

Created By: mothered  
<https://www.socialengineers.net>



**The Risks Of SEing Repeatedly Without Care**

In this day and age, social engineering has taken on a whole new meaning on how attack vectors are executed and the Intentions behind deceiving a given target. For Instance, If you hit a Google search and navigate to (SEing) Internet forums/boards or Discord servers, over 90% of discussions will pertain to **purchasing products online, and then tricking representatives to generate refunds or dispatch replacement Items at their expense**. In social engineering parlance, this is referred to as **"company manipulation and exploitation"**, and very with good reason. The objective is to **manipulate** the company's reps and **exploit** their vulnerabilities - which perfectly describes the above-quoted title.

Each and every company's defence mechanism can be penetrated, regardless of what level they operate on but In order to do that, It's of the utmost Importance to **use a strategic approach and not raise any suspicion whatsoever**. And the way It's done, is by **selecting a "method" that's perfectly suited to the nature of the product In question**, thereby It supports the attack right from the get-go, and helps ensure It heads In the right direction to ultimately have the claim finalized In favor of the SE'er. For example, If you're familiar with [the partial method](#), you'd know to choose something **less than "120 grams"**, for the reason that It will not be detected on the majority of shipping scales.

After contacting the rep/agent telling him of the missing Item, an [Investigation](#) was opened to establish why your order was partially filled. Given **the product was so light and circumvented every weighing facility, there wasn't any evidence to decline the claim**, hence your bank account was credited and you kept the original purchased Item. It's quite exciting when goods are obtained without paying a single dime, and because the company was SED with minimal disruptions, **It's very easy to become fixated on refunding them over and over again** - and that's when problems begin, namely when **"carelessly and repeatedly SEing the same company"**.

And If the **"same carrier" is servicing your deliveries**, Issues may also be experienced with them - **specifically when using the [DNA \(Did Not Arrive\)](#) method**, for the fact that you're blaming the carrier for failing to deliver your packages. As a result of all Incidents, a number of consequences are to be expected - which can affect you on a **personal level**, as well as your **online account**, the standing of your **residential address** and on the rare occasion, **legal proceedings** could also be In effect. Now I'm not suggesting that such events **will** happen, but rather there's every possibility that they **"may happen"** - particularly If you neglect to take precautionary measures with your social engineering behavior.

That's where I come in. What you will learn from this article, is **how to significantly reduce the risks of your SEs raising suspicion when "the same company & carrier are involved"**, thus it will allow you to continue SEing in a safe and secure fashion. What you're about to read may not apply to your current environment, but **can be triggered at any time**, so be sure to absorb every word from this point onwards. In each topic below, I've also listed the **"Impact" that's most likely to occur with the company and carrier due to the SE's actions**, which will provide you with a clear understanding of what the risks relate to. Okay, without further ado, let's rip into it.

## Repeatedly SEing The Same Company:

When you have one or more favorite methods that you're proficient in formulating, and **they've worked against the "same company" ex-amount of times**, there's no doubt you'll predominantly choose those methods over the rest. After all, given they've succeeded with the company in question, it makes perfect sense to keep utilizing each one. However **"using"** them is one thing, and **"overusing"** them is quite another - as it will often lead to **repeatedly hitting the same company (with the same account) many times in a row** and as such, it'll set off alarm bells among reps who're assessing your claim.

For example, let's say you've successfully refunded with the **wrong item received method 4 times in as many weeks** on (who else but) Amazon, by saying that a completely different product was received to the one that was originally purchased. Now I want you to think about it logically for a minute. What are the chances of Amazon (or any company for that matter) **making a separate picking & packing error "4 times in 4 weeks?"**. I'll answer it for you - **"zero"**. Sure, your claim was obviously approved on each occasion, but it doesn't necessarily mean your SEing activities will remain unnoticed - **the company may decide to take some sort of action at a later date**, which brings me to my next point in the subtopic below.

### Impact - Online Account Flagged

When you're on a winning streak from one SE to another, **it's very easy to get carried away and lose track of precisely when each one took place**, and while you may be under the impression that your refunds have been settled in their entirety, behind the scenes of the company's claims department, **"records are kept of every communication and claim"**. Essentially, if the rep/agent has reason to investigate your account, perhaps due to (for

example) Identifying that quite a few wrong items you've returned were not part of their Inventory, **they'll not only check those incidents, but also every other transaction.**

What they generally look for, is unusual spending patterns and basically any irregular activity performed on the account, such as a **high volume of refunds within a particular time frame.** If the events are not too serious and ***do not warrant an immediate closure*** (more on this in the next subtopic), "**your account will be flagged**", meaning it's being actively monitored for **suspicious behavior.** Given every company differs in the way they format and word their messages, I cannot possibly cover the lot, so I'll provide a typical OFM email generated by Amazon as follows:

