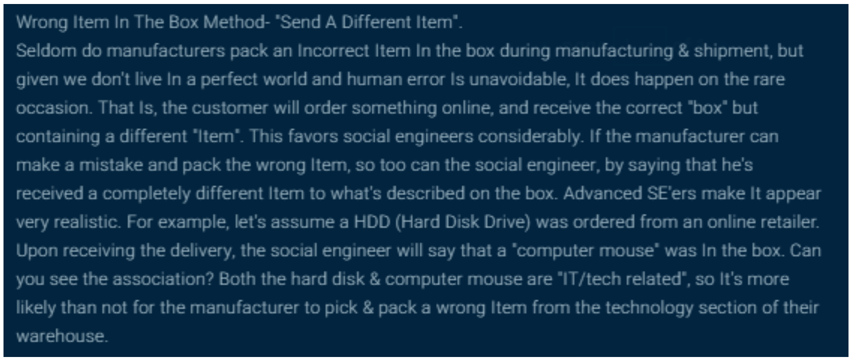
3. Called partial refunding

This method involves ordering multiple items in the same order and claiming that only one out of the 5 arrived. (Mostly used for clothing refunds or pc components)

1. You order the items you actually want to refund and on top of that add something cheap into the order (can be 1-2 cheap items) IMPORTANT: It has to come in a single package.
2. You wait atleast 2-3 days after receiving the products.
3. You start a live chat with the rep , as usual be nice and likeable but show that you are very frustrated and disapointed.
4. Say that you've ordered multiple items but only X arrived (X being the cheapest item)
5. Always make up a good story that this order was urgent because its a special event or a birthday. just use your brain there are endless possabilities
6. Some stores will ask you to fill an afiidavit but some will just issue you a partial refund for all the expensive items you didnt receive.

Figure 7: Anonymously authored guide recommends effective social engineering script for partial refunding method, September 11, 2020.

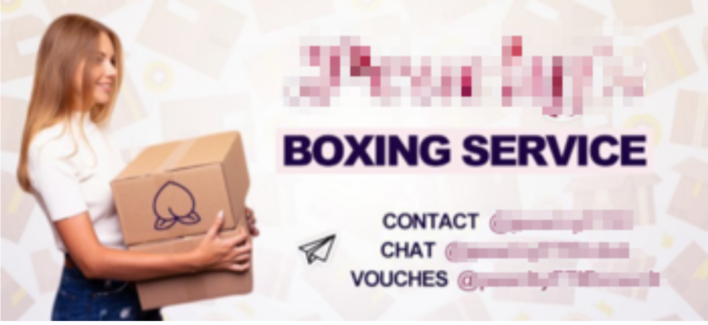
"Wrong Item Arrived"/"Wrong Item In the Box" – Here the social engineer claims the retailer has sent the incorrect item, then return a similar, but much cheaper, item that the retailer stocks in their inventory. Social engineering guides emphasize the psychological components of pulling off this method. "Let's assume a HDD (Hard Disk Drive) was ordered from an online retailer. Upon receiving the delivery, the social engineer will say that a 'computer mouse' was in the box. Can you see the association?" asks a threat actor in his Social Engineering Guide. "Both the hard disk & computer mouse are 'IT/tech related', so it's more likely than not for the manufacturer to pick & pack a wrong item from the technology section of their warehouse."

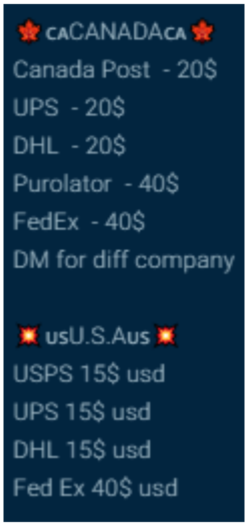


Wrong Item In The Box Method- "Send A Different Item".
Seldom do manufacturers pack an Incorrect Item In the box during manufacturing & shipment, but given we don't live In a perfect world and human error Is unavoidable, It does happen on the rare occasion. That Is, the customer will order something online, and receive the correct "box" but containing a different "Item". This favors social engineers considerably. If the manufacturer can make a mistake and pack the wrong Item, so too can the social engineer, by saying that he's received a completely different Item to what's described on the box. Advanced SE'ers make It appear very realistic. For example, let's assume a HDD (Hard Disk Drive) was ordered from an online retailer. Upon receiving the delivery, the social engineer will say that a "computer mouse" was In the box. Can you see the association? Both the hard disk & computer mouse are "IT/tech related", so It's more likely than not for the manufacturer to pick & pack a wrong Item from the technology section of their warehouse.

Figure 8: Social engineering guide emphasizes psychological dimension of claiming wrong item arrived, September 17, 2020.

"Boxing" – This method entails contacting the retailer's customer support to claim an item is defective, then returning the box without the purchased item and claiming the item got stolen during delivery. Since packages are weighed during shipment, social engineers generally place dry ice of equivalent weight, then tamper with the box so as to give the impression that the box had been tampered with during transit. There are professional social engineering services that charge a premium of as little as $15 to "box" an item, taking on the risk of performing this fraud at the post office.

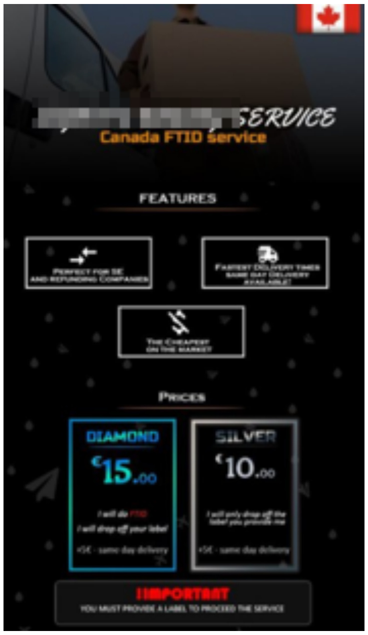



caCANADAca
Canada Post - 20$
UPS - 20$
DHL - 20$
Purolator - 40$
FedEx - 40$
DM for diff company

usU.S.Aus
USPS 15$ usd
UPS 15$ usd
DHL 15$ usd
Fed Ex 40$ usd

Figures 9 and 10: A boxing service advertised on instant messaging platform, August 14, 2020; threat actor advertises boxing service pricing on instant messaging platform, July 13, 2020.

False Tracking ID/FTID – Similar to the boxing method, the FTID method requires first arranging for the return shipment of an item (be it because the item is allegedly damaged, you no longer need it, etc.). The social engineer then edits the prepaid return shipping label, usually downloaded as a PDF from the retailer, so that postal delivery tracking *falsely* indicates the goods have returned to the vendor. As with boxing, this often entails outsourcing the editing to a third-party service (an "FTID" service or "vouched label editor.") Often this service is an add-on to a boxing service.


[redacted] SERVICE
Canada FTID service

FEATURES

Perfect for SE and refunding companies

Fastest delivery times same day delivery available!

