CHECK POINT

EXPOSURE MANAGEMENT

# How Threat Actors Are Weaponizing Public Complaints Against Airlines and Other Brands

# TABLE OF CONTENTS

# INTRODUCTION

A delayed flight. A card declined abroad. A refund that never arrived. Almost every one of those complaints ends up in the same place: a public post on social media, tagged to a brand, written by someone who is already frustrated and wants an answer today.

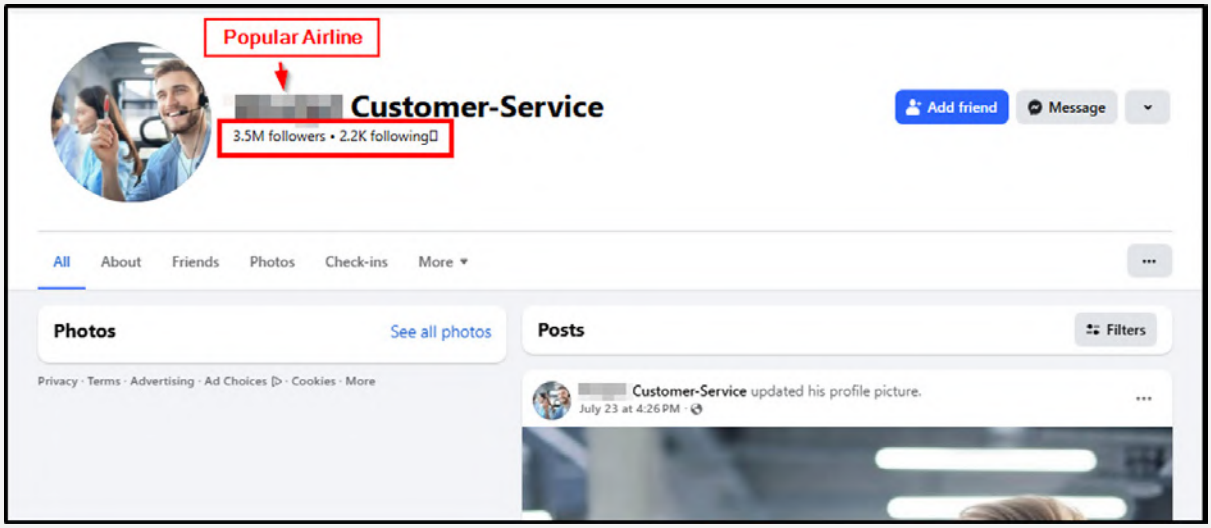
That queue is public. Anyone can read it. Anyone can answer it.

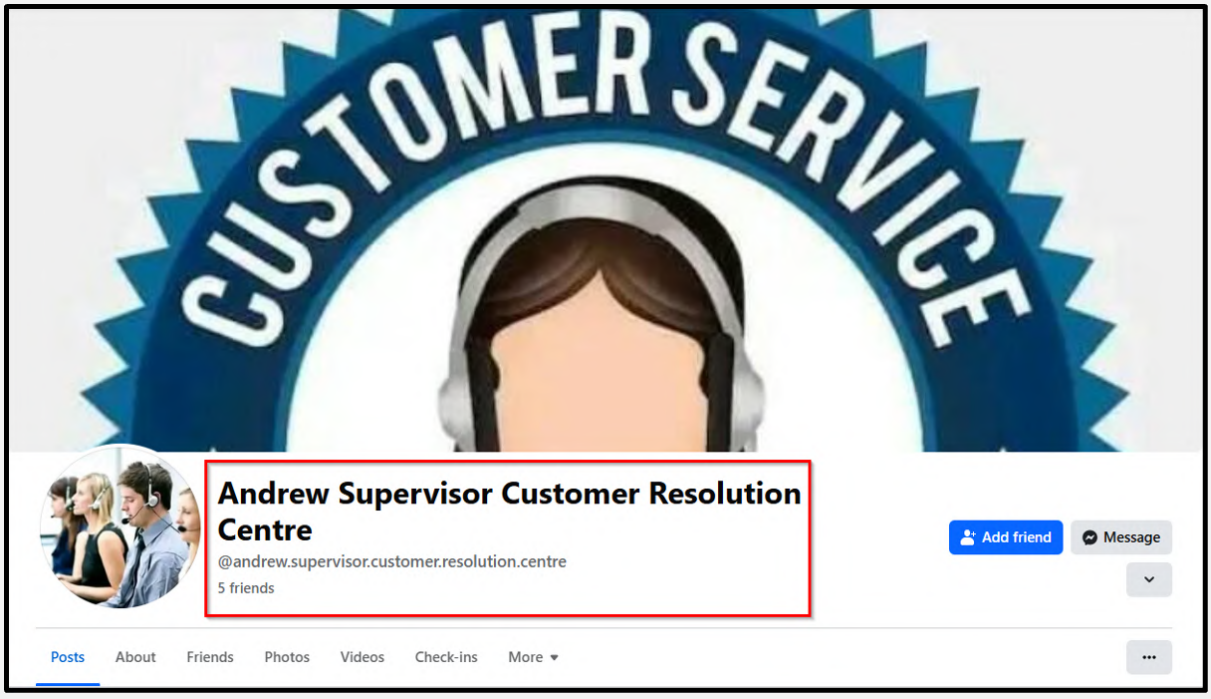
A coordinated group of scammers has built a business on answering it first. They breach nothing. They impersonate the brand outright, sitting in the replies beneath its own posts, borrowing its tone, and stepping into the gap left by every complaint the real support team never reached. By the time a victim realizes what is happening, they have handed these impersonators their identity details and their card, believing they are claiming money they are owed. Individual losses run into the thousands.

We engaged with the scammers directly, followed a single public reply through to the payment page, and mapped the sequence end to end. What follows is how the scam works, who is behind it, and what brands and their customers can do about it.

## Type of impersonating accounts on social media

The threat actor (TA) impersonation accounts **do not always include the brand name or logo** in their profile (see Figures 3 and 4 for examples). During the preliminary investigation phase, it was observed that accounts created on X (Twitter) **more frequently contained the brand logo** compared to those on Facebook. However, both X and Facebook accounts use the same techniques and language as the official brand account to lure victims into their scam.




Sometimes impersonating accounts on X appear more sophisticated and targeted, using official brand profile photos, cover images, and descriptions in both English and French.

We observed in thousands of cases that TA's maintain and are creating X, Facebook, Instagram accounts, persistently impersonating **airlines, their vacations brands, Customer Support, and Representatives,** often with variations of these terms in the usernames and handles.

### Support-function naming [Airline] then:

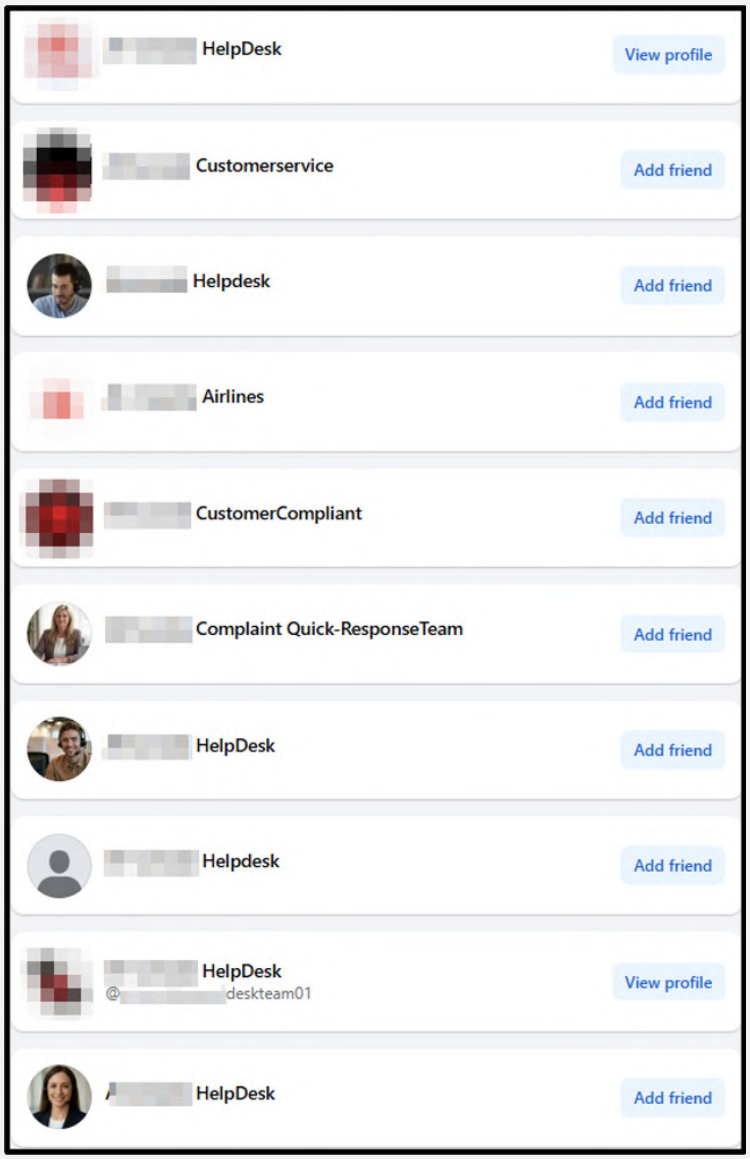
- Customer Support, Customer Service
- Help Desk, Support Desk, Service Desk, Care Desk, Help Service

