Message from Dave Dyson:

18th November 2016

As you may already know, we recently became aware of suspicious activity on the system we use to upgrade existing customers to new devices and I wanted to update all our customers on what happened and what we have done.

I understand that our customers will be concerned about this issue and I would like to apologise for this and any inconvenience this has caused.

Once we became aware of the suspicious activity, we took immediate steps to block it and add additional layers of security to the system while we investigated the issue.

On 17th November we were able to confirm that 8 customers had been unlawfully upgraded to a new device by fraudsters who intended to intercept and sell on those devices.

I can now confirm that the people carrying out this activity were also able to obtain some customer information. In total, information from 133,827 customer accounts was obtained but no bank details, passwords, pin numbers, payment information or credit/debit card information are stored on the upgrade system in question.

We believe the primary purpose of this was not to steal customer information but was criminal activity to acquire new handsets fraudulently.

We are contacting all of these customers today to individually confirm what information has been accessed and directly answer any questions they have.

As an additional precaution we have put in place increased security for all these customer accounts.

We have been working closely with law enforcement agencies on this matter and three arrests have been made.

I understand that this will have caused some concern and inconvenience for our customers and for that I sincerely apologise.

David Dyson

CEO

What has happened? Am I affected or at risk?

We understand you are naturally concerned.

We’re aware of an attempted fraud issue regarding upgrade devices and are working with police & relevant authorities on the matter. We would like to reassure customers that their financial details are not at risk.

We can commit to you that in the unlikely event we see any illegal activity on your account, including unauthorised access, we will inform you as soon as that has been identified. No financial data such as Bank accounts or credit / debit cards are involved in this matter and your passwords and pin numbers have not been compromised.

So far we know that 8 devices have been stolen and those customers have been contacted. A system which is used to identify which customers are eligible for an upgrade was accessed by someone unlawfully.

Of course if you see any suspicious activity relating to your mobile account then please call us immediately.

Do you know when this occurred?

Within the last week we discovered suspicious activity and started our investigations and formally notified the Police. Our investigation is still underway and we are working with the Police very closely.

What is an upgrade system?

This is a system used to identify which customers are eligible for an upgrade. No financial information, such as card or bank details, are held on this system.

What information has been accessed?

We are still investigating but we can confirm that no payment or card information has been accessed. We have contacted those customers who have been impacted by upgrade fraud.

Why didn’t you tell customers sooner?

This is an ongoing criminal investigation and we are working with the Police to establish the full facts. We have contacted those customers who have been impacted by upgrade fraud.

How was it accessed?

This is an ongoing criminal investigation and we are working with the Police to establish the full facts.

Have you had any previous losses of data?

Upgrade fraud of this type is an ongoing industry issue.

Who did this?

We are working with the Police to establish who was behind this criminal attack.

Are you assuming that they are Three staff?

We are working with the Police to establish who was behind this criminal attack. Our focus is on identifying instances of handset fraud and preventing any further fraud following this attack

Were customer passwords lost?

Customer passwords weren’t lost. This was direct, fraud activity on our upgrade system

Have you notified the regulators/card providers?

No financial information is stored in this system. All the relevant authorities and regulators have been informed.

Should customers contact customer service?

Of course if they are worried they can, however we are contacting customer we believe may have been affected directly.

Has any information already been used or sold on by the fraudsters?

Our investigation has determined the purpose of this was to fraudulently obtain brand new mobile phones.

Can the information stolen be used to take money from my account/steal my identity?

We would reassure customers that their data has been secured and no payment or card information has been accessed.

We are contacting those customers who may need to take additional steps to mitigate any risk.

Should customers cancel their credit/debit cards?

We would reassure customers that their data has been secured and no payment or card information has been accessed.

You have broken my trust, how will you compensate me for it?

We have already confirmed that no financial information has been accessed. At this stage only 8 devices have obtained through this investigation.

I don't trust Three to keep my data secure, I want to cancel right now.

We have put in place enhanced controls to protect your mobile account and would assure you that Three takes the security of your data very seriously.

When will I know if I am impacted?

This is a live investigation, however we have already contacted all impacted customers. We have put in place enhanced controls to protect your mobile account and would assure you that Three takes the security of your data very seriously.

If I am one of those whose details were compromised, how can I make myself more secure?

We have contacted those customers who have been affected by this incident. We would recommend that, if you haven't created passwords or an account PIN (personal identification number) on your Three account that you do so as a precaution. You may wish to change any existing PINs or passwords on your account to further safeguard your details.

Are you working with the Police on this matter?

Yes. We have been working with external law enforcement agencies, specifically the NCA and the NCSC. Both organisations provide advice to consumers on how to keep your data safe and protect yourself from fraud. Details of these organisations and what they do can be found at www.ncsc.gov.uk and www.nationalcrimeagency.gov.uk

Three is very grateful for the support these organisations have provided during this investigation.

SIM Only deals.

Pay As You Go.

iPhone 7.

iPhone 7 Plus.

Privacy & Cookies.

Contact us.

Price Guide.

Media Centre.

Sitemap.

Delivery Information.