The cheapest on the market

Prices

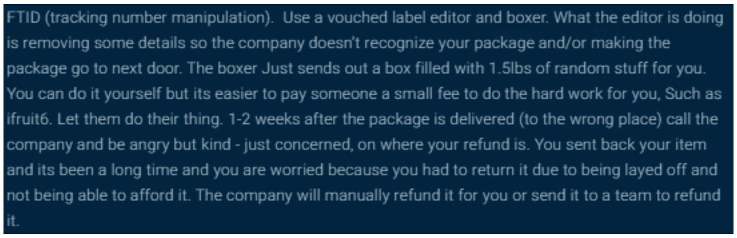
DIAMOND
€15.00
I will do FTID
I will drop off your label
+5€ - same day delivery

SILVER
€10.00
I will only drop off the label you provide me
+5€ - same day delivery

!!IMPORTANT
YOU MUST PROVIDE A LABEL TO PROCEED THE SERVICE

Figure 11: Boxing service operating in Canada offers FTID add-on, May 20, 2020.

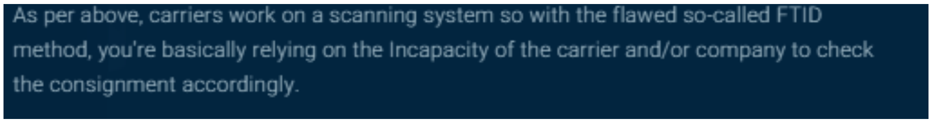
The anonymous author of one refunding guide explains: "You can do it yourself but it's easier to pay someone a small fee to do the hard work for you....1-2 weeks after the package is delivered (to the wrong place) call the company and be angry but kind – just concerned, on where your refund is. You sent back your item and it's been a long time and you are worried because you had to return it due to being layed [sic] off and not being able to afford it." Here, too, the technical method is only as strong as the emotional manipulation powering it to completion.



FTID (tracking number manipulation). Use a vouched label editor and boxer. What the editor is doing is removing some details so the company doesn't recognize your package and/or making the package go to next door. The boxer Just sends out a box filled with 1.5lbs of random stuff for you. You can do it yourself but its easier to pay someone a small fee to do the hard work for you, Such as ifruit6. Let them do their thing. 1-2 weeks after the package is delivered (to the wrong place) call the company and be angry but kind - just concerned, on where your refund is. You sent back your item and its been a long time and you are worried because you had to return it due to being layed off and not being able to afford it. The company will manually refund it for you or send it to a team to refund it.

Figure 12: Anonymous author manual emphasizes that success of FTID method rests on emotional manipulation, July 11, 2020.

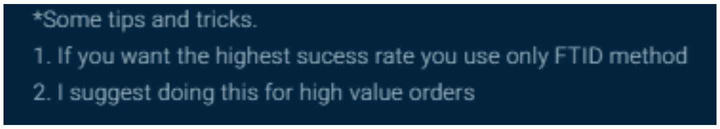
A threat actor on one closed deep web forum suggests the FTID method only works with large retailers that do not cross-check the receipt of the consignment, but only that the tracking ID has arrived.



As per above, carriers work on a scanning system so with the flawed so-called FTID method, you're basically relying on the Incapacity of the carrier and/or company to check the consignment accordingly.

Figure 13: Threat actor suggests FTID method for targeting large retailers, September 16, 2020.

One guide suggests that "if you want the highest success rate you use only FTID method," and that this is the preferred method for high-value orders.



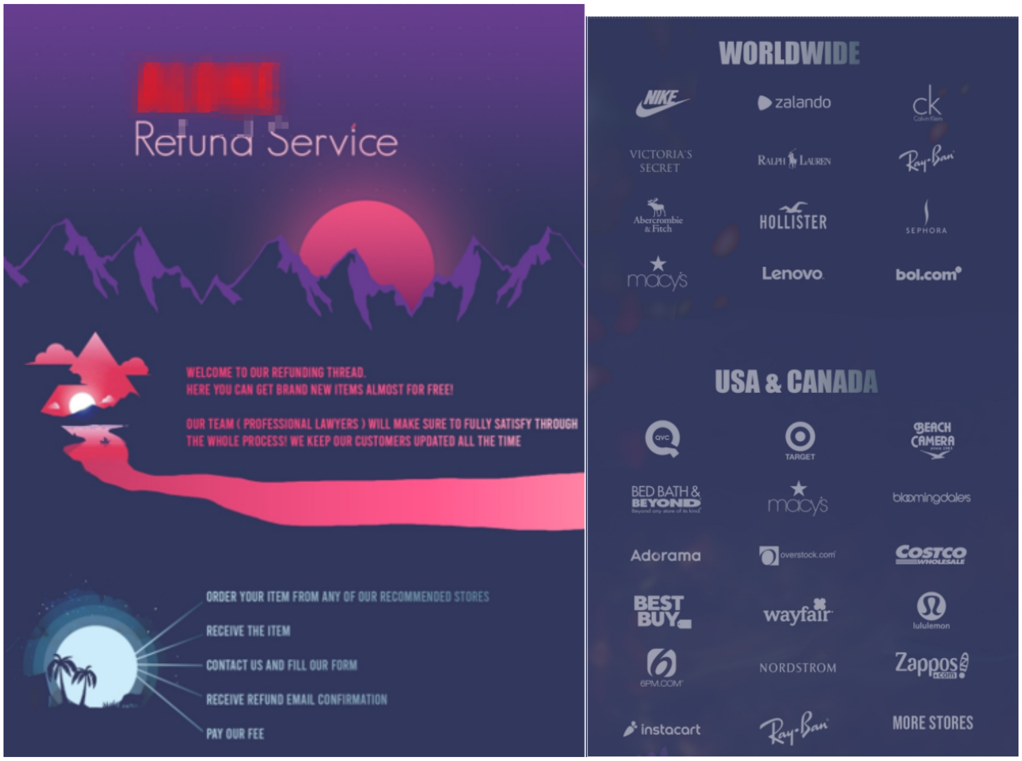
*Some tips and tricks.

1. If you want the highest sucess rate you use only FTID method
2. I suggest doing this for high value orders

Figure 14: Anonymous threat actor recommends FTID method for high-value orders, September 11, 2020.

SHOP TALK: "GREED IS THE BIGGEST MISTAKE A SOCIAL ENGINEER CAN MAKE"

The underground discourse of threat actors peddling their refunding services, as well as threat actors refunding exchanging tips and best practices, reveals that certain e-commerce vendors more frequently attract the attention of threat actors. In the past year, Amazon attracted the most threat actor attention, followed by Apple and Walmart. This attention inevitably relates to the size and popularity of these retailers, but a study of underground refunding manuals reveals that social engineers are acutely attuned to the unique weaknesses and protocols of different retailers, sharing advice on which retailers to target by which methods - and for how much.



[redacted] Refund Service

WELCOME TO OUR REFUNDING THREAD.
HERE YOU CAN GET BRAND NEW ITEMS ALMOST FOR FREE!

OUR TEAM (PROFESSIONAL LAWYERS) WILL MAKE SURE TO FULLY SATISFY THROUGH THE WHOLE PROCESS! WE KEEP OUR CUSTOMERS UPDATED ALL THE TIME

- ORDER YOUR ITEM FROM ANY OF OUR RECOMMENDED STORES
- RECEIVE THE ITEM
- CONTACT US AND FILL OUR FORM
- RECEIVE REFUND EMAIL CONFIRMATION
- PAY OUR FEE

WORLDWIDE

USA & CANADA

MORE STORES

Figures 15 and 16: Threat actor advertises refunding service - "FTID, boxing & more methods" October 13, 2020. The threat actor highlights which retailers he can target with his services.