### Claims and compensation naming

- Claims Department, Direct Claim
- Claim Review, Claim Assist, Claim Response, Claim Report
- Review Unit

### Live-contact naming

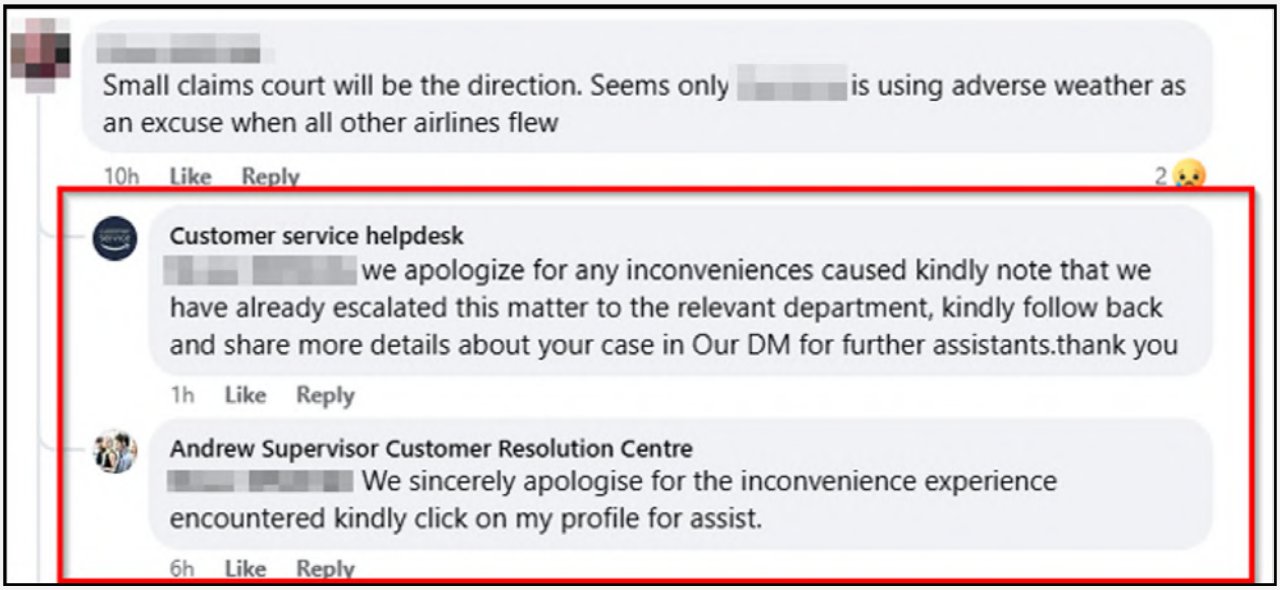
- Chat Hub
- Live Assistance

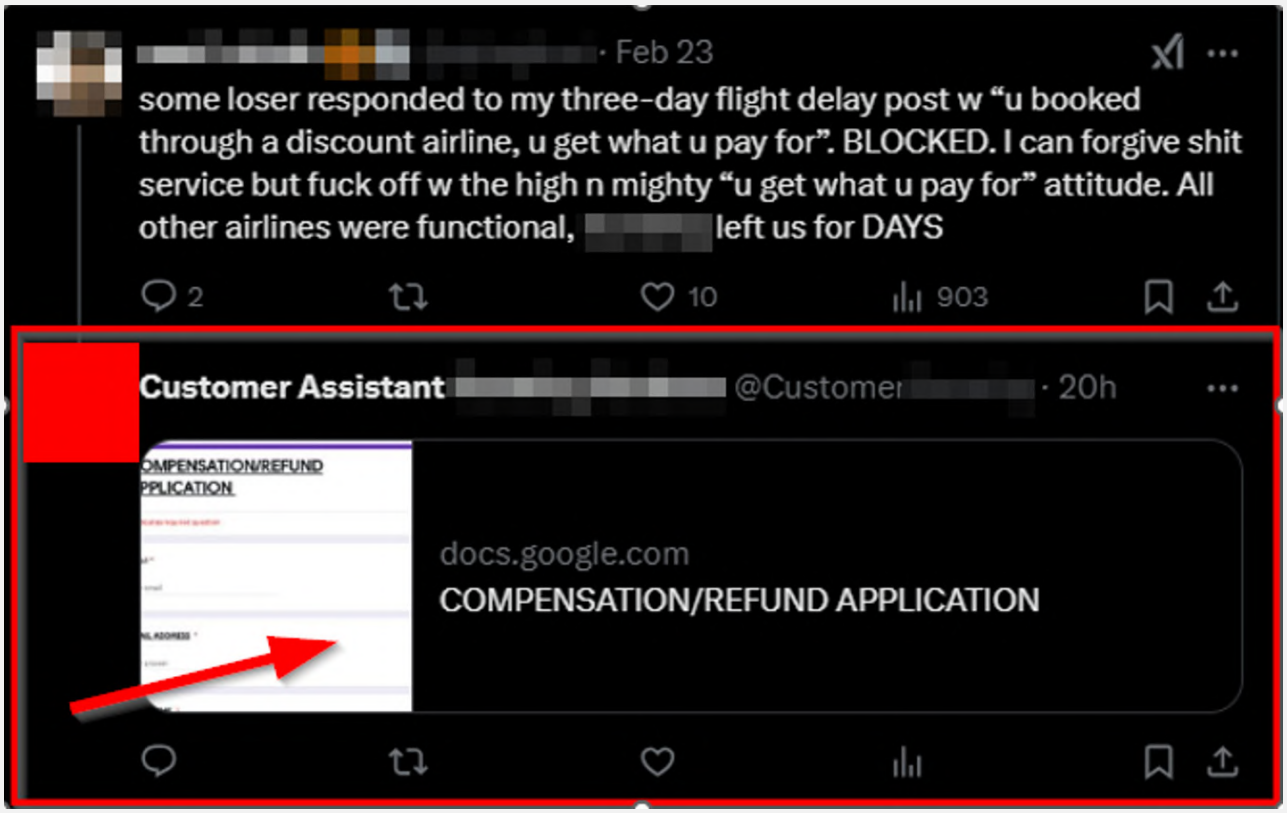


## Impersonating accounts engagement with users

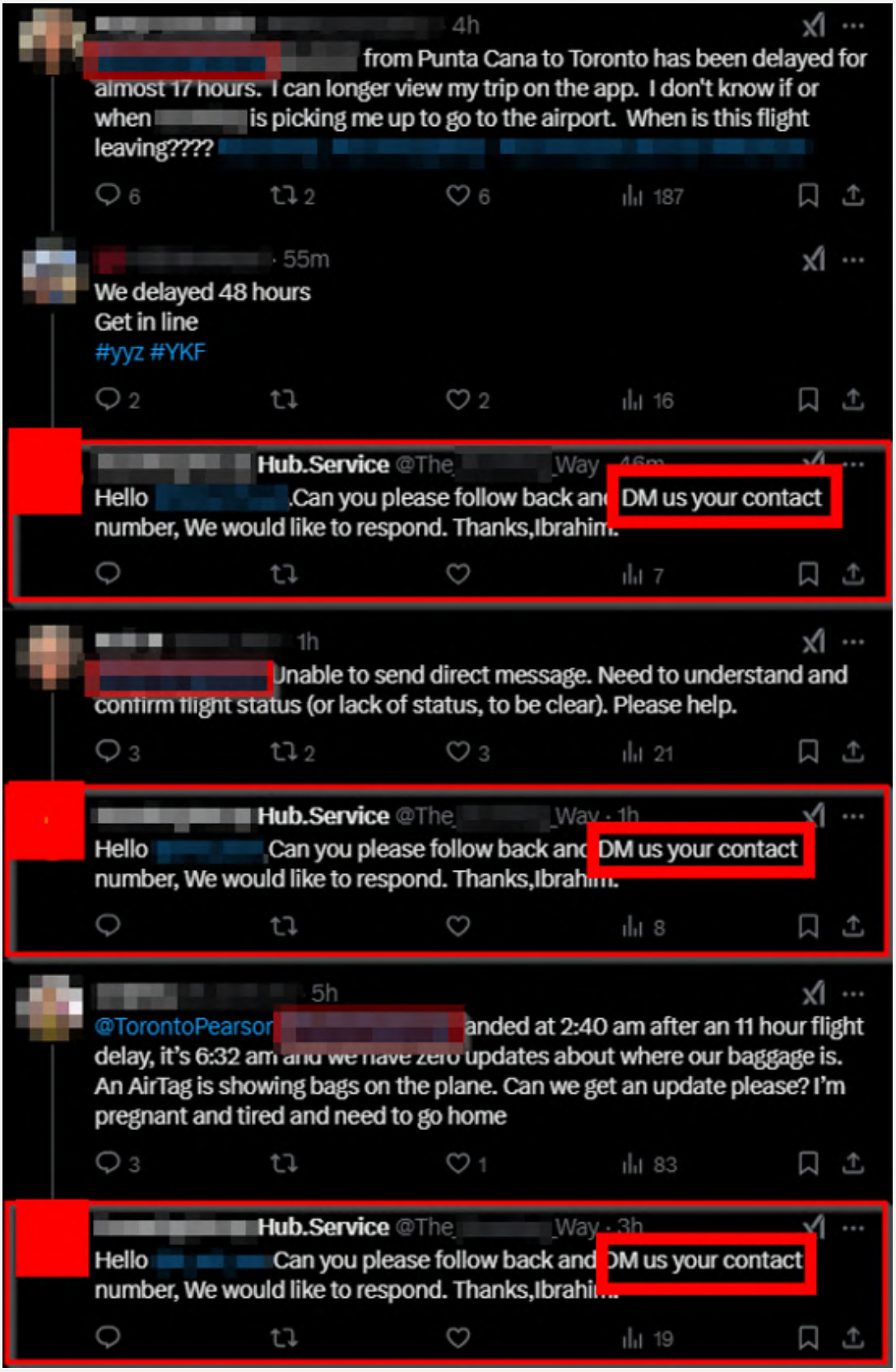
Initial findings during the investigation, before making HUMINT contact with the threat actors, showed that they **actively comment and reply to disgruntled, agitated, and complaining customers** on the airline's verified posts. They often begin by apologizing for the inconvenience and then kindly ask the customers to share more details and direct message (DM) them.

