Thank you for your letter dated 11 October regarding the recent criminal cyber-attack against our US parent company, Equifax Inc.

First and foremost, I offer my sincere personal apologies to anyone who has been impacted by this incident. Although the cyber-attack exploited a US website application vulnerability, unfortunately some UK data was impacted. I can, however, confirm that no credit account information (such as balances or debts owed) relating to UK consumers was impacted.

Your committee asked Equifax to explain what happened and how UK consumers may be impacted. I hope the information below and response to your questions helps explain how this criminal attack affected the UK, and the steps Equifax Ltd has taken to protect consumers.

In your letter, you expressed concern at the length of time it took Equifax Ltd to notify consumers. I want to assure you that from the moment we learned about the incident, our team worked around the clock to identify the impacted UK consumers and to develop a plan to inform and protect them in the most appropriate way. I thought it worthwhile to set out the timeline of events and the process we followed, from being alerted by Equifax Inc of the cybersecurity incident, to notifying UK consumers. As explained below, once Mandiant, the independent cybersecurity firm that was engaged to conduct a forensic analysis of the incident, had transferred the complete impacted data set to the UK and concluded its forensic investigation on 2 October, Equifax Ltd was then able to identify all the impacted consumers that would need to be contacted, and on 13 October began posting consumer letters.

Your questions are answered below. Annex I contains a short note setting out the facts of the attack and the details of our response. Annex II lists the remediation services we have offered impacted UK consumers. Please note the distinction between Equifax Inc in the US and Equifax Ltd in the UK, where relevant. All dates refer to 2017 unless otherwise specified.

Chronology of events

29 July – 30 July
Equifax Inc's security team noticed suspicious activity around the US consumer online dispute portal.

2 August
Equifax Inc contacted King & Spalding, the company's outside counsel, regarding a potential security incident. King & Spalding engaged Mandiant to perform a forensic investigation. Equifax Inc notified the FBI.

2 August – 2 October
Equifax Inc and Mandiant conducted a confidential forensic investigation to discover which consumers and data had been potentially impacted.
21:30 UK time Equifax Inc issued a press release in the US regarding the cybersecurity incident. This announcement notified Equifax Ltd of the US data breach and confirmed that, although a forensic investigation was still ongoing, some data relating to UK consumers may be impacted.

Before 10:00 UK time Equifax Ltd notified UK regulators, the Financial Conduct Authority (FCA) and Information Commissioner’s Office (ICO), that some data relating to UK consumers may have been impacted by the cyber security attack in the US. Equifax Ltd also notified the National Crime Agency (NCA). Equifax Ltd was reliant on Mandiant’s ongoing investigation for information regarding the extent to which data pertaining to UK consumers had been impacted.

Mandiant delivered its initial analysis to Equifax Ltd while its forensic investigation was still ongoing. Mandiant informed Equifax Ltd that records relating to UK consumers may have been accessed and that the relevant data fields included various combinations of:

- Name
- Date of birth
- Phone number
- Email address

Equifax Ltd shared this information with the FCA and ICO.

After discussions with regulators, and based on available information from Mandiant’s ongoing investigation, Equifax Inc conducted analysis and estimated that approximately 300,000 UK consumers had a combination of their name, date of birth, phone number and email address accessed in the cyber-attack. We determined this group to be at the highest risk of identity theft.

To inform the public of our plans to notify consumers and offer them appropriate protection, Equifax Ltd issued a press release with an initial estimate of the number of consumers we expected to notify. Recognising that Mandiant’s investigation was ongoing, we added a contingency of 100,000, in case the final review revealed more consumers who would need to be contacted. This brought our risk-based estimate to 400,000. This approach was agreed by the FCA and ICO who reviewed and discussed our press release in advance of its release.

Equifax Ltd obtained a full copy of the impacted UK data from Equifax Inc in order to expedite the analysis and accelerate the process of contacting consumers. Our objective was to create a mailing database of relevant consumers by cross-referencing other Equifax Ltd proprietary data held in the UK against the information received from Equifax Inc. The data transfer required a secure environment so that the data could be interrogated safely and without further compromise. The transfer process was completed on 22 September. By using advanced analytical techniques and other data sets to enrich the fragmented file, Equifax Ltd was able to attribute identities to more consumers than Mandiant had initially identified.

Equifax Inc notified Equifax Ltd that further investigation showed that email addresses pertaining to UK consumers were not present in the data.

The discovery that email addresses were not impacted changed the risks to which UK consumers were exposed. Equifax Ltd also identified some driving licence numbers in the impacted files, although some were duplicates and others seemed to be incorrectly formatted. Further work was required to match this data to consumers.
Mandiant informed Equifax Ltd that it had identified a second data source containing UK data that also may have been impacted in the cyber-attack on Equifax Inc. Mandiant sent that file to the UK on 2 October and the Equifax Ltd team began analysis.