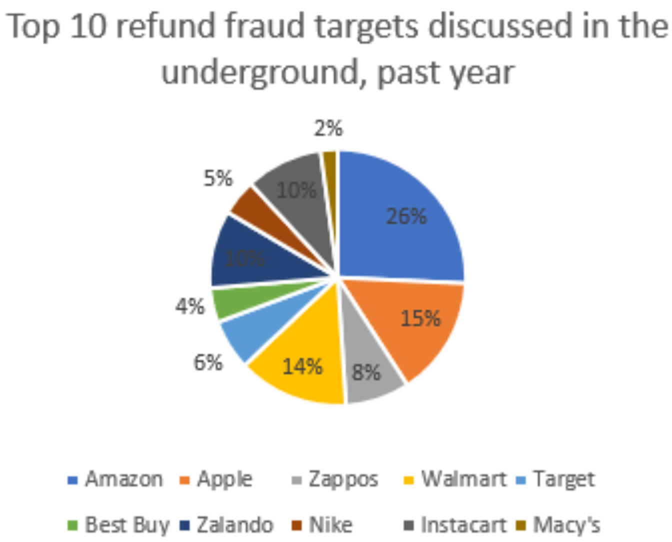
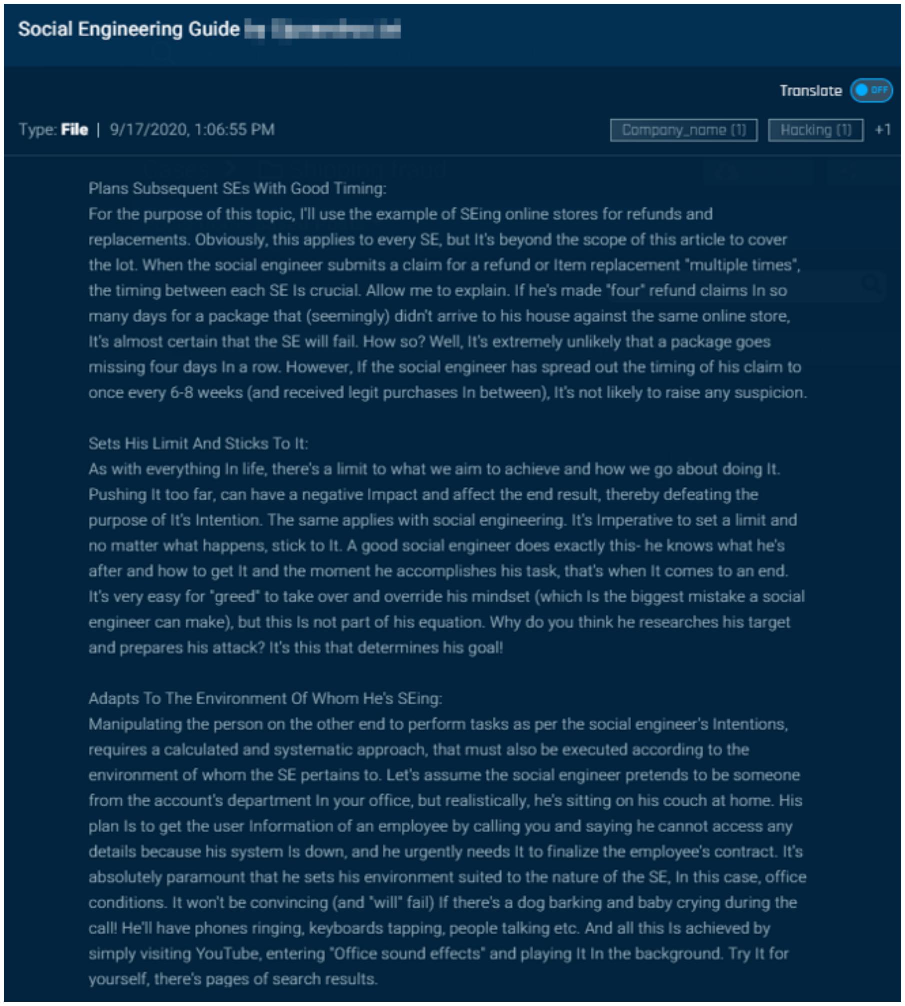


Figure 17: Distribution of top 10 refunding targets discussed on the underground in English over the past year.

Under the guise of "getting into the mind of a social engineer," one threat actor's comprehensive social engineering guide ticks off the traits that make a successful social engineer. "The social engineer can be an absolute genius with his research and information gathering, as well as having an exceptional set of skills when preparing and executing his attack, but this means very little if he's lacking in confidence," he writes. A good social engineer manipulates his victim by "assuming an authoritative figure" and taking control of the situation.

Sounding not unlike a guerrilla combat manual, the threat actor recommends perseverance, an ability to improvise, avoiding over-complicating the situation, and having a solid exit strategy, meaning to finish off the attack on a polite note without raising suspicion and not timing the next attack too soon. "It's imperative to set a limit and no matter what happens, stick to it. A good social engineer…knows what he's after and how to get it and the moment he accomplishes his task, that's when it comes to an end." Greed, he writes, "is the biggest mistake a social engineer can make."



Social Engineering Guide [redacted]

Type: File | 9/17/2020, 1:06:55 PM

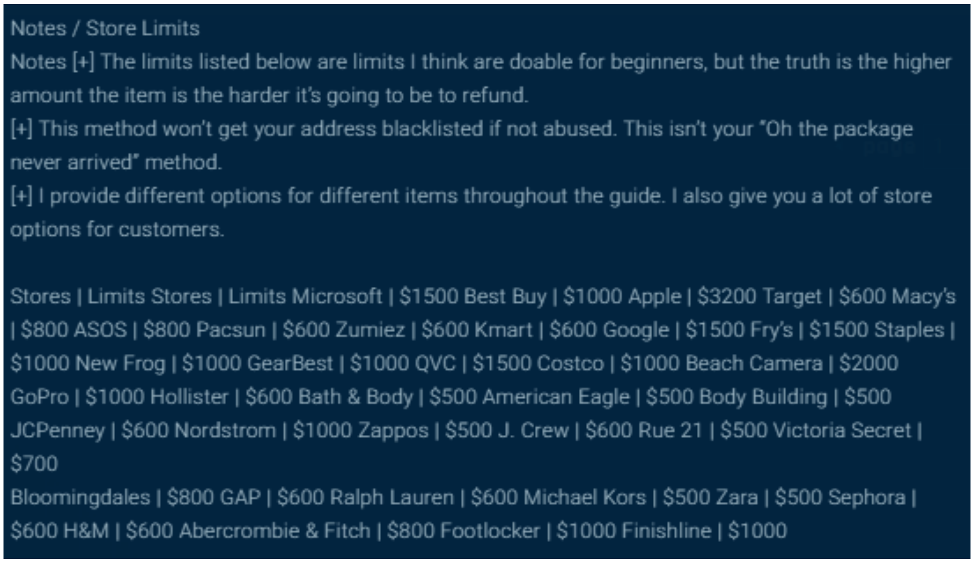
Plans Subsequent SEs With Good Timing:
For the purpose of this topic, I'll use the example of SEing online stores for refunds and replacements. Obviously, this applies to every SE, but It's beyond the scope of this article to cover the lot. When the social engineer submits a claim for a refund or Item replacement "multiple times", the timing between each SE Is crucial. Allow me to explain. If he's made "four" refund claims In so many days for a package that (seemingly) didn't arrive to his house against the same online store, It's almost certain that the SE will fail. How so? Well, It's extremely unlikely that a package goes missing four days In a row. However, If the social engineer has spread out the timing of his claim to once every 6-8 weeks (and received legit purchases In between), It's not likely to raise any suspicion.