This practice is identical to the methods used by official brand accounts, which is likely why the threat actors are using brand channels to lure their victims.



In the image below, we can see a threat actor account impersonating an airline on X. The account is responding to multiple individuals who are **tagging the official brand** account with their concerns. The threat actor then hijacks, replies, and asks the users to follow the account back and direct message (DM) their contact phone number.



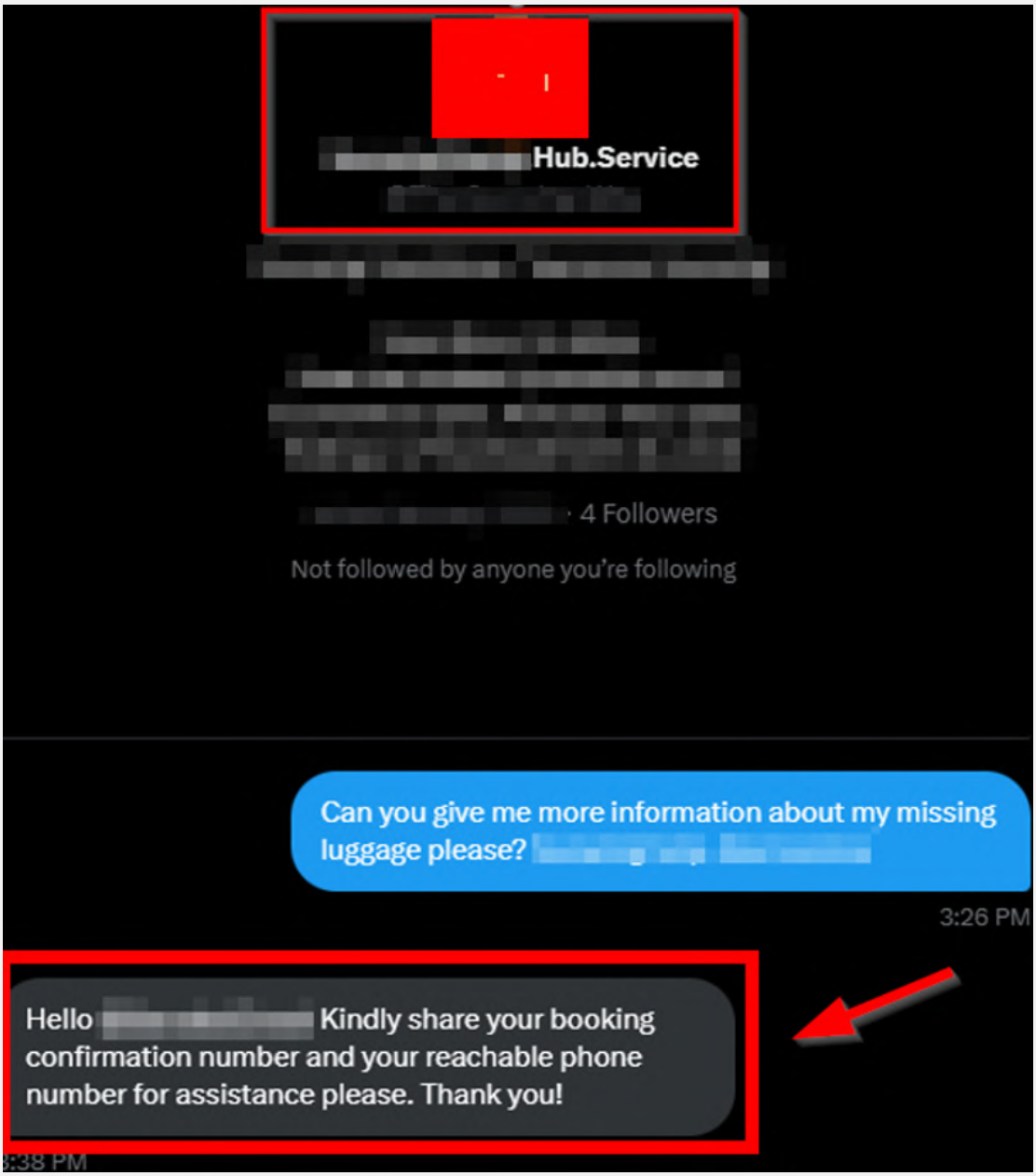
# HUMINT INVESTIGATION

## Engagement with threat actor social media accounts

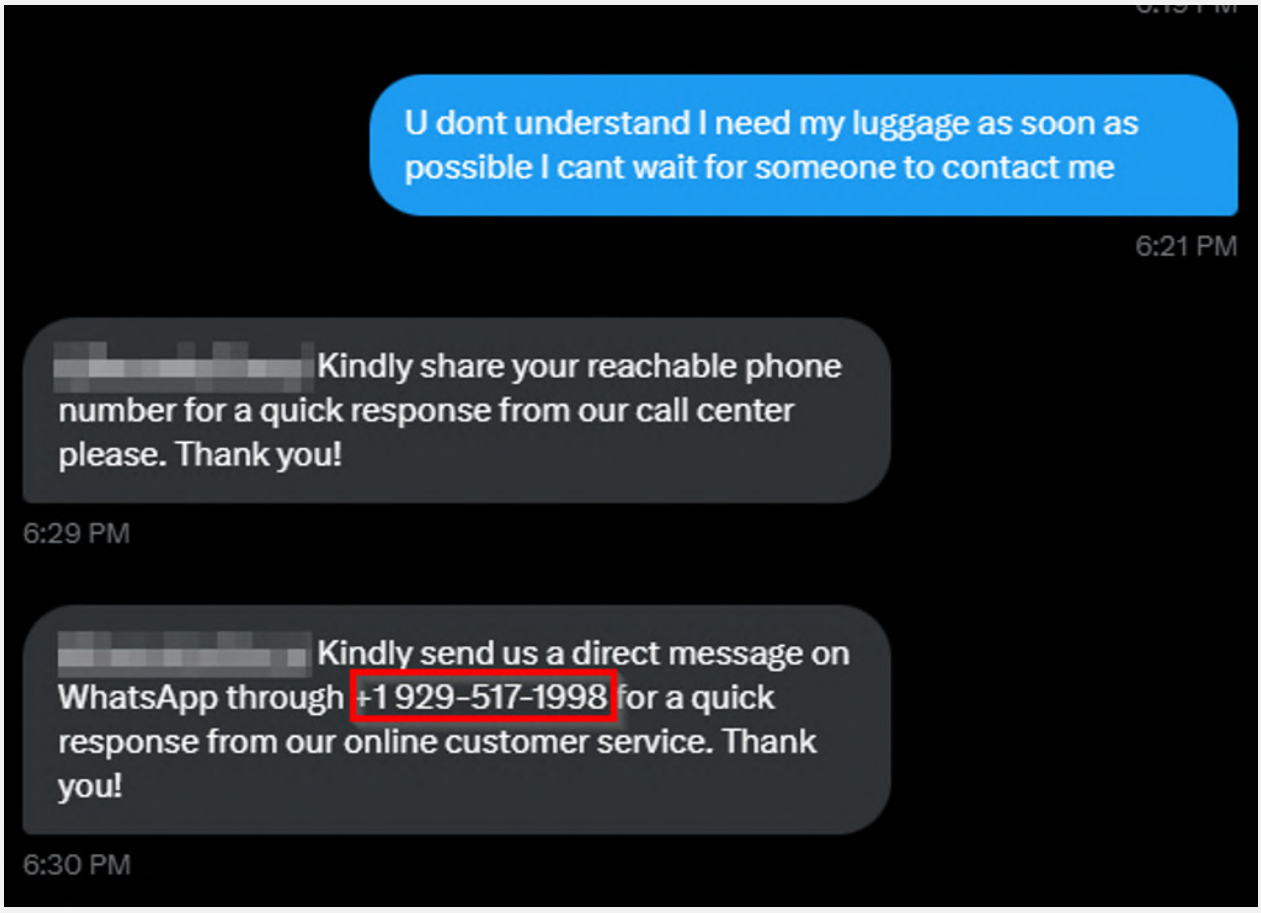
While conducting the **HUMINT investigation**, we attempted to engage with the impersonating accounts. Some accounts were inactive and did not respond, while others replied instantly.

