

Data Transparency Strawman

Fraud Prevention Philosophy

What is your approach to Fraud Prevention?

Fraudsters are constantly becoming more intelligent with the ways they commit crimes. Therefore, protecting you and your money is an absolute priority for us.

To better defend you and the wider financial system from financial crime, we are making significant investments in technologies, processes and in our people.

We want to ensure that you feel secure and educated against one of the fastest growing types of crime in the UK. So, if you don't feel sure when speaking to someone you don't know, or you have received digital correspondence that you aren't happy about, contact us.

What controls do you have in place/How do we protect you?

Two factor authentication – our Secure Key gives you added protection against the threat of fraud. It generates a temporary code which you use to access digital banking. You need your PIN or password, Touch ID, Face ID or Android Fingerprint. It means only you can access your accounts.

Real-time fraud detection system – as part of our digital security promise, we'll safeguard your money by keeping a look out 24/7 for unusual activity on your account. From time to time we may get in touch with you to check on anything suspicious.

Behavioural analysis – we use behavioural analysis to help make sure it's really you giving us instructions for your online banking. This tech builds a profile which helps us reduce fraud.

One-time passwords – we use Verified by VISA or MasterCard Identity Check Service for online purchases. If we need to check that a purchase is genuine, we will send you a unique 6-digit SMS passcode. The passcode is only used as an identity check and you should never share it with anyone.

Bank name display – we use bank name display when you set up a new payee to confirm which bank you are sending money to.

Transaction monitoring – we may send you a text message to confirm whether a card transaction has actually been made by you or to ask you to contact us regarding possible unusual activity on your account. If you are unsure, please contact the number on the back of your debit or credit card.

Helpful hints – our fraud and security centre on our website outlines key information on what we do to keep you safe and secure online, including how to protect yourself.

Free Security Software – we recommend you have security software (such as IMB Trusteer Rapport) as well as additional anti-virus software on your PC.

Customer Education and Awareness

What do you do to educate your customers to ensure they are fully aware of the latest fraud trends/advice?

Top Tips on Website

We have a dedicated Fraud and Security Centre on our public website which can be found by navigating to the 'Help' tab.

The help tab is located beneath the top navigation bar to Login or Register for Online Banking.

Advertising

Working with Rachel Riley (TV Personality), we've developed advertising campaigns to keep you up to date about the most recent scams.

Initiatives

We are proud to be a founder sponsor of Get Safe Online who help to protect people, finances, devices and businesses from fraud, abuse and other issues encountered online.

We are also a supporter of the Take Five campaign, have signed up to their voluntary code and made a commitment to meet their minimum standards.

Banking Platforms

Using the latest technology, we send tailored and relevant messages to you through online and mobile banking platforms to make you aware of any potential fraud threats.

Industry Expert

We have strong connections with the Dedicated Card and Payment Crime Unit (DCPCU), a police section of UK Finance. They have spent time educating our frontline staff on the most recent fraud and scam threats.

Community Events

We bring educational presentations to a wide range of people across the UK. This includes sections on ways to stay safe online and around most common fraudulent activity to look out for.

Branch Network

We have a Scams Leaflet available for you to take away along with information on Take Five.

We have fraud warnings/messages on our ATMs to let you know of the potential card fraud that can take place when you use an ATM.

Social Media

On our official Twitter, YouTube and Facebook pages, we post top tips on staying safe and understanding how you can protect your information from being stolen.

Contact

How and when we would contact our customers

One-time passcodes – when we need to verify who you are – like when you need to swap your digital secure key from an old phone to a new phone or you pay for something online with your card – we'll send a unique code to the most up to date mobile number we have for you.

The text will say exactly what the code is for, like creating a new payee. This code should only ever be typed into your digital banking and never shared with anyone, including us.

If you get a one-time passcode message you're not expecting, give us a call on 03456 002 290.

Text Alerts – if we notice something suspicious or need to get in touch with you, we may send you an alert either by email or text message.

Check our text messages page to see what our regular text messages look like and also see some messages commonly sent by fraudsters.

While we may ask you to reply to messages, we'll never:

- Ask you for self-generated codes from your secure key
- Include a link to a log in page
- Ask for your complete security number, password, or card number
- Ask you for answers to your security questions.

If you're not sure whether a text or email is genuine, Stop. Don't click on any links. Don't open any attachments. Just forward the email to phishing@hsbc.co.uk and we'll investigate it or call us on the numbers below.

In the UK: we offer an around the clock service to all our customers who can contact us on:

Premier customers: 03457 707 070

All other customers: 03457 404 404

Outside of the UK: For all customers: +44 1226 261 010

If you believe there has been a fraudulent bank transfer or bill payment that you did not authorise please call us on 03456 100 135 (Monday to Friday, 9:00am to 6:00pm).

If you have authorised a bank transfer or bill payment and now believe you have been the victim of a scam, please call us on 03455 873523 (24/7).

How we collaborate with the rest of the industry

Industry initiatives/collaboration

- We are members of UK Finance and take an active part in Industry Fraud initiatives.
- We are members of CIFAS – the UK Fraud Prevention Service.
- We contribute to the funding of the Dedicated Card and Payment Crime Unit who focus on card, cheque and payment fraud crimes.
- We share fraud intelligence with UK Finance and Law Enforcement to protect our customers.
- We have signed up to Take Five to provide our customers with up to date advice on fraud prevention.
- We are a participant of the Banking Protocol which helps to prevent our customers falling victim to fraudsters and rogue traders by working with law enforcement.
- We work with other banks to quickly recover fraudulent money for our customers.
- We are pleased to be among the first banks to sign up to the Contingent Reimbursement Model Code as part of our commitment to protecting our customers from fraud.
- We are a founder sponsor of Get Safe Online providing our customers with advice on how to protect yourself against fraud and identity theft.
- We are members of the National Fraud Database.

Summary

Fraudsters are criminals and can pretend to be someone they are not – like HSBC or the Police – to find out information about their victims. You should always make sure that the person you are talking to is who you think they are. We will never ask you for your security information like your digital or physical secure key codes. When we contact you about fraud, we will use email, phone calls and text messages and if you aren't sure, contact us.

We will continue to work alongside others in the industry to best protect our customers against this ever-changing threat.

Accessibility

If you need any of this information in a different format, please let us know. **This includes large print, braille, or audio.** You can speak to us using the live chat on our website, by visiting one of our branches, or by giving us a call.

There are also lots of other options available to help you communicate with us. Some of these are provided by third parties who are responsible for the service. These include a Text Relay Service and a British Sign Language (BSL) Video Relay Service, to find out more please get in touch. You can also visit: hsbc.co.uk/accessibility or: hsbc.co.uk/contact.

hsbc.co.uk

HSBC UK Bank plc. Registered in England and Wales with number 09928412.

Registered Office: 1 Centenary Square, Birmingham, B1 1HQ, United Kingdom. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Our Financial Services Register number is 765112.

DCP314 ©HSBC Group 2023. All Rights Reserved.