Mandiant completed its investigation and published a summary of its findings.

Equifax Ltd established that the compromised data in the second file included information about UK subscribers to Equifax.co.uk services. This file contained 96,275 records, relating to around 27,000 consumers.

Equifax Ltd informed the UK regulators of this development.

Detailed figures on the number of consumers impacted by the cyber-attack can be found in Annex I. There is no evidence of credit account information being impacted.

Throughout this process, Equifax Ltd extensively engaged with the FCA regarding the potentially impacted consumers and data, the draft letters to consumers, and press releases. We also had ongoing conversations with the ICO, NCA, DVLA, National Cyber Security Centre and Cifas.

Equifax Ltd met with senior FCA representatives.

Equifax Ltd issued a press release containing the revised number of 693,665 consumers to whom Equifax Ltd will write, and described our consumer remediation recommendations.

Equifax Ltd began printing letters to relevant UK consumers.

Equifax Ltd began posting letters.

To summarise, Equifax Ltd began writing to consumers 11 days after receiving the full set of impacted UK data (between 2 and 13 October). In that time, we conducted analysis and completed the labour-intensive process of matching each potentially impacted consumer identity with a valid home address. In doing so, Equifax Ltd recognised that much of the compromised data was several years old and sought to avoid rushing a mailing exercise that originally included, for example, deceased persons and out-of-date addresses.

With regard to your specific questions:

1. When did Equifax first become aware of the breach? When did it become aware that it included data on UK citizens? When did it inform the ICO and the FCA about the breach?

The security team at our US parent company, Equifax Inc, first observed suspicious network traffic associated with a portal used by US consumers to report disputes online on 29 July. They acted quickly to take the relevant portal offline, which in effect removed the access route used by the attackers. At this point, the scale of the attack was not known but Equifax Inc began an investigation into whether consumer data may have been impacted.

Equifax Inc disclosed the breach on 7 September in a press release issued at 21:30. Equifax Ltd learned about the breach and that some UK consumers' personal information may have been impacted. Based on the forensic work of internal resources and the cybersecurity firm, Mandiant, Equifax Ltd established that the UK core consumer credit data (such as balances and debts owed) or credit referencing systems were not impacted.

Equifax Ltd informed the UK regulators – the FCA and the ICO – before 10:00 on 8 September.

2. What was the “process failure” that allowed data of UK consumers to pass from Equifax Ltd to Equifax Inc, the US parent company between 2011 and 2016?
The data related to an historic system that was used by some UK business customers to validate consumers’ identities. The original software had been written in the US for US clients. In creating a version for the UK market, some functions of the platform were retained in the US. In 2014, Equifax Ltd decided to make the product wholly UK-based and began to transfer UK clients to an updated version in the UK. The process concluded in 2016. The process error was that the historic data remained in the US.

3. On 15 September, Equifax stated that 400,000 UK residents had potentially been affected by the breach. Why was its initial estimate so much lower than the figures published on 10 October? And can you provide assurances that data related to other UK citizens has not been compromised?

Equifax Ltd’s UK press release issued on 15 September provided an estimate of the number of impacted consumers based on Mandiant’s initial investigation as well as an additional contingency number, which led us to estimate that we would need to contact fewer than 400,000 individuals. This was based on our understanding from preliminary information provided by Mandiant that UK consumers’ email addresses had been compromised, and was released after discussions with the FCA and ICO.

Once we were able to repatriate the data files to the UK and conduct our own analysis, Equifax Ltd confirmed that email addresses had not been compromised, as initially believed. However, we also discovered that some UK consumers’ driving licence numbers were accessed. On 2 October, we received a second file from Mandiant, which contained data relating to Equifax.co.uk subscribers.

Our revised figures, published on 10 October, were based on Equifax Ltd’s own analysis of all known impacted data, including the second file provided by Mandiant. At the time of the first press release (15 September) we reasonably relied on the information before the investigation was complete. Once Equifax Ltd received the additional impacted data, we used the analytical tools, techniques and datasets we have available to establish valid identities and attribute home addresses to write to the impacted consumers.

Our methodology to determine the group of impacted UK consumers to whom we would write was developed in discussion with regulators. In the period between the two press releases, we agreed with regulators to contact impacted UK consumers that had name, date of birth and phone number accessed.

Mandiant’s review of the impacted data was completed on 2 October and they concluded that there is no evidence that any additional UK data was impacted.

4. Does the breach include information from electoral rolls purchased by Equifax? If so, has this information been compromised?

No.

5. Why has Equifax chosen not to contact, or offer any support, to individuals who have had name and date of birth compromised?