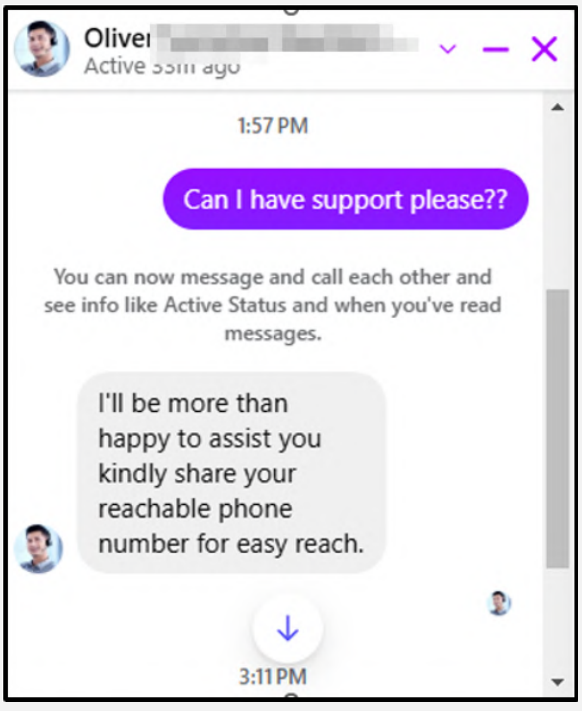
The impersonating accounts often responded with a message asking us to "kindly" share a reachable phone number along with our concern and booking number. We made several attempts to obtain their phone number or email first, but they seemed reluctant to provide it. The threat actors were persistent in requesting that we send our numbers, assuring us they would contact us at the appropriate time.

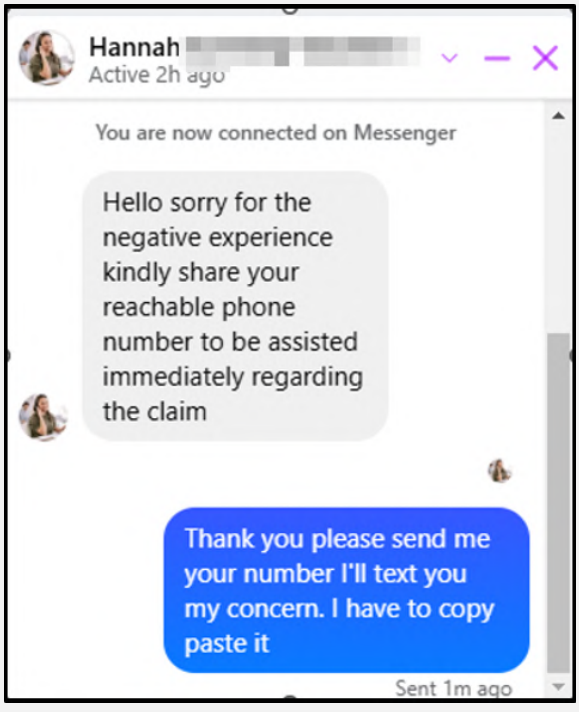
**We believe this is done to create the illusion of interacting with a legitimate customer support representative while also giving them time to prepare a scam tailored to the victim.**



After a few attempts, we were able to get a threat actor to provide their phone number, which allowed us to investigate before making any contact with them. This was the only instance where the threat actor provided us with their phone number.



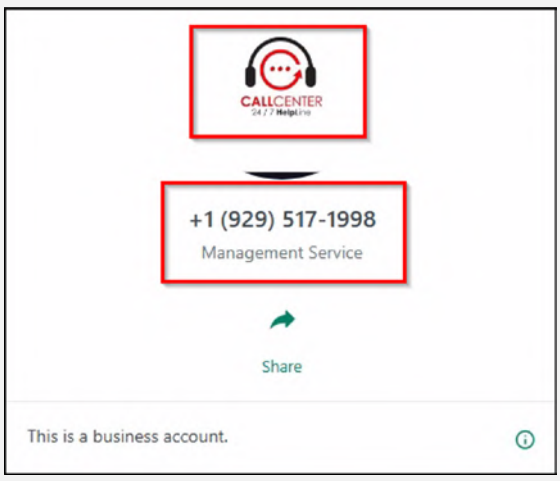



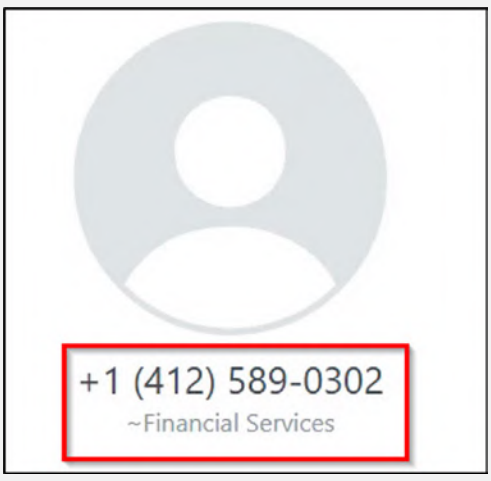
## Threat actor phone numbers

We engaged with **three separate phone numbers** from accounts claiming to be from airline support, all of which communicated with us via **WhatsApp.** The threat actors use WhatsApp because it is a widely popular service that only requires an internet connection after the account is activated with a phone number. All of the numbers were **Business Accounts.**

We believe this scam campaign is originating from **Kenya.** Additionally, we tested and confirmed that virtually bought phone numbers and accounts can be purchased online for a small fee and used to activate WhatsApp accounts in different regions worldwide. The individual activating the account can be located in an entirely different region from the phone number they are using.

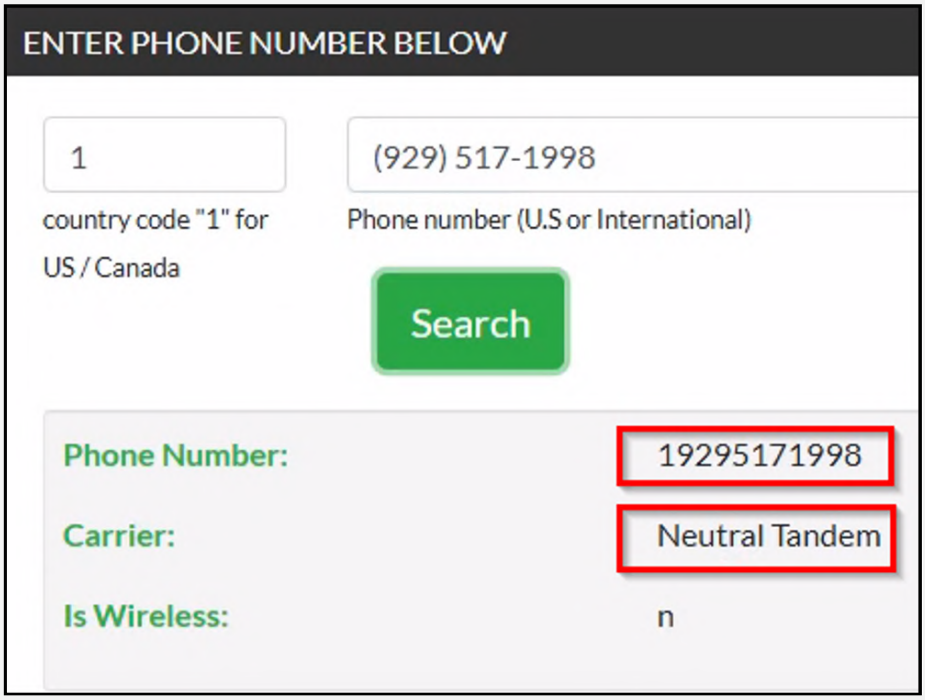
In Figures 12 and 13, we can see two separate phone numbers based in New York (929) and Pennsylvania (412), United States.



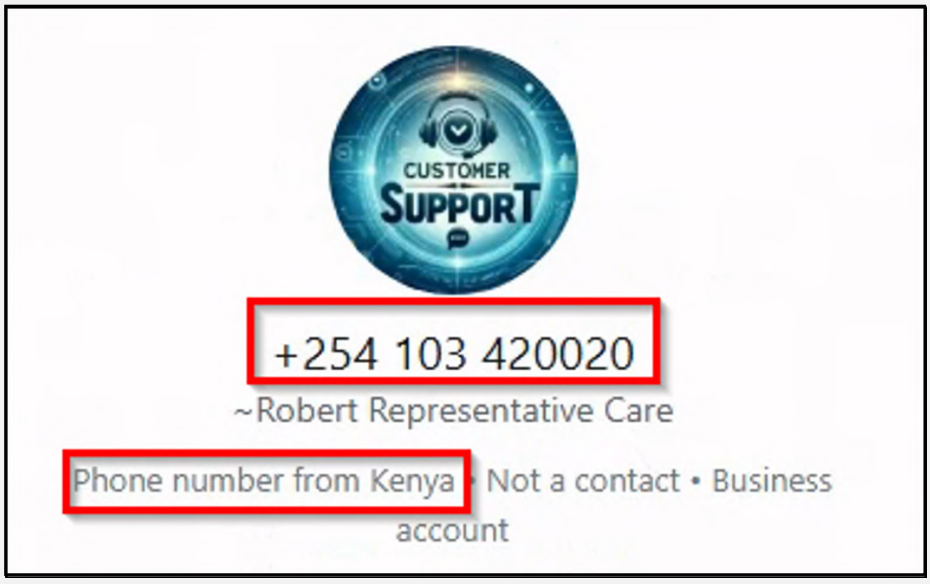



Upon checking the numbers, we verified that they are not original or legitimate. This indicates that they are either voice over internet protocol (VOIP) numbers or WhatsApp accounts activated using burner numbers, allowing communication solely through an internet connection.

It was also discovered that Neutral Tandem was the carrier for one of the phone numbers, suggesting that the number is being routed through Neutral Tandem's switching infrastructure for call handling, rather than being directly connected to a specific carrier's network.




