**Fraudulent Transactions done with many credit card holders of Standard Chartered Bank at websites of Dmarket.com etc.**

Dear Readers,

This is to bring to your kind attention that a large number of credit card holders of Standard Chartered Bank have faced fraudulent international transactions at websites like dmarket.com, neonet.pl in amounts ranging into lakhs of rupees. These victims have reported these fraud transactions to stanchart bank within the time frame given by RBI, but the bank has not reversed these transactions permanently even after the matter being escalated to their principal nodal officer. Finally, we have reached to CEO Ms. Zarin Daruwala for a resolution and being told that we will be replied back in a weeks time.

In all these cases the bank keeps giving copy and paste template that they have shared OTP on mobile/email and hence the customer is liable. The bank is not at all doing any investigation on a series of similar transactions in these websites and taking action.

This is summary of the amounts the victims which are part of a WhatsApp group have been duped of so far.

|  |
| --- |
| **Disputed Fraud Transaction Summary of Victims** |
|  |  |  |
|  | **Credit Card** | **Debit Card** |
| Vaibhav | 101500 |  |
| Sujit Kumar | 102000 |  |
| Navneet Kumar | 37,000 |  |
| Dr Satya | 418355 |  |
| Vipul | 134000 |  |
| Sai | 234963 | 12912 |
| TOTAL | 1,027,818 | 12912 |

A common pattern seen is use of dmarket.com and transactions happening in early hours in India when most of the people are sleeping.

Now, we will be sharing some of the case details with you all in the victim’s own words.

**Vaibhav Aggarwal**

Two fraudulent international transactions were carried out by cybercriminals on my credit card which on were reported within 7 days to stanchart bank via complaint no SR201012112414 on 20th December, 2019 and the bank provided temporary credit. I also had filed a police FIR.

Then after some sham internal investigations the bank on Jan 25, 2020 sent a mail stating "We note that the said transactions were incurred post validating the credentials such as card number and the OTP triggered to your registered mobile number. An unique password (One Time Password) for each and every transactions will be generated and it serves as another level of authentication to carry out an online transaction. A review of our records indicates that the above-mentioned transactions were carried out on a 3D secured website post successful validation of your card credentials and the OTP which was sent to your registered mobile number, the said transactions were approved"

I asked them to share the VISA chargeback investigation report and case facts to prove that these transactions are done by me. But the bank has not provided any details mentioned below

1) No proof provided that these transactions were done on my residential address and i have received any goods

2)No proof provided about the delivery of product/services availed against the payment

3)Unavailability of ECI 3DS and CVV Response

4) No proof on matching of shipping and AVS matched billing address.

5) IP address used for the two transactions

In no way are they able to prove the same by sharing complete facts asked by me. Sending an OTP doesn’t mean that the OTP has actually been used in these transactions. The bank must share proofs of this which they are not able to. The bank is not able to prove that loss is due to negligence by a customer, such as where he / she has shared the payment credentials (Burden of proof 10. The burden of proving customer liability in case of unauthorized electronic payment transactions shall lie on the PPI issuer)

Also, it is common knowledge that international transactions don’t need OTP anyhow.

Even after making a complaint to the banking ombudsman their reply and stand remains the same without giving any investigation report and proving that transaction was done by the customer.



**Navneet Kumar**

My credit card was used for fraudulent international transactions without my knowledge on 17th February, 2020 card number \*\*9543 between 02:30- 02:35 AM. The amount was 512$(37000 INR).I complained to standard charter about these fraud transaction on same day around 2:30Am. When I called customer care they have blocked my Credit card immediately . When i asked customer care without OTP how this transaction has happened they informed me that it's a international transaction thats why it got approved without OTP. Because OTP is not required for international transaction. I was not using my credit card at all. I have never done a transaction with this card. They have increased my Credit limit automatically and after that this incident happened.Next day I got a call from fraud department about this transaction and I was informed that there was a fraud attempt on my card from a mac book but when I asked about the ip address and location as i don't own any mac-book, they refused to reveal it and told me they will investigate and let me know.After some days investigation started and closed without informing me the outcomes of it. When I called again then they informed me that They have found this transaction authentic in their investigation. When I asked for proof they didn't answered.about this fraud and a charge back was done and transactions reversed. One more thing i want to highlight is despite of too many request my credit card was not closed. Standard charted request number for closing of card-SR200006364. Dispute number -9142.

**Dr Satya**

My name is Satya Ranjan Patra, I was holding standard chartered credit card. On the night of 14 jan 2020, I was woke up to drink water and checked my phone, I got shocked when I saw a series of messages regarding online transaction from my credit card. Then I immediately inform bank regarding this fraud transaction through number they provided in their message “ Call 18002586465 if you have not done this transaction”.

On the same day I reported this incident to cyber crime Bhopal and raise a dispute in bank.