A combination of name and date of birth in the hands of a criminal does not in itself constitute sufficient information to increase materially the risk of identity takeover or similar malicious activity. Much of this information is available publicly (e.g., on social media, Wikipedia, or Companies House). In the absence of a postal address, phone number or other data, the hacker is unlikely to be able to defraud a consumer. There are other methods of reducing risks to consumers who are in this category that are discussed below, as well as our reasons for recommending those methods.

Equifax Ltd has a range of databases that are not publically available. Our own expert data scientists have had difficulty in matching the records impacted by this cyber-attack with known and validated UK consumers’ home addresses. Equifax Ltd concluded that the risk of writing letters of such sensitivity to home addresses which, in many cases, may be invalid would be an inappropriate course of action and would lead to unnecessary distress and risk for many individuals. The risk for consumers would increase if mail tampering were able to link home addresses to otherwise unusable data. Throughout our discussions, the ICO advised that it would be unwise for Equifax Ltd to write to individuals unless we had sufficient certainty that the correct person at a valid home address was being contacted.
As a credit reference agency, Equifax Ltd has mature business relationships with each of the UK high street banks. We are currently engaging with our banking clients (who between them represent over 90% of the UK’s current accounts) to explore how we can work together to alert the banks of possible fraud risk on the accounts which belong to potentially impacted customers whom are the closest match to those in the impacted data set. We expect this to be an additional effective route to consumer protection and fraud prevention.

Additionally, Equifax Ltd has already put in place a process whereby we will engage with any consumer who contacts us with concerns (whether or not they were impacted by the breach) and discuss with them the range of protections available, including the Equifax Protect service. These are described in Annex II.

Equifax Ltd has offered support to consumers who are worried about the risk of identity fraud and will continue to do so. We have endeavoured to help, quickly and discreetly, any consumer who has contacted us with concerns. In forming the decisions regarding the consumers to notify, and to make contact by posting letters, we engaged with regulators, including the FCA, ICO and the NCA.

6. When do you expect the notification process to be complete?

We have completed the notification process by posting letters to consumers in the first three risk categories (the four categories are listed on page 7 in Annex I). The process is underway for notifying consumers in the fourth category, whose name, date of birth and telephone number was impacted. It is necessary for Equifax Ltd to phase the process of posting letters so that we can promptly and effectively answer phone calls from impacted consumers. The final notification date will be dependent on the consumer response rates we experience, but we expect to complete the notification process by 24 November.

7. Can you confirm that the services you are offering to affected individuals offer no guarantee or insurance against identity theft, and provide no compensation in the event that an individual falls victim to identity theft?

No service available in the market today offers a guarantee against identity theft. The protections we offer to impacted consumers are a series of layered risk management tools that should significantly reduce the risk of identity theft.

Many consumers have already enrolled in remediation services that Equifax Ltd has made available. The protections we have offered (detailed in Annex II), especially the Cifas protective registration, have been shown to be useful tools in identifying identity takeover and fraud, and reducing the negative outcomes of such activity. We believe that relying only on an insurance-based solution would be the wrong approach for consumers.

For the majority of impacted UK consumers we have notified, the main risk is unwanted cold calling. The National Cyber Security Centre has issued advice to consumers about dealing with suspicious phone calls, emphasising that individuals should not divulge any security information.

Consumers who have potentially had their driving licence numbers or Equifax.co.uk membership information impacted have been offered a free comprehensive ID protection service, that will enable them to monitor their personal data. The service provides enrolled consumers with access to credit information, and alerts them to potential signs of fraudulent activity. The service incorporates web and social media monitoring, alerting the consumer to publicly available information about them. These services are free to use, simple to sign up to, and provide immediate protection for consumers. Annex II contains the information we have posted to impacted consumers describing the services available. This includes information about services provided by other UK-regulated organisations that consumers may prefer to take up in addition to, or instead of, the free services offered by Equifax Ltd.

8. What compensation will Equifax be providing to individuals whose sensitive personal data has been breached, and who have thereby been put at much higher risk of identity theft?
The protections we are offering consumers are proportionate to the risks posed by this cyber-attack. The purpose of our offered remediation tools is to prevent harm to consumers. Evidence suggests that the risk of identity theft is relatively low.

As a FCA regulated business, Equifax Ltd already sets out to provide fair treatment to people who have concerns or complain about Equifax Ltd, and we have a good record of responsible conduct. If, in the future, a consumer believes he or she has been the victim of identity theft and believes the Equifax Inc breach was the cause, the complaint will be investigated fairly and promptly. All complaints will be considered individually on a case by case basis. All complainants also have the opportunity to take their case to the Financial Ombudsman Service if they disagree with our assessment and resolution of their complaint. We believe this represents a fair and effective method of remediating consumer distress and inconvenience.

9. What compensation will be paid to those who fall victim of fraud due to the information which ends up in the public domain due to the leak from Equifax?

Please see our answer to question 8.