The third number named Robert Representative Care appeared to be originating from **Kenya.**

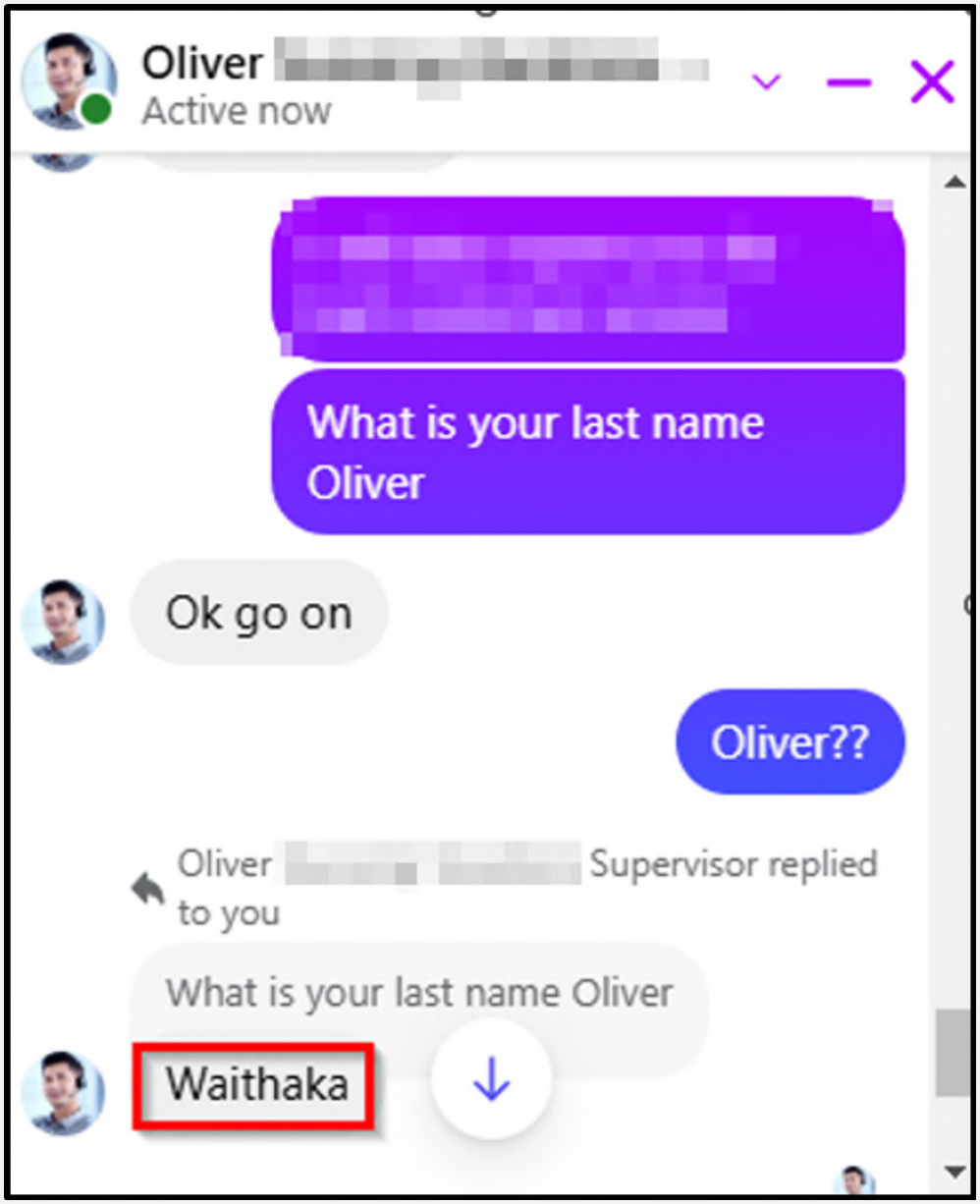


## Further engagement and location verification

In addition to sending us messages via WhatsApp, the threat actors proceeded to call us. After accepting the calls, there was a 5-second silent pause, followed by 3-9 seconds of silence, indicating some sort of connection transfer on their end. This could further suggest that they are using **voice over internet protocol (VOIP)** to secure their connection.

As the engagement continued, they appeared to speak broken English with thick accents. They appeared very aggressive and seemed to follow a highly directed and scripted process that they had practiced or used before.

Additionally, we managed to get one of the threat actors to provide their last name, which turned out to be a Kenyan word.




The name **Waithaka** is generally a Kenyan surname that means "of the land." Additionally, it is also an area within Nairobi, Kenya.

# Exposing the scams

While conducting our **HUMINT investigation**, we discovered **three** different scams being used by the threat actors to steal money from victims seeking compensation for their complaints.

All the scams are designed to gather as much personal information from the victim as possible, with the ultimate goal of tricking them into **sending money to the threat actor through different international money transfer platforms,** while believing they are receiving compensation.

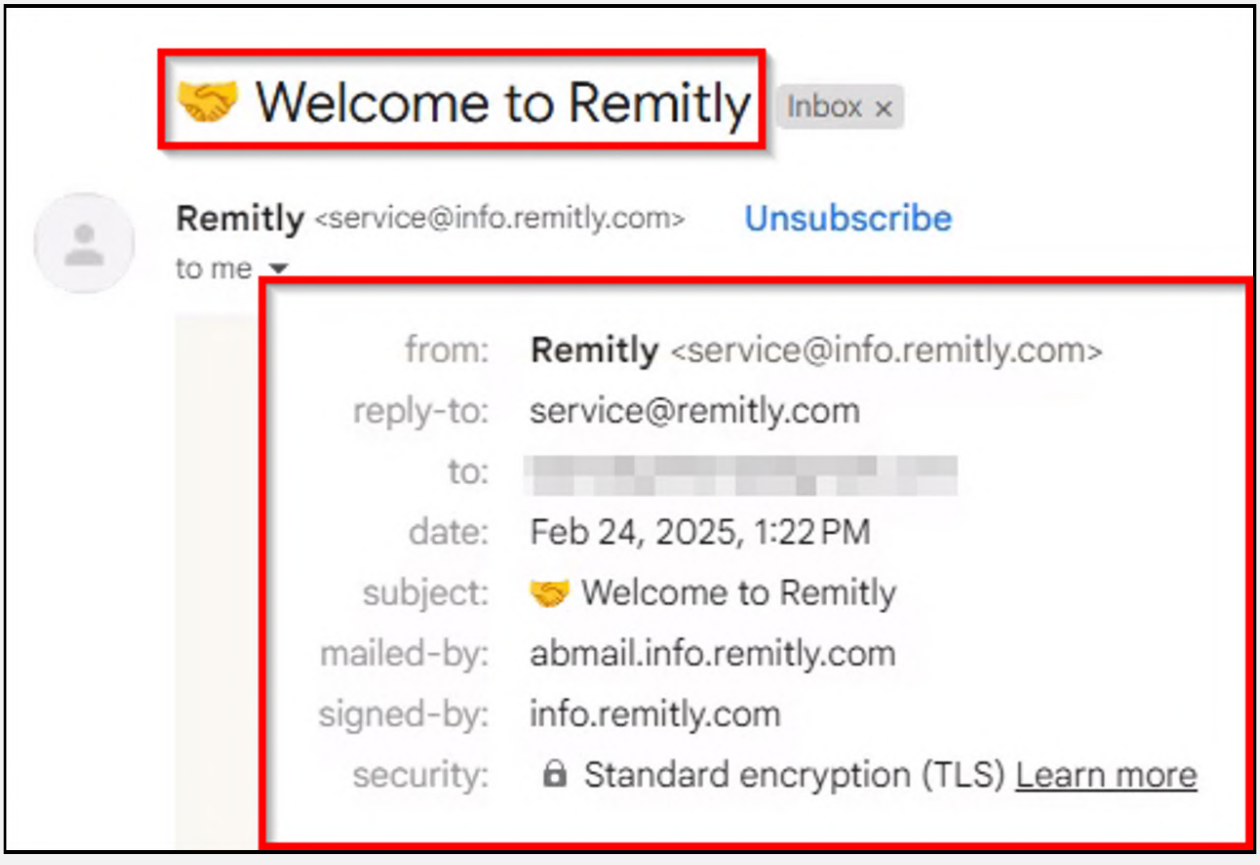
## Scam 1 – remitly.com

When engaging with phone number **+1 (929) 517-1998**, the threat actor asked via WhatsApp for our **full name, email, booking details, and our complaint,** including the **total cost of our flight, vacation, or hotel.**

After providing the information requested by the threat actor, we waited for a return phone call. We suspect that they used this information to tailor and set up the next stage of the scam.