Sets His Limit And Sticks To It:
As with everything In life, there's a limit to what we aim to achieve and how we go about doing It. Pushing It too far, can have a negative Impact and affect the end result, thereby defeating the purpose of It's Intention. The same applies with social engineering. It's Imperative to set a limit and no matter what happens, stick to It. A good social engineer does exactly this- he knows what he's after and how to get It and the moment he accomplishes his task, that's when It comes to an end. It's very easy for "greed" to take over and override his mindset (which Is the biggest mistake a social engineer can make), but this Is not part of his equation. Why do you think he researches his target and prepares his attack? It's this that determines his goal!

Adapts To The Environment Of Whom He's SEing:
Manipulating the person on the other end to perform tasks as per the social engineer's Intentions, requires a calculated and systematic approach, that must also be executed according to the environment of whom the SE pertains to. Let's assume the social engineer pretends to be someone from the account's department In your office, but realistically, he's sitting on his couch at home. His plan Is to get the user Information of an employee by calling you and saying he cannot access any details because his system Is down, and he urgently needs It to finalize the employee's contract. It's absolutely paramount that he sets his environment suited to the nature of the SE, In this case, office conditions. It won't be convincing (and "will" fail) If there's a dog barking and baby crying during the call! He'll have phones ringing, keyboards tapping, people talking etc. And all this Is achieved by simply visiting YouTube, entering "Office sound effects" and playing It In the background. Try It for yourself, there's pages of search results.

Figure 18: Social engineering manual sketches out the character traits and habits necessary to successful refund scamming, September 17, 2020.

It is precisely the limits of social engineering – so critical, in this threat actor's eyes, to its success – that occupies much of the underground shop-talk by refund scammers. An anonymously authored guide lists the upper limits of scams "doable for beginners" at different online stores. By this analysis, the most vulnerable company is Apple, which could be scammed for as much as $3,200. Of fashion retailers, Footlocker leads the pack, with this guide suggesting they could be scammed for as much as $1,000.

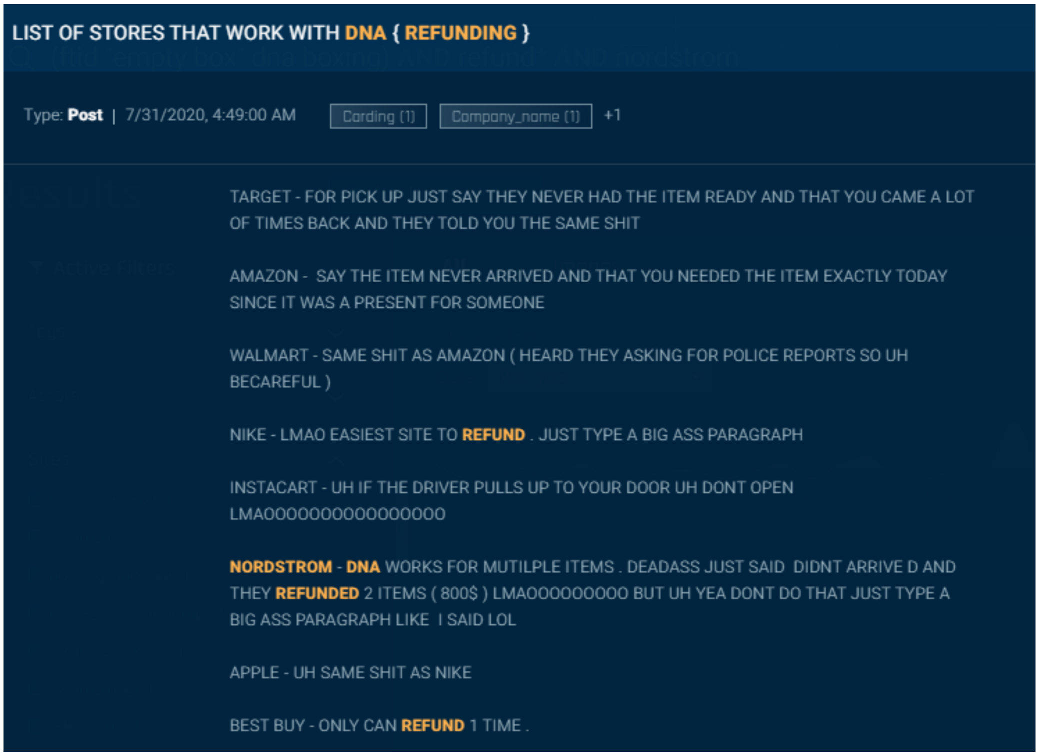


Notes / Store Limits
Notes [+] The limits listed below are limits I think are doable for beginners, but the truth is the higher amount the item is the harder it's going to be to refund.
[+] This method won't get your address blacklisted if not abused. This isn't your "Oh the package never arrived" method.
[+] I provide different options for different items throughout the guide. I also give you a lot of store options for customers.

Stores | Limits Stores | Limits Microsoft | $1500 Best Buy | $1000 Apple | $3200 Target | $600 Macy's | $800 ASOS | $800 Pacsun | $600 Zumiez | $600 Kmart | $600 Google | $1500 Fry's | $1500 Staples | $1000 New Frog | $1000 GearBest | $1000 QVC | $1500 Costco | $1000 Beach Camera | $2000 GoPro | $1000 Hollister | $600 Bath & Body | $500 American Eagle | $500 Body Building | $500 JCPenney | $600 Nordstrom | $1000 Zappos | $500 J. Crew | $600 Rue 21 | $500 Victoria Secret | $700
Bloomingdales | $800 GAP | $600 Ralph Lauren | $600 Michael Kors | $500 Zara | $500 Sephora | $600 H&M | $600 Abercrombie & Fitch | $800 Footlocker | $1000 Finishline | $1000

Figure 19: Anonymously authored guide indicates upper limits for refunding scams of various retailers, September 11, 2020.

Threat actors also share tips as to which online stores to target by which methods. Posting in July 2020, a threat actor on one hacking forum shared a list of online retailers targetable by the "DNA" (did not arrive) method. He singled out Nike as the "easiest site to refund" alongside Apple. With Amazon, he recommends pressuring customer support with a sob story about needing the purchased item today as it was a gift; similarly for Walmart, except there he suggests treading with caution, as they're more likely to involve the police. With Best Buy he suggests you can only employ the DNA method once, but Nordstrom is allegedly less vigilant about repeat offenders.