*"Hello,*

*We noticed that you have requested refunds for a large number of orders. We understand that occasional problems with orders are expected in the normal course of business, however the unusually high number of problems that you have reported with your orders, exceeds this exception.*

*When unusual account activity such as this comes to our attention, we evaluate each account on a case-by-case basis to determine if additional action or account closure is necessary. As a result, **we can no longer compensate you for additional issues** with your shipments. **If this problem continues**, we may no longer allow you to buy on our site.*

*If you believe you may have received this message in error, or if you would like to clarify your order activity, please respond to this email within 30 days".*

That's a standard automated message sent by Amazon's Account Specialist team (just a bunch of office staff with a fanciful name!), to **warn you that you've claimed too many refunds on the account in question.** Notice how I've highlighted some words in green? That's because they actually denote that **the account is still active.** Here's an explanation:

**We can no longer compensate you for additional issues** - "**additional issues**" means the account can still be used in future.

**If this problem continues** - "**continues**" implies further purchases on the same account.

If you've been SEing consistently for quite a while by using the same account for every transaction on a very regular basis, you'd obviously try and refund every purchase made. That's the point of social engineering - to obtain goods absolutely free of charge, but **the more you claim, the greater the chance of attracting attention from customer service representatives**. And If you don't change your approach and keep SEing one product after another by acting Irresponsibly, **your online account may well and truly be closed without notice**. That's right, **you will not be told In advance** of your wrongdoing, but Instead you'd wake up one morning to check your emails and a message to this effect will be sitting In the Inbox.

*"I can confirm that your account has been closed due to unusual returns activity, and It Is also correct that this decision has been made after taking a number of factors Into consideration.*

*Passing over the full details as to what exactly these factors are Is something we're not able to do - we're unable to share this Information as If It were to be made public, It could lead to more unfair use of our service. If you have any other questions at all, please ask.*

*Best wishes, Peter".*

The message above Is pretty vague and other than stating "**unusual returns**", It doesn't specify why It was closed but one thing for sure, **once an account has been "permanently closed" especially by Amazon, that's the end of It - (for the most part) It's gone for good**. You'd then need to go through the arduous task of creating new accounts, by changing every Identifiable detail linked to the old one, **hoping that multi-accounting will not be detected**. It's certainly an Inconvenience, and It could've easily been prevented, If you took the time to Implement a number of measures to minimize the risk of account closure. So how do you do that? **Here's my short list of recommendations that will help ensure the account's longevity.**

- Use a mature account (at least 12 months old)
- Allow a sufficient gap between each SE (to play It safe, 6-7 weeks from one SE to the next)
- Perform legit purchases on the same account (self-explanatory)
- Alter the value of the Items (hit low value Items every now and then)
- Don't use the same method many times In a row (no need to explain this)

- Give the SE a break for a while (stop for a couple/few months and repeat It every so often)
- Don't always refund (throw In replacements to break the same pattern of behavior)
- Log In from the same environment (a VPN may Indicate the account has been compromised, so for security purposes, the company may close It).

### Impact - A Cease & Desist Notice Issued

Even though this Is not very common In the social engineering sector, It's paramount to be well Informed of a **"Cease and Desist"** notice - namely due to **the seriousness of Its nature**. Here's what I mean. When an SE'er goes too far with **obtaining refunds & replacements against the same company**, a **"C&D"** (Cease and Desist) letter Is sent by the company **asking the social engineer to stop his activities**. Basically, It alerts him that his actions are In breach of the company's contract and/or terms, and to **Immediately stop what he's doing**. Think of a **C&D** as a warning notice to terminate requests for refunds.

Now this Is where It begins to get serious. If the SE'er Ignores the Cease and Desist and continues along the same path, such as **keep refunding after the notice was sent, then the company who Issued the notice, can take legal action**. In the worst-case scenario, legal proceedings could already be In progress - which will be stated In the letter. As you can see, the consequences are significant, hence the moment you receive a C&D notice, don't take It as a joke by allowing **"greed"** to take over and Impair your judgment - **put an end to your social engineering straight away!**

### The Same Carrier Repeatedly Servicing Your Goods:

As you are aware, when looking to refund a company many times In succession, **It's crucial to apply a number of precautionary measures from one SE to the next**, thereby It will help prevent raise suspicion and allow each SE to flow with minimal complications. And of equal Importance, Is **"taking note of the carrier who's servicing your deliveries"**. A lot of SE'ers tend to purely focus on the online store, and many fail to recognize that serious ramifications may also be experienced when **"the same carrier company delivers packages to the same destination"**.