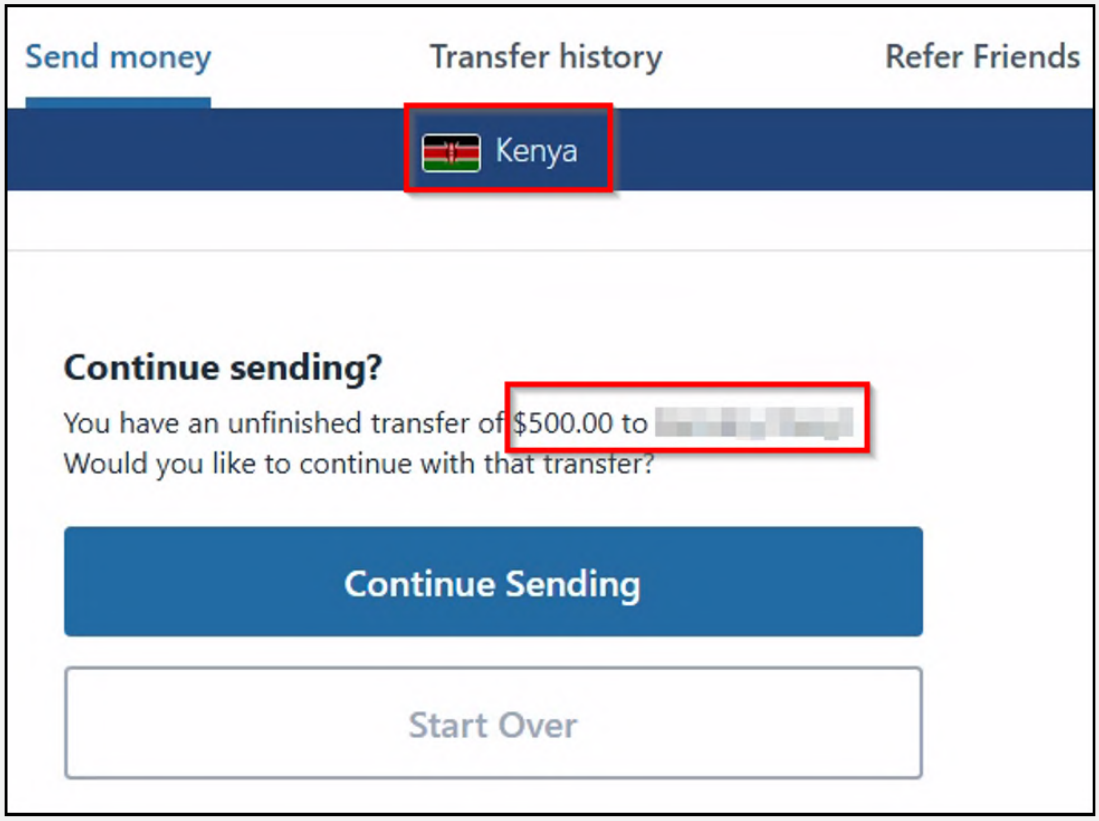
They explicitly stated that they were "verifying our claim" and ultimately determined that we had been granted compensation. The threat actor instructed us to check our email on our phone and **download the application** they had sent. They repeated multiple times to only open the application on our mobile phone. **The links could have contained malware or grabbers.**

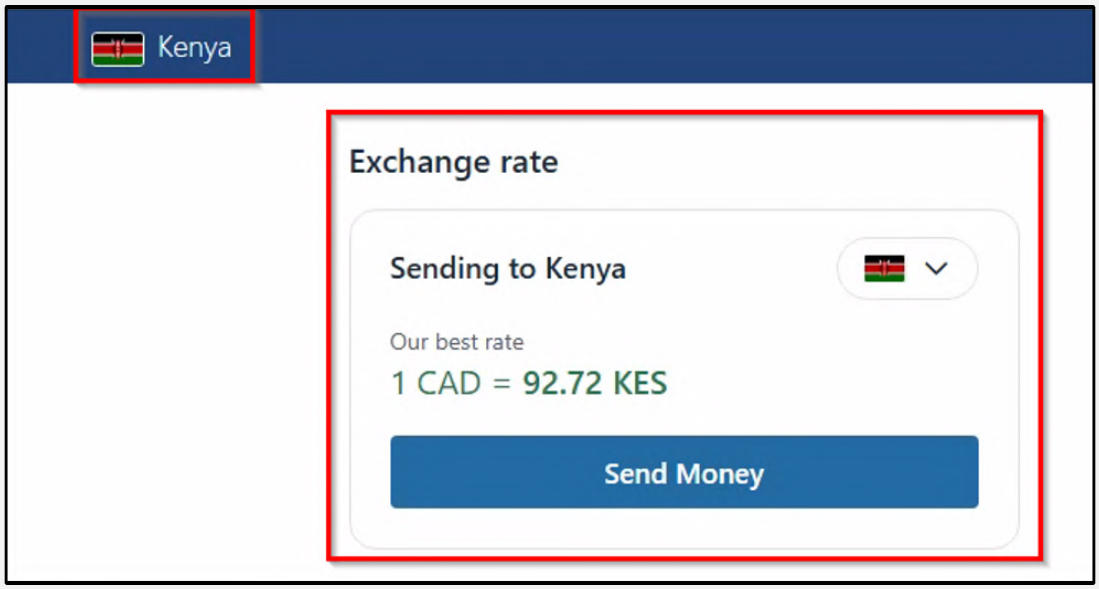
We received an email welcoming us to **Remitly,** which is a digital money transfer service that allows individuals to send money **internationally** quickly and securely.



At this stage, we logged into **Remitly (remitly.com)** using the email we provided to gather as much information as possible and determine what the threat actor was trying to achieve. We discovered that as soon as we logged into our account, there was an unfinished transfer of $500 **to the name** we had provided them.

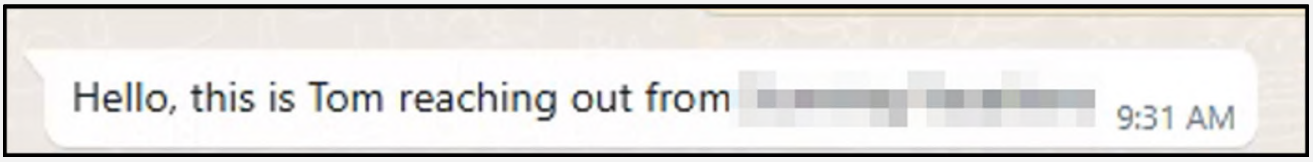
This indicates that the threat actor created an alternative account using our name, registered our email with Remitly, and then **initiated a payment to Kenya,** hoping the victim would believe they were receiving their compensation. As we continued the process, we were asked to enter **credit card information** and more details to complete and finalize the payment.