LIST OF STORES THAT WORK WITH **DNA** { **REFUNDING** }

Type: **Post** | 7/31/2020, 4:49:00 AM Carding (1) Company_name (1) +1

TARGET - FOR PICK UP JUST SAY THEY NEVER HAD THE ITEM READY AND THAT YOU CAME A LOT OF TIMES BACK AND THEY TOLD YOU THE SAME SHIT

AMAZON - SAY THE ITEM NEVER ARRIVED AND THAT YOU NEEDED THE ITEM EXACTLY TODAY SINCE IT WAS A PRESENT FOR SOMEONE

WALMART - SAME SHIT AS AMAZON (HEARD THEY ASKING FOR POLICE REPORTS SO UH BECAREFUL)

NIKE - LMAO EASIEST SITE TO **REFUND** . JUST TYPE A BIG ASS PARAGRAPH

INSTACART - UH IF THE DRIVER PULLS UP TO YOUR DOOR UH DONT OPEN LMAOOOOOOOOOOOOOOOO

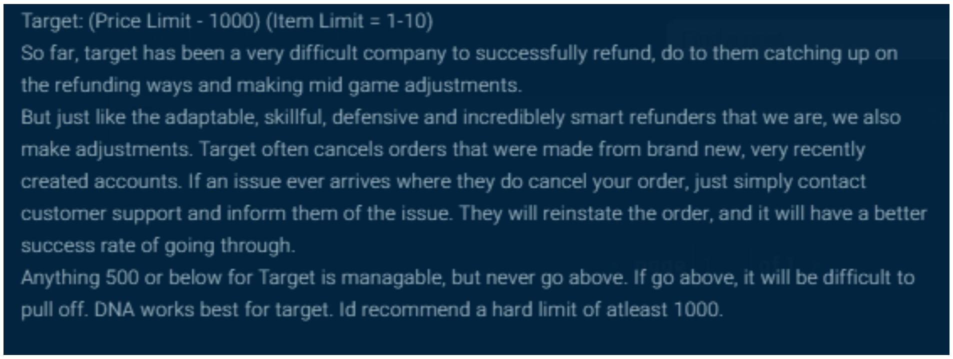
NORDSTROM - **DNA** WORKS FOR MUTILPLE ITEMS . DEADASS JUST SAID DIDNT ARRIVE D AND THEY **REFUNDED** 2 ITEMS (800$) LMAOOOOOOOOOO BUT UH YEA DONT DO THAT JUST TYPE A BIG ASS PARAGRAPH LIKE I SAID LOL

APPLE - UH SAME SHIT AS NIKE

BEST BUY - ONLY CAN **REFUND** 1 TIME .

Figure 20: Threat actor lists stores to target with DNA method, July 31, 2020.

Some companies are consistently singled out as difficult targets to refund scam. Target, for instance, is singled out by the anonymous author of one refunding guide a "very difficult company to successfully refund" due to them "catching up…and making mid-game adjustments."

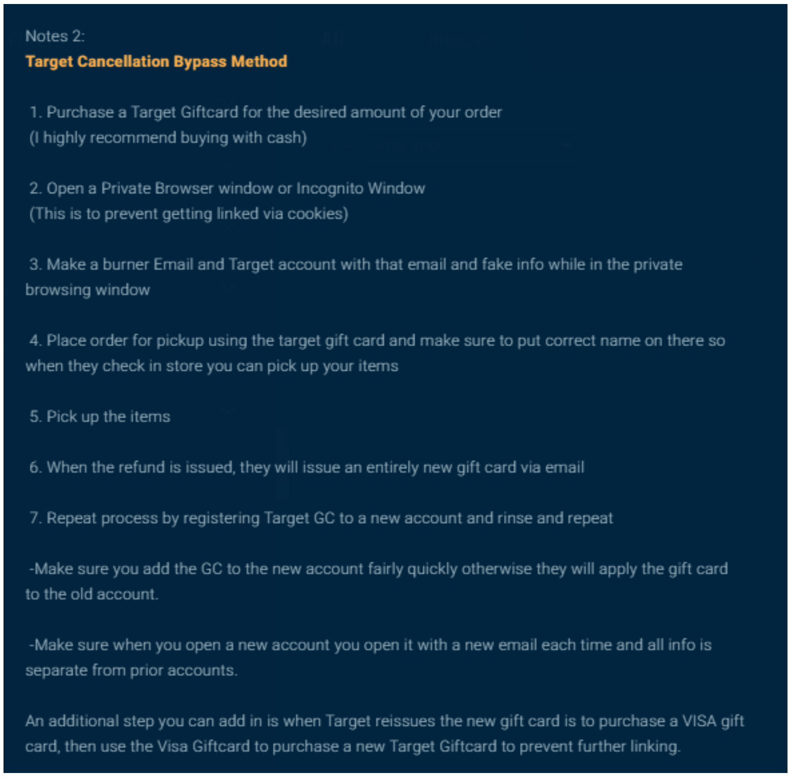


Target: (Price Limit - 1000) (Item Limit = 1-10)
So far, target has been a very difficult company to successfully refund, do to them catching up on the refunding ways and making mid game adjustments.
But just like the adaptable, skillful, defensive and incrediblely smart refunders that we are, we also make adjustments. Target often cancels orders that were made from brand new, very recently created accounts. If an issue ever arrives where they do cancel your order, just simply contact customer support and inform them of the issue. They will reinstate the order, and it will have a better success rate of going through.
Anything 500 or below for Target is managable, but never go above. If go above, it will be difficult to pull off. DNA works best for target. Id recommend a hard limit of atleast 1000.

Figure 21: Anonymous author of refunding guide offers refunding victim landscape, September 28, 2020.

The threat actor takes Target's vigilance as a challenge – "just like the adaptable, skillful, defensive and incredibly smart refunders that we are, we also make adjustments" – exemplifying the iterative cat-and-mouse game between social engineers and their victims.

Indeed, as if to spite Target, the same guide includes as an annex a "Target Cancellation Bypass Method," recommending purchasing a Target gift card; making a burner email and Target account with said email while in a private browsing window; placing an order using the Target gift card; arrange for a refund, which Target will issue in the form of a gift card; register this gift card to an entirely new burner email and Target account; "rinse and repeat."



Notes 2:
Target Cancellation Bypass Method

1. Purchase a Target Giftcard for the desired amount of your order
(I highly recommend buying with cash)

2. Open a Private Browser window or Incognito Window
(This is to prevent getting linked via cookies)

3. Make a burner Email and Target account with that email and fake info while in the private browsing window

4. Place order for pickup using the target gift card and make sure to put correct name on there so when they check in store you can pick up your items

5. Pick up the items

6. When the refund is issued, they will issue an entirely new gift card via email

7. Repeat process by registering Target GC to a new account and rinse and repeat

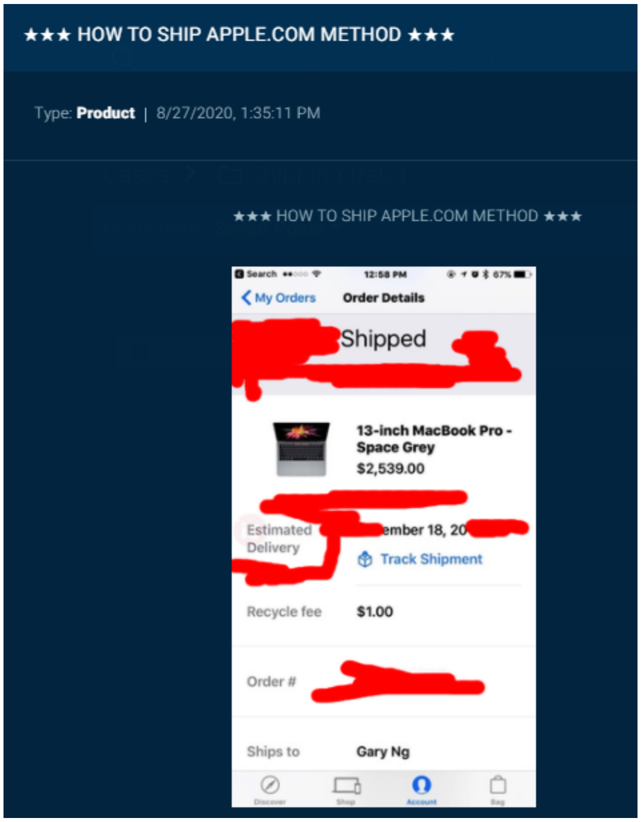
-Make sure you add the GC to the new account fairly quickly otherwise they will apply the gift card to the old account.