After taking all necessary action I am waiting for a bank’s reply and after one month bank replied “Transaction was done on the secured website and OTP is sent to registered mobile number”.

I just want to put some facts to you please reply me with concrete answers:-

1. The card was with me in my possession at all times during fraudulent transactions. I was not using the card for last 6 months till date of fraudulent transaction happened. It means NIL transactions on my card.

2. I did not clicked on any spam or phishing link as i am totally aware that i do not need to disclose my card details with any third party.

3. As per my trail mail, you will find that I have got only one OTP sms early in the morning as per trail mail, when I was sleeping which also means I did not shared it with anyone but two transactions were reported on statement, why? and please tell me OTP is used for smaller amount or for bigger amount with evidence.

4. When I woke up in the night, I observed following sms also to which i immediately responded. StanChart: For your account security, please respond urgently to verify your transaction. SMS 1 if you made the transaction; SMS 2 if you did not to +918800475522. I immediately sent 2 to +918800475522 which you can check from your records that you received sms from my registered mobile number. My number is postpaid and same is appearing on my mobile bill also. Now it was Banks system fault that it should had stopped the transaction immediately and should not had allowed merchant to claim these transactions.why the same happened as it is your Bank system Flaw?

5. I further request you to please provide me the IP address of the system from where the secured transaction( as per your saying) happened, you can check the IP location of the hacker by the same. I was in Bhopal with my family and i have the eye witness to the same. Same can be confirmed with my tower location of my mobile. I request you to prove that it was definitely done by me with concrete evidence.

6.Further to that, I request you to please check the shipping and billing address with the merchant to prove my involvement whether my name is appearing or not and it was me who have only availed the services from the merchant.

 7. The transactions were done in USD but initially i was only informed of the below sms to which i responded by sending 2 to +918800475522. You can check your records. If i responded with 2, why did not the bank immediately stopped this transaction and allowed merchant to claim it? Again, your bank system flaw.

9. Most importantly, i called your bank immediately same day same time at 4:05 AM regarding these fraudulent transactions and informed them regarding these frauds but your bank said, let us wait for 48 hrs and let it allow to be claimed by merchant and then you can raise the dispute. I was assured that i will be helped on every possible way but now bank is saying that i carried these transactions. My simple question to you all is that if I had informed on the same day and at same time, why the bank does not immediately stops the payment when the customer immediately says that these were not done by the customer, please explain?

10. I as a vigilant and awared customer have done my duty by immediately informing the bank regarding these unauthorised transactions immediately same day and at same time which comes under zero liablity policy of RBI.

11 The merchant name is PSP \*dmarket Gibralter GI which is domiciled outside India and is not known to me by any means. I also don’t know what kind of goods or services they provide?

Now the Onus is on the Bank to prove that it was indeed done by customer only as per RBI Circular No . RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6th, 2017 and in absence of any detailed investigation report, they cannot prove the same. I also understand that as an honest customer, I have given all my facts and figures to the bank which clearly indicates that I am innocent and hacking happened with the Bank. I would also like to clearly mention that till my lifetime, I will not pay a single penny to the Bank as I did not used the card for these fraudulent transactions.

**Vipul**

Hi. I am Vipul Bansal. I faced 2 fraudulent transactions on dmarket.com and alsen.pl on Feb 5 at 3:44 AM and 3:51 AM respectively. I was sleeping at that time. When I woke up in the morning, I complained about it to SCB customer care and they blocked my card and asked to dispute the transactions within 2 days. I raised dispute in the transactions on Feb 7 and also made a police complaint to cyber cell. Bank subsequently made temporary reversal. After a few days I again contacted them and they said that they have closed the complaint and found that this was a 3d secure transaction and OTP was used and making me liable for this. I asked them for investigation report but till now they have not been able to provide any investigation report to me and are not cooperating at all

**Conclusion**

The banks security seems compromised and hackers are taking advantage of this. It is shocking that the bank is not trying to investigate such a series of scams with its customers. All of us have made sure to tell all our friends, relatives and collagues to cancel their credit cards with stanchart to avoid being a victim of such frauds. Also, we are trying to let normal Indians know about this issue using the following links

1. change.org/p/standard-chartered-bank-standarrd-chartered-bank-not-helping-credit-card-customer-in-fraud-international-trans
2. <https://www.linkedin.com/posts/vipul-bansal-782234b3_scb-fraud-standardchartered-activity-6654761834534539264-_tDn>

**Resolution expected**

All of us want that these fraudulent transactions are reversed permanently and the bank immediately takes action as to how their credit cards are being hacked so easily. We hope their CEO – Ms Zarin Daruwala will look into this as their bank’s reputation will finish like this. We have got few calls from CEO office recently, but still the final resolution to reverse these transactions is not done

A global bank should have its risk systems in place and make sure its customers are protected from frauds.

 Regards

Stanchart Victims