As a result, It can Impact on both **"yourself"** and the **"carrier driver"** on personal level, thus you'd certainly want to avoid It at all costs. I've discussed these In the last two subtopics prior to concluding this guide. Additionally, **"your residential address can also be affected"**, therefore It's Imperative to Identify the causes before they have the opportunity to begin, so let's first check out what can happen when **your residential address Is flagged and blacklisted**.

### **Impact - Residential Address Flagged/Blacklisted**

The fact Is, SEing In the capacity described In this article, Isn't exactly based on legit grounds and as such, **many SE'ers prefer to anonymize where their packages will be delivered - a commonality being a drop house**, which Is a vacant home that has no association to the social engineer whatsoever. However, **It can be difficult locating a separate drop for every delivery** - particularly when frequently ordering products from various retailers, hence the best option Is to simply **use your own residential address**. If you give the Impression that the SE Is a legitimate claim by manipulating It accordingly, there's nothing to worry about, but the same cannot be said **"when the same carrier Is regularly attending your home"** - namely when using the **DNA method**.

How so, you ask? Well, It's similar to refunding the same company many times In a row - **records are stored and accounts are put under the microscope** leading to account closures, but the difference with carriers, Is that once your residential address has been flagged and blacklisted by the carrier Itself, **"It (may) apply to every company who uses the same carrier to deliver goods"**. For *example*, If **"DHL"** has blacklisted your address (due to claiming that you did not receive an array of packages) and It's partnered with Amazon, John Lewis and Zalando, then **deliveries from those companies via "DHL" to your address may be refused**. Understood? Good! So be sure to SE wisely with the **DNA method** - **don't overdo It with the same carrier**.

### **Impact - The Carrier Driver Contacting You**

Prior to making a start, do note that this only relates to the **DNA method** when saying the package (that the driver did In fact deliver), was not received by you, nor any member of your household. **Because carrier drivers are well aware that they've done their job properly, by dropping off their deliveries at the correct address, they tend to take offense when people**



**state otherwise.** And If your behavior Is repeated with the **DNA**, many drivers take matters Into their own hands and **visit the SE'ers home**, or get **In touch by phone**. Be It one or the other, the driver will ask questions about the delivery, and why you've said It wasn't received. Sometimes he'll even **ask to sign a document** - just to clear himself of any wrongdoing.

Given you haven't purposely targeted him and It's his choice to take It personally, **you need to protect yourself from his demanding attitude, and not allow him to emotionally affect you.** There are occasions when he'll do whatever It takes to get In contact with you, and If It means generating 20+ phone calls or continually visiting your house until someone answers the door, he'll do exactly that on a daily basis. Some SE'ers feel as though they must explain themselves, by speaking with the driver and complying with his requests, which Is NOT the case at all. **He's a "delivery driver", not a police officer, thus he has no right to set foot on your private property Interrogating you** (so to speak), so don't bother opening the door or answering your phone.

### **Impact - The Carrier Driver Losing His Job**

From a social engineering standpoint of refunding companies who make millions/billions of dollars In profit each year, there's no harm done financially, but It's a different story altogether If **"your SEing contributes to the carrier driver losing his job"**. No one should be fired at the expense of your SEs - they too have bills to pay and mouths to feed, so **It's vital to social engineer In a fashion that will not Impact on the driver's occupation.** In order to do that, you need to ensure that your SEing affairs remain within the confines of your very own environment, and do not play any role with the carrier driver and his deliveries.

Although you cannot control what the company does with your claim, the one thing that can be done on your end, Is to **significantly decrease the risk of the driver potentially finding himself on the unemployment list** as follows. If you SE regularly and consistently and It's the **same driver** dropping off your packages, **do NOT use the DNA method each and every time.** Too many claims for nonreceipt of goods when **the same carrier driver Is Involved**, may result In some sort of reprimand/punishment from his boss - possibly Issuing an official warning or **fired for failing to fulfil his role as a delivery driver.** The message Is loud and clear - **be a responsible SE'er**, by respecting the driver for **"who he Is"**, as opposed to **what he does** for a living.



## In Conclusion:

The objective of this article is to give you a very good insight of how and why **repeated SEing** in a careless manner, is likely to have an impact on you **personally**, inclusive of **affecting the standing of your online account**, as well as the possibility of your **residential address being blacklisted**. Moreover, and as you've just read above, you've learned that **your actions may also compromise the carrier driver's job** - which you're now aware of how to prevent that from happening with future SEs. All in all, you've attained the skill set and knowledge to social engineer in a way that will help secure a positive outcome with every SE performed.

You may reference my work, only if you credit its source namely

<https://www.socialengineers.net>

Downloaded From:

<https://www.seing.org>