-Make sure when you open a new account you open it with a new email each time and all info is separate from prior accounts.

An additional step you can add in is when Target reissues the new gift card is to purchase a VISA gift card, then use the Visa Giftcard to purchase a new Target Giftcard to prevent further linking.

Figure 22: Anonymous author of refunding guide offers a customized method for refund scamming Target, September 28, 2020.

Sometimes threat actors detect a vulnerability for social engineering around a certain product launch or busy season. One alleged "Apple.com method" simply hinges on taking advantage of Apple's allegedly loosened security as it tries "to cope with the millions of people trying to preorder the new iPhone."



★★★ HOW TO SHIP APPLE.COM METHOD ★★★

Type: **Product** | 8/27/2020, 1:35:11 PM

★★★ HOW TO SHIP APPLE.COM METHOD ★★★

[redacted] Shipped

13-inch MacBook Pro - Space Grey
$2,539.00

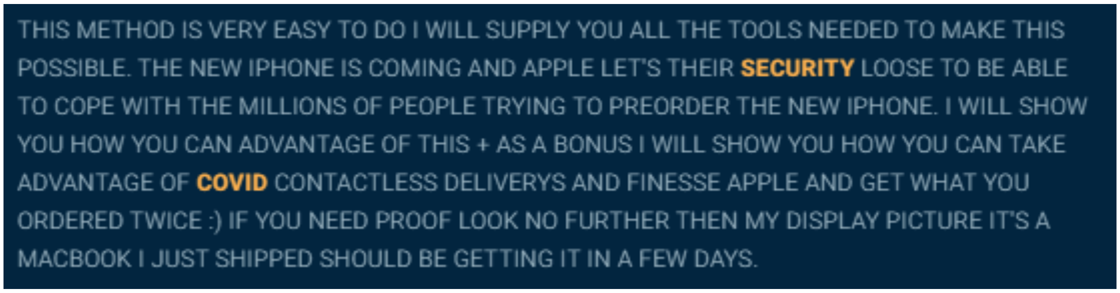
Estimated Delivery [redacted]

Track Shipment

Recycle fee $1.00

Order # [redacted]

Ships to Gary Ng

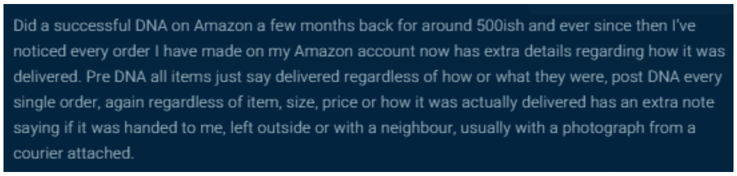


THIS METHOD IS VERY EASY TO DO I WILL SUPPLY YOU ALL THE TOOLS NEEDED TO MAKE THIS POSSIBLE. THE NEW IPHONE IS COMING AND APPLE LET'S THEIR **SECURITY** LOOSE TO BE ABLE TO COPE WITH THE MILLIONS OF PEOPLE TRYING TO PREORDER THE NEW IPHONE. I WILL SHOW YOU HOW YOU CAN ADVANTAGE OF THIS + AS A BONUS I WILL SHOW YOU HOW YOU CAN TAKE ADVANTAGE OF **COVID** CONTACTLESS DELIVERYS AND FINESSE APPLE AND GET WHAT YOU ORDERED TWICE :) IF YOU NEED PROOF LOOK NO FURTHER THEN MY DISPLAY PICTURE IT'S A MACBOOK I JUST SHIPPED SHOULD BE GETTING IT IN A FEW DAYS.

Figures 23 and 24: Threat actor offers "Apple.com method" for refunding, exploiting launch of new iPhone, August 27, 2020.

COVID-19 AND REFUNDING: "THE EMOTIONAL VECTOR OF ATTACK IS WIDE OPEN"

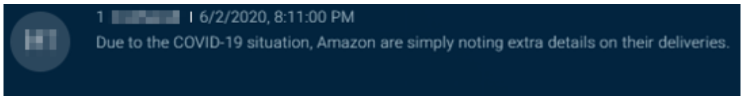
Posting in early June 2020, a threat actor on a closed forum noted that after performing a refunding scam, every delivery from Amazon comes attached with “an extra note saying if it was handed to me, left outside or with a neighbour, usually with a photograph from a courier attached.” Is this new company policy, he asked, or had his account been flagged of his mischief?



Did a successful DNA on Amazon a few months back for around 500ish and ever since then I've noticed every order I have made on my Amazon account now has extra details regarding how it was delivered. Pre DNA all items just say delivered regardless of how or what they were, post DNA every single order, again regardless of item, size, price or how it was actually delivered has an extra note saying if it was handed to me, left outside or with a neighbour, usually with a photograph from a courier attached.

Figure 25: Threat actor worries Amazon had flagged his account after successfully pulling off DNA scam, June 2, 2020.

In response, another threat actor counseled that, in light of the COVID-19 situation, Amazon is noting extra details on its deliveries.

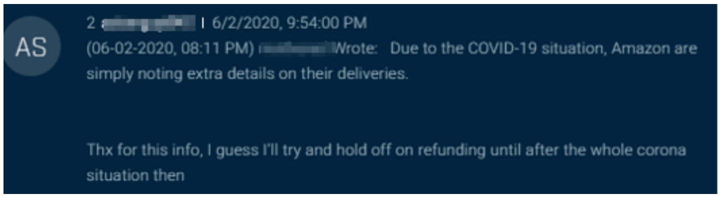


1 [redacted] | 6/2/2020, 8:11:00 PM

Due to the COVID-19 situation, Amazon are simply noting extra details on their deliveries.

Figure 26: Threat actor notes Amazon deliveries noting extra details during the COVID-19 pandemic, June 2, 2020.

One forum member took this update as an indication to “hold off on refunding until after the whole corona situation.”



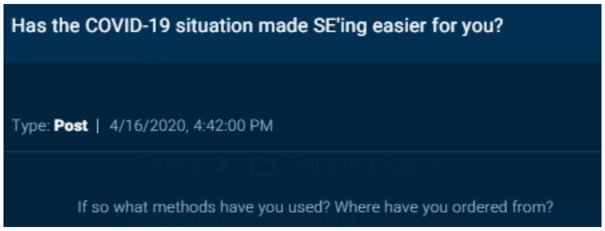
2 [redacted] | 6/2/2020, 9:54:00 PM

(06-02-2020, 08:11 PM) [redacted] Wrote: Due to the COVID-19 situation, Amazon are simply noting extra details on their deliveries.