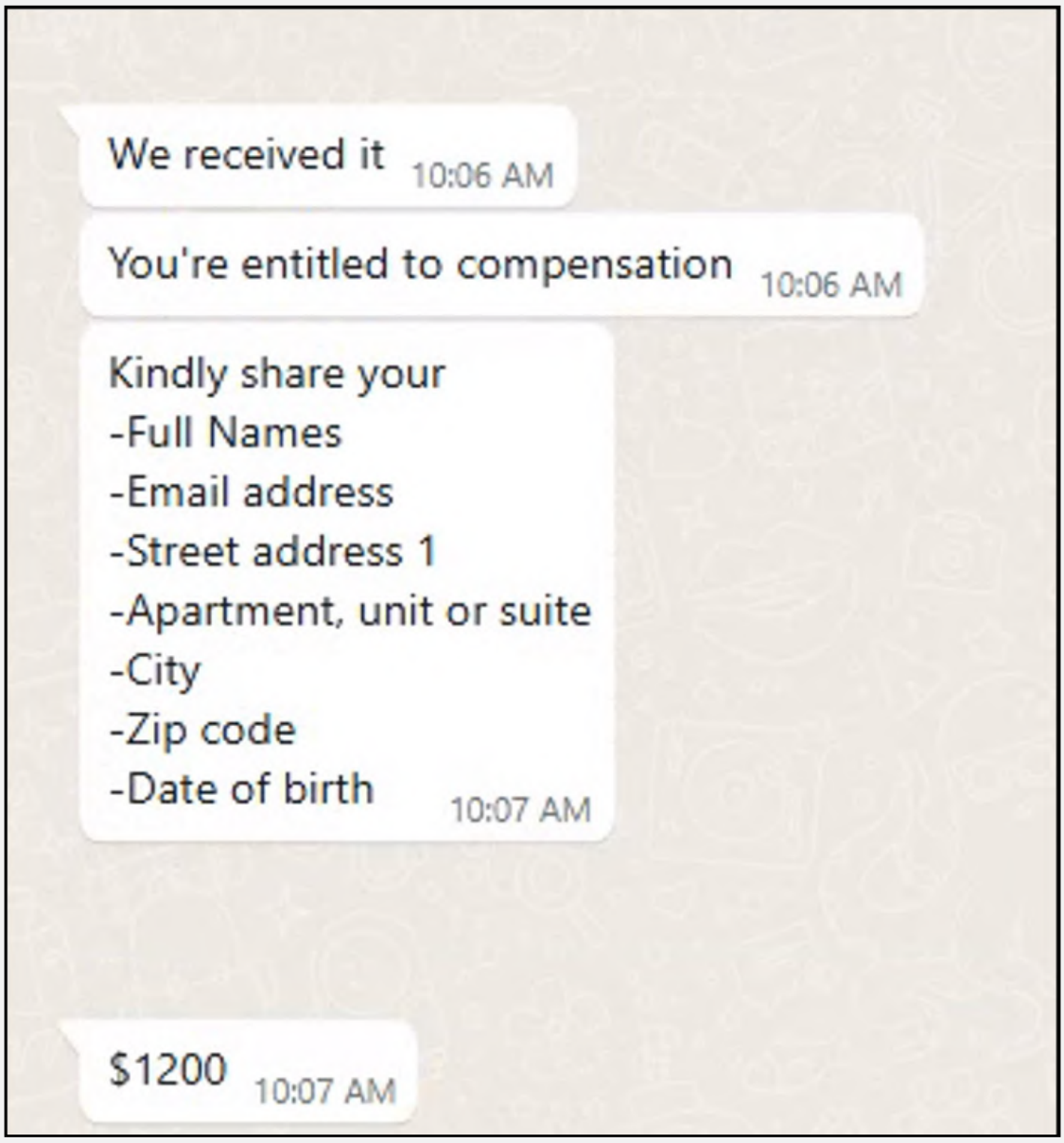



## Scam 2 – lemfi.com

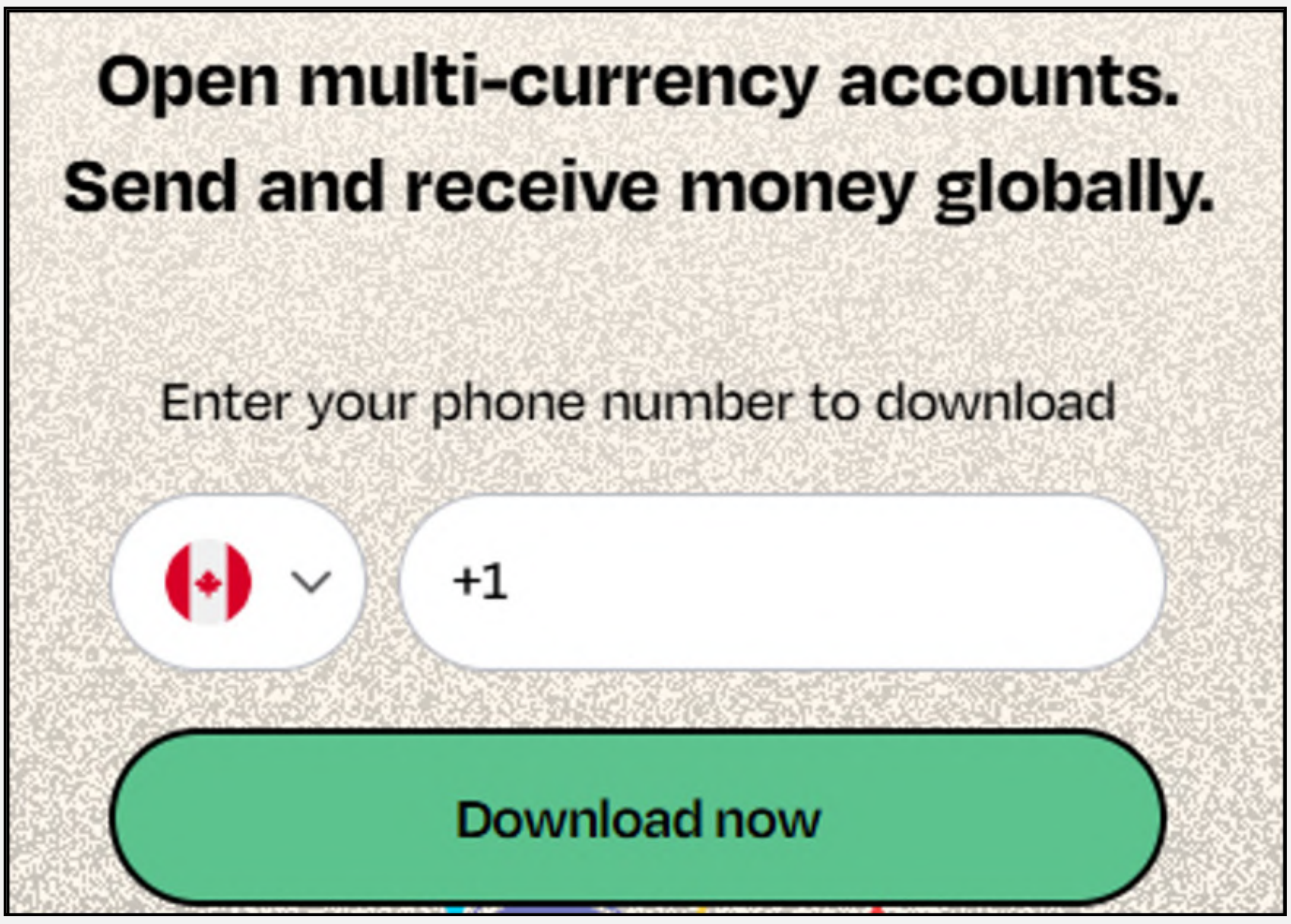
After we gave the impersonating **airline** account our number, they initiated a conversation with us on WhatsApp specifying that they were **Tom from the airline** from the phone number **+1 (412) 589-0302.**




Like the first scam, the TA requests to send them as much personal information as possible. The TA requested our **full name, email, address, DOB and confirmed we were entitled to $1200 worth of compensation** after sending our complaint.



Continuing the process with the threat actor, they later claimed to be sending an **SMS** to our number from **Lemfi (lemfi.com)** in order to verify our identity. However, this was not for identity verification but rather to sign us up and prompt us to download the Lemfi mobile application, which is another international payment app designed to simplify cross-border money transfers.


This likely follows the same process as the first scam to social engineer the victim into sending money to the threat actor in **Kenya** while believing that they are receiving compensation for their claim.

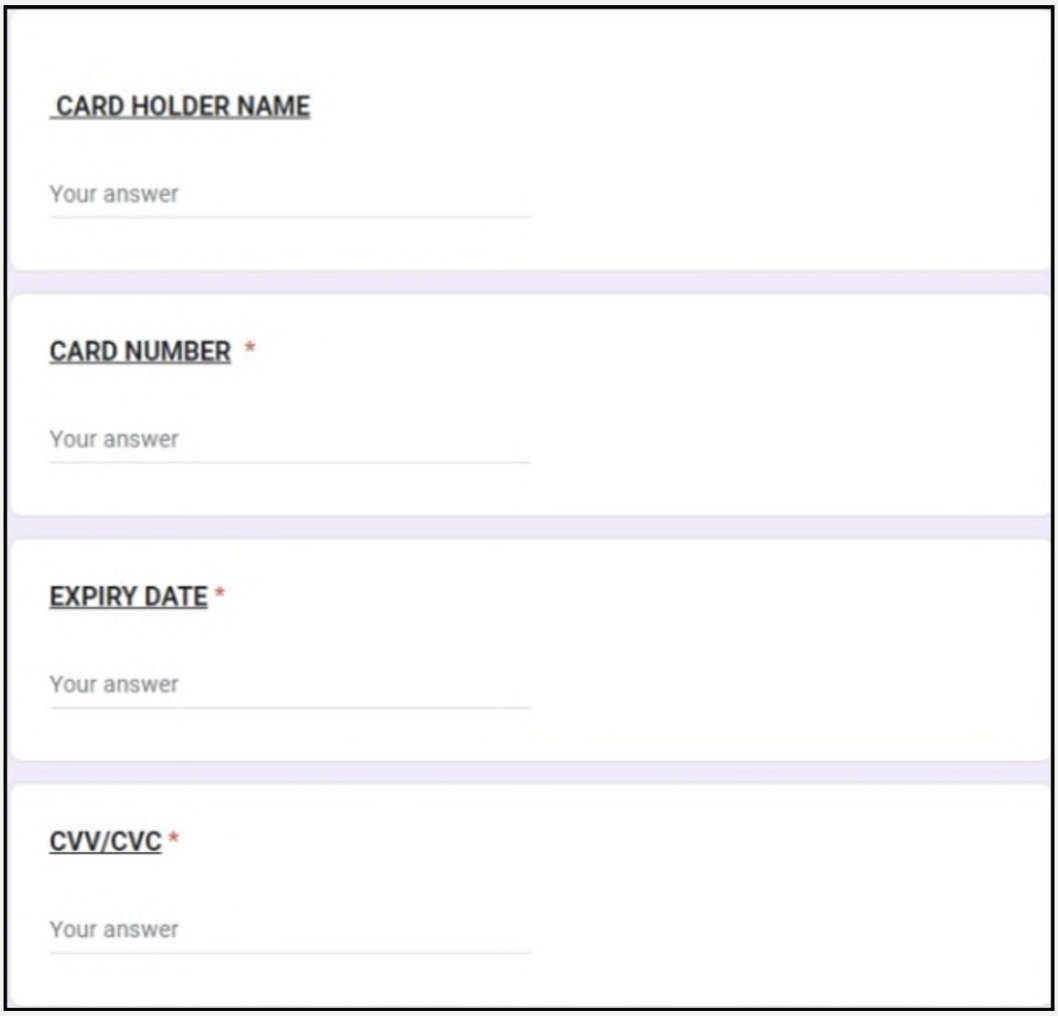
## Scam 3 – worldremit.com

After messaging several other impersonating airline social media accounts, we received a WhatsApp message from a **Kenyan** phone number, **+254 103-420020.**

The threat actor continued in the same manner as the two previous scams, asking us to provide as much information as possible, including our names, email, and complaint. They then sent a link to a **Google Form,** which is the same one shown in Figure 7. The form has since been taken down, but similar ones are still available.

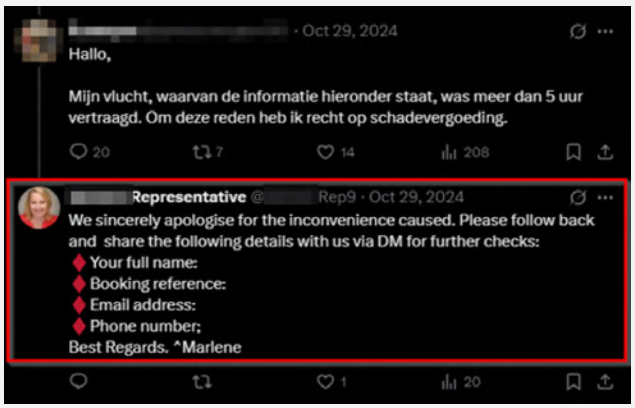
- **https://docs[.]google[.]com/forms/d/e/1FAIpQLScdyoi2KuEjIOtAdLHKNA1NyEL9IXcqYm69btSXfK2k7BN17g/viewform**

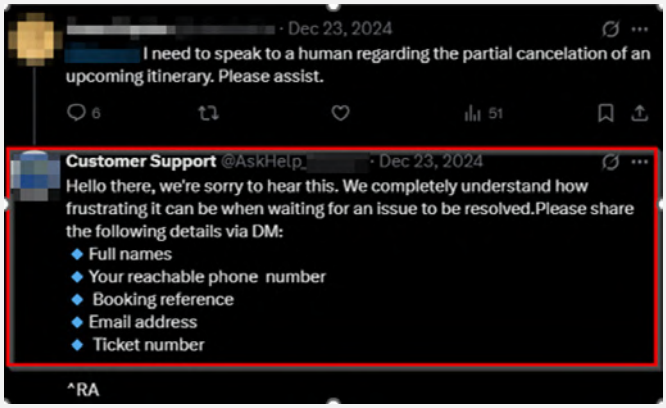

The forms are named **"COMPENSATION/REFUND APPLICATION"** and ask the individual to enter their personal details to apply for a refund and compensation.

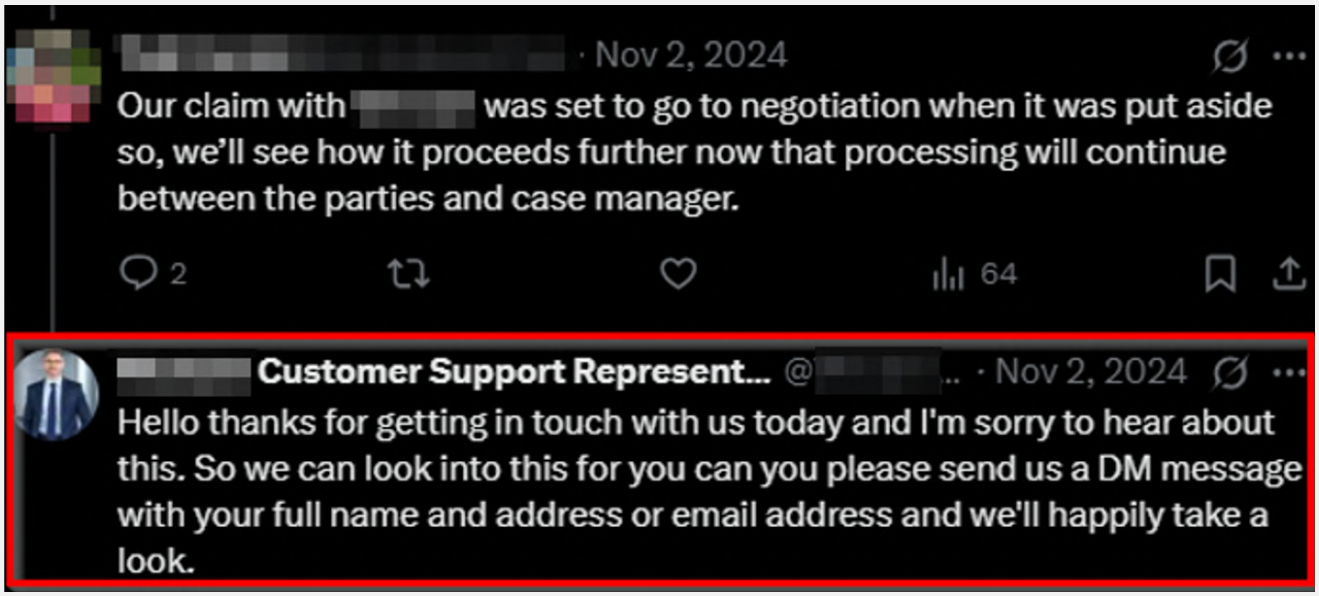


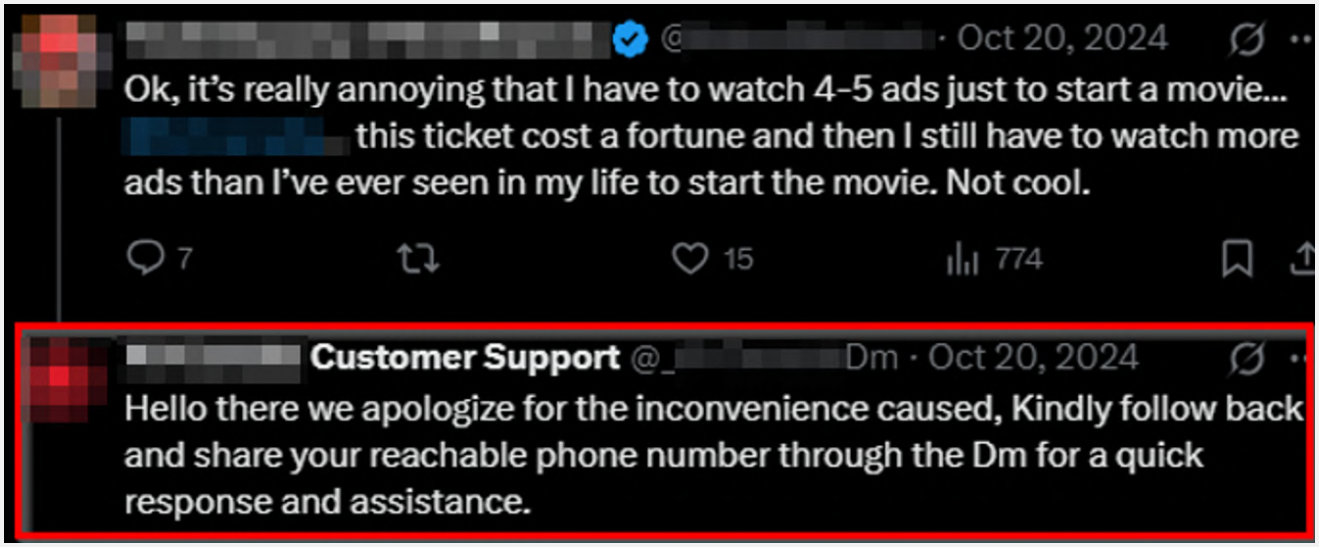
# IS THIS UNIQUE TO ONE AIRLINE?

When searching for similar accounts of the same nature for most North American airlines, we found several that they share the same characteristics. They appear to be using the **same tactics and language.** Therefore, it is **unlikely that this campaign is unique to any single airline.** Individual brands become popular avenues for these threat actors at different times, which could be a result of current success or ongoing experimentation.



# SUMMARY AND RECOMMENDATIONS

## Conclusion

This investigation uncovered an ongoing, well-coordinated social engineering campaign using advanced techniques to scam airline customers out of thousands of dollars. The threat actors are exploiting airlines' active engagement with dissatisfied customers on social media to lure victims.

The scam targets individuals who are frustrated, dissatisfied, or seeking compensation online. By creating fake accounts on X and Facebook impersonating airlines, their vacations brands, Customer Support, and Representatives, the threat actors are attempting to lure victims into sending direct messages to obtain their phone numbers and continue to seduce and trick innocent victims into thinking they are receiving compensation/money, when it reality they are sending it to the fraudsters.

**Our HUMINT investigation revealed several key elements:**

They are using WhatsApp numbers activated through fraudulent/bought accounts to communicate with victims over an internet connection.

Although their numbers on WhatsApp appear to be based in the United States, they are directing payments to Kenya and seem to be from there as well.

They request personal information including emails, phone numbers and credit card information. In some cases, they send a Google Form intended to steal information.

They have a guided social engineering technique that is designed to mimic official customer support mechanisms.

They send out emails/SMS activation for account to different international payment applications and websites such as Remitly and WorldRemit.

The scam ultimately tries to get users to believe they are getting compensation/refunded when they are sending money to Kenya.

New impersonation accounts are being created daily in the hundreds.

# Recommendations

## Take Down Impersonating Accounts:

Airlines should continue the proactive approach of taking down the impersonating accounts across all platforms. Prompt reporting and removal will help limit the scammers' ability to interact with potential victims.

## Educate Employees and Customers:

Airlines should develop an initiative to inform their customers and employees about these impersonation scams through official channels such as email newsletters, website notifications, and social media posts. Clear communication about the nature of the scam, warning signs, and how to verify official brand accounts will help customers stay alert and avoid falling victim to these fraudulent schemes.

## Reevaluate the Official Use Social Media Accounts:

Airlines should reconsider their social media strategy, particularly when responding to customer complaints. While customer support engagement is important, they should avoid soliciting private information such as phone numbers or booking details through public posts or direct messages. A more secure communication method, such as moving complex or sensitive interactions to official channels (like customer service phone lines or secure portals), should be prioritized.

## Contact Twitter and Facebook:

Airlines should reach out to the social media platforms (Twitter and Facebook) directly to report the large volume of impersonating accounts. Collaborating with these platforms can help expedite the removal of fraudulent accounts and bring attention to this ongoing issue. They should also request heightened monitoring of these platforms for any emerging impersonation campaigns targeting their brand.

## Contact International Money Transfer Websites:

Airlines should alert international money transfer services, such as Remitly, WorldRemit, and others, about the abuse occurring through their platforms. By notifying these companies about the scams and providing relevant account details or suspicious activities, they can help prevent these platforms from being used by scammers to complete fraudulent transactions. Working with these platforms may also lead to quicker responses to stop fraudulent payments and protect potential victims.

# CONTACT US


## ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

## USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

## SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

## PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

## UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

## JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001


## ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.
With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: checkpoint.com/exposure-management