Thx for this info, I guess I'll try and hold off on refunding until after the whole corona situation then

Figure 27: Threat actor decides to suspend refunding activities during the COVID-19 pandemic, June 2, 2020.

The exchange highlights the whack-a-mole dynamics at play for refund scammers during the COVID-19 pandemic. It creates the perfect storm of panic, uncertainty, and an increasing reliance on virtual shopping (as opposed to brick-and-mortar) which makes online retailers more vulnerable. Their increased vigilance, in turn, deters some social engineers, while it drives others to concoct even more sophisticated refunding methods.



Has the COVID-19 situation made SE'ing easier for you?

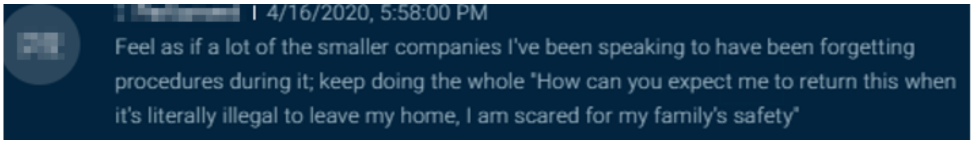
Type: **Post** | 4/16/2020, 4:42:00 PM

If so what methods have you used? Where have you ordered from?

Figure 28: Threat actorstarts thread on COVID-19's effects on social engineering, April 16, 2020.

Some threat actors suggest that the new social dynamics taking shape around COVID-19 lend themselves to the emotional manipulation key to effective social engineering.

In a thread titled "Has the COVID-19 situation made SE'ing easier for you?" on one closed forum, a threat actor suggests it has been easier to convince retailers to issue a refund without returning the allegedly damaged item; 'Keep doing the whole 'How can you expect me to return this when it's literally illegal to leave my home, I am scared for my family's safety," they wrote.

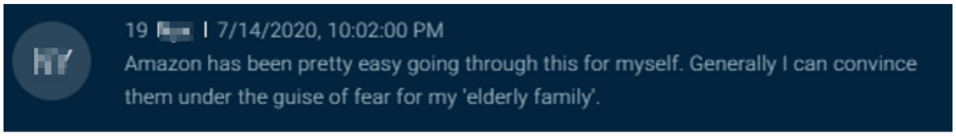


[redacted] | 4/16/2020, 5:58:00 PM

Feel as if a lot of the smaller companies I've been speaking to have been forgetting procedures during it; keep doing the whole "How can you expect me to return this when it's literally illegal to leave my home, I am scared for my family's safety"

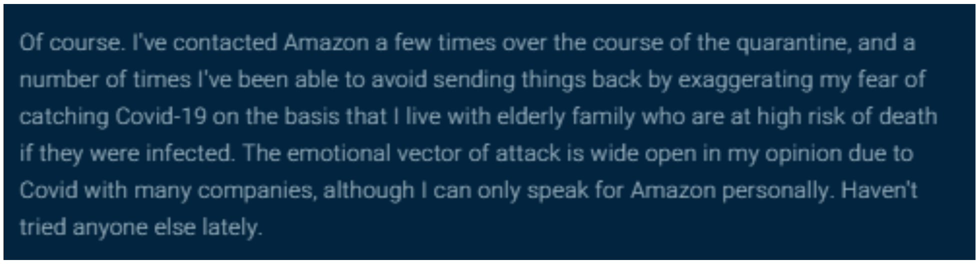
Figure 29: Threat actor claims to take advantage of fraught emotional situation for social engineering, April 16, 2020.

Another threat actor similarly revealed that they have "been able to avoid sending things back by exaggerating my fear of catching Covid-19 on the basis that I live with elderly family who are at high risk of death...The emotional vector of attack is wide open."



19 [redacted] | 7/14/2020, 10:02:00 PM

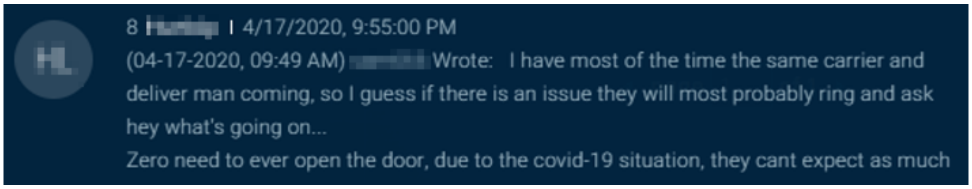
Amazon has been pretty easy going through this for myself. Generally I can convince them under the guise of fear for my 'elderly family'.



Of course. I've contacted Amazon a few times over the course of the quarantine, and a number of times I've been able to avoid sending things back by exaggerating my fear of catching Covid-19 on the basis that I live with elderly family who are at high risk of death if they were infected. The emotional vector of attack is wide open in my opinion due to Covid with many companies, although I can only speak for Amazon personally. Haven't tried anyone else lately.

Figures 30 and 31: Threat actor suggests lying about fear for elderly family members as effective social engineering tactic, July 14, 2020 and July 16, 2020.

Anotherr threat actor suggested that social distancing made it easier to avoid one's deliveryman – and thus to circumvent the due diligence of a delivery man certifying physical handover of a package – making it easier to falsely claim that a delivery had not arrived.



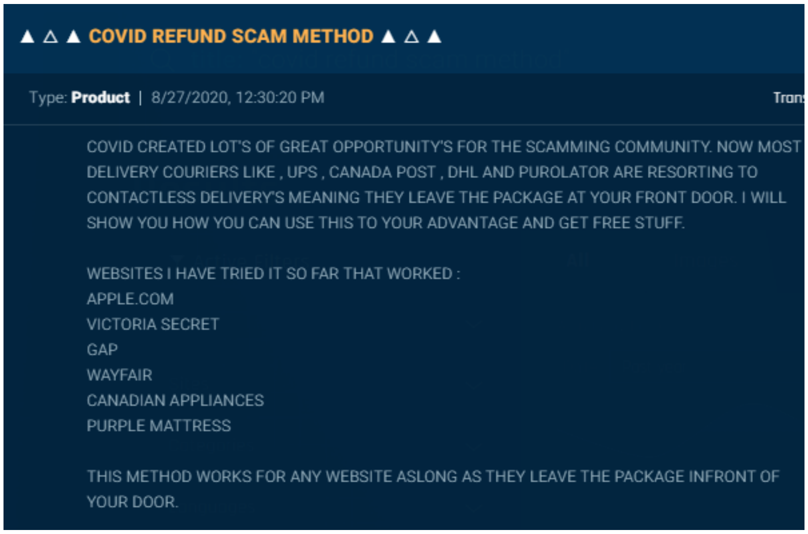
8 [redacted] | 4/17/2020, 9:55:00 PM

(04-17-2020, 09:49 AM) [redacted] Wrote: I have most of the time the same carrier and deliver man coming, so I guess if there is an issue they will most probably ring and ask hey what's going on...

Zero need to ever open the door, due to the covid-19 situation, they cant expect as much

Figure 32: Threat actor says the pandemic legitimates not opening the door to mailman, April 17, 2020.

In August 2020, a scam vendor on a dark web marketplace suggested that refund scammers could exploit delivery couriers such as UPS, Canada Post, DHA and Purolator by resorting to contactless delivery out of hygiene concerns. The method had allegedly worked with shipments from major retailers such as Apple, Victoria's Secret, and Gap.



▲ △ ▲ COVID REFUND SCAM METHOD ▲ △ ▲

Type: **Product** | 8/27/2020, 12:30:20 PM Tran

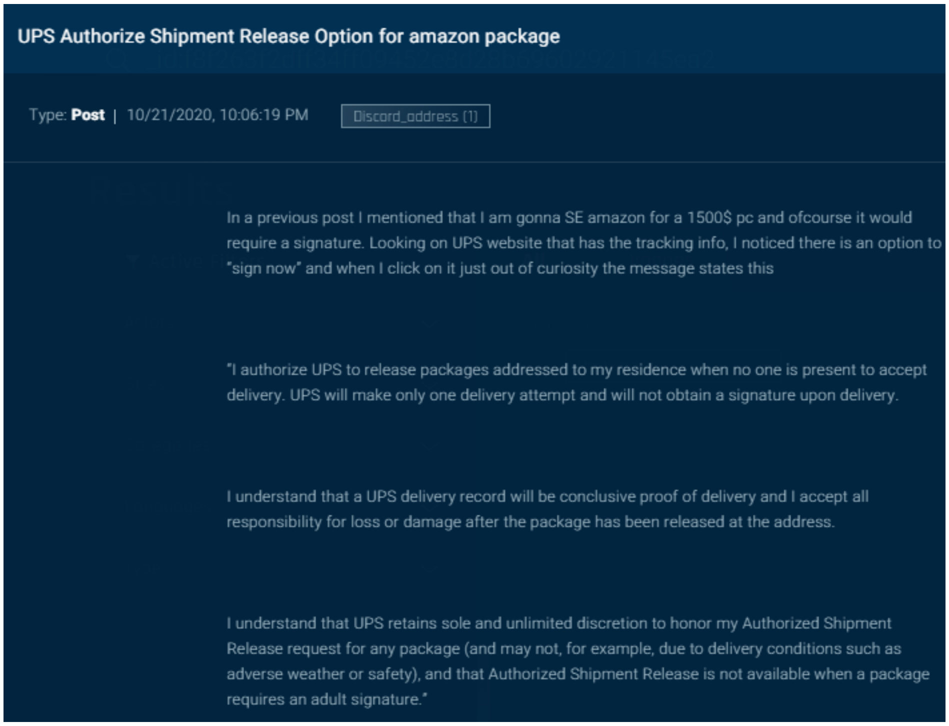
COVID CREATED LOT'S OF GREAT OPPORTUNITY'S FOR THE SCAMMING COMMUNITY. NOW MOST DELIVERY COURIERS LIKE , UPS , CANADA POST , DHL AND PUROLATOR ARE RESORTING TO CONTACTLESS DELIVERY'S MEANING THEY LEAVE THE PACKAGE AT YOUR FRONT DOOR. I WILL SHOW YOU HOW YOU CAN USE THIS TO YOUR ADVANTAGE AND GET FREE STUFF.

WEBSITES I HAVE TRIED IT SO FAR THAT WORKED :
APPLE.COM
VICTORIA SECRET
GAP
WAYFAIR
CANADIAN APPLIANCES
PURPLE MATTRESS

THIS METHOD WORKS FOR ANY WEBSITE ASLONG AS THEY LEAVE THE PACKAGE INFRONT OF YOUR DOOR.

Figure 33: Dark web vendor lists sites vulnerable to refund scams in light of loosened delivery procedures, August 27, 2020.

However, delivery couriers have become more vigilant around the period's unique vulnerabilities. In late October 2020, a threat actor on one closed forum shared that UPS is now requiring either in-person signatures or an online signature authorizing UPS to release packages when no one is present and indicating that "a UPS delivery record will be conclusive proof of delivery."



UPS Authorize Shipment Release Option for amazon package

Type: **Post** | 10/21/2020, 10:06:19 PM Discord_address (1)

In a previous post I mentioned that I am gonna SE amazon for a 1500$ pc and ofcourse it would require a signature. Looking on UPS website that has the tracking info, I noticed there is an option to "sign now" and when I click on it just out of curiosity the message states this

"I authorize UPS to release packages addressed to my residence when no one is present to accept delivery. UPS will make only one delivery attempt and will not obtain a signature upon delivery.

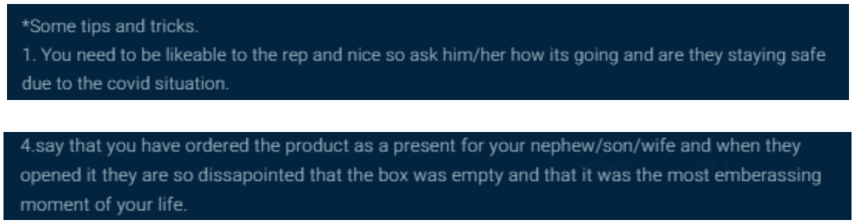
I understand that a UPS delivery record will be conclusive proof of delivery and I accept all responsibility for loss or damage after the package has been released at the address.

I understand that UPS retains sole and unlimited discretion to honor my Authorized Shipment Release request for any package (and may not, for example, due to delivery conditions such as adverse weather or safety), and that Authorized Shipment Release is not available when a package requires an adult signature."

Figure 34: Threat actor notifies of upgraded Amazon and UPS security procedures making DNA refunding method more difficult, October 21, 2020

CONCLUSION

Social engineering is in many ways a theater genre, and it is no accident that so many of the "refunding" manuals circulating on the underground read like scripts. "You need to be likeable to the rep and nice so ask him/her how it's going and are they staying safe due to the covid situation," urges one underground guide for refunding; to pull off the "empty box" method, says the same guide, "say that you have ordered the product as a present for your nephew/son/wife and when they opened it they are so disappointed that the box was empty and that it was the most embarrassing moment of your life." Social engineering is ultimately a matter of exploiting human psychology with good acting.



*Some tips and tricks.
1. You need to be likeable to the rep and nice so ask him/her how its going and are they staying safe due to the covid situation.

4.say that you have ordered the product as a present for your nephew/son/wife and when they opened it they are so dissapointed that the box was empty and that it was the most emberassing moment of your life.

Figures 35 and 36: Anonymously authored refunding manual recommends precise scripts for effective emotional manipulation in social engineering, September 11, 2020.

Chatter on the digital underground about refunding offers an incredible resource for understanding threat actors' best practices as they are played out to a variety of audiences; every attempt is another rehearsal, every forum thread a compendium of director's notes. Threat actors borrow and learn from each other how best to elicit sympathy and manipulate fear with different target audiences and refine their TTPs accordingly. The COVID-19 situation has provided social engineers with increased fear and sympathy as creative fodder.

E-commerce enterprises would be remiss in thinking they can mitigate this fraud by patching only the technical loopholes around the COVID-19 situation, such as tightening their shipping practices. For the best social engineers, these are creative provocations to improvise around. Exploitation of the situation for the best social engineers means, above all, scripting their lies to the pitch of the fears and sympathies of their targets.