10. What are the data sharing arrangements between Equifax Ltd and TDX Group; and is there a risk that data held by the latter may also form part of the breach?

Equifax Ltd performs data enrichment services for TDX Group (TDX), in support of TDX’s debt collection and debt administration activities for private and public sector clients.

Data enrichment typically involves TDX passing a file of data to Equifax Ltd, with a request for relevant additional data relating to those data subjects to be returned. TDX also uses other data suppliers. The process is documented on a client-by-client basis. Data is processed in this way based on TDX’s legitimate interests (acting on behalf of its clients) in administering and collecting debts. As part of its activities, TDX oversees a panel of debt collection agencies, to whom relevant data is typically passed to support the efficient collection of debt. Equifax Ltd does not retain TDX data following the completion of the enrichment process.

Equifax Ltd systems hosted in the UK are separate from the US business, and were not impacted by the breach announced by Equifax Inc on 7 September. TDX systems were similarly not affected. Nonetheless, we are reviewing security operations across all operations and will make improvements as appropriate.

Conclusion

This incident cuts to the heart of what Equifax does. It is our responsibility to fix the problem, and we will. We also believe that it is time for business and government to come together to confront the massive economic and national security threats represented by cyber criminals. There are no fail-safe means to prevent cyber-attacks, and every organisation is at risk. The challenge requires a combined effort across public and private organisations, and Equifax Ltd is committed to working with other businesses and policymakers to help build stronger cyber security defences for the benefit of consumers and our economy.

I would like to take this opportunity to publically pay tribute to Equifax Ltd employees who have been working around the clock in conjunction with government agencies, regulators, and investigatory authorities, in order to identify and assist potentially impacted UK consumers.

I hope my response reassures you that Equifax Ltd has endeavoured to act in the best interests of UK consumers. Please do not hesitate to contact me should you require any further information.

Yours sincerely,

Patricio Remon
ANNEX I

ADDITIONAL INFORMATION

What happened?

On 7 September, our US parent company Equifax Inc announced it had been the victim of a criminal cyberattack. We now believe that this criminal attack occurred through a combination of human error and technological error. The human error involved the failure of Equifax Inc personnel to apply an upgrade to the Equifax Inc US consumer dispute portal in March 2017. The technological error involved a scanner which failed to detect the vulnerability on this particular portal after the upgrade should have been made. Both errors have since been addressed as well as comprehensively reviewed. On 29 and 30 July, Equifax Inc security team noticed suspicious activity around the US consumer online dispute portal. To understand the scale and impact of the cyber incident, Equifax Inc employed a recognised independent expert cyber security firm, Mandiant, to analyse the potential impact of the breach.

Equifax Ltd is a separate UK entity with its own systems and servers and was not breached. Equifax Ltd confirmed this in a statement to the UK media on 15 September.

Regrettably however, files dating between 2011 and 2016 relating to UK consumers were held in the US and were impacted by this incident. Although these files contained duplicate information, spurious fields, and sizeable test datasets, they also included some data relating to actual UK consumers.

Equifax Inc commissioned an independent cybersecurity firm, Mandiant, to conduct a forensic investigation into the data that may have been impacted as part of the incident. Mandiant concluded their investigation on and had transferred the files containing UK consumer data to Equifax Ltd by 2 October.

Equifax Ltd has brought to bear proprietary analytical tools, techniques and data asset in order to ‘fill in the blanks’ and attempt to establish actual consumer identities and attribute current home addresses to impacted UK consumers.

After consultation with the FCA and ICO, Equifax Ltd started to post letters to relevant impacted consumers on 13 October.

What did the files contain?

Equifax Ltd’s audit of the impacted data relating to UK consumers identified:
- File one contained 12 variables (data fields);
- File two contained 269 variables (data fields).

Within the total impacted data, the following variables could be potentially used to identify individuals:
- File one: full name, date of birth, phone number, driving licence number;
- File two: full name, phone number, email address, username, password, secret question, answer to secret question, and masked credit card number.

Note that not all these variables were populated in every record.

The remaining variables in both files contained either blank fields or data that were not identifiable to an individual. Examples include:
- ‘event status’ (y or n)
- ‘system date’ (CREATE_SYSDT)
- ‘data class’ (MEDIA or blank)
- DOC_CD_OVM (blank, O or V)

The vast majority of these variables were system-generated.

What were the results of Equifax Ltd’s investigation?

Equifax Ltd announced on 10 October that our analysis was complete and that we expect to contact 693,665 people by post. This number comprises four consumer risk categories as follows:
- 12,086 consumers who had an email address associated with their Equifax.co.uk account in 2014 accessed (sourced from file 2)
14,961 consumers who had portions of their Equifax.co.uk membership details – such as username, password, secret questions and answers and partial credit card details – from 2014 accessed (sourced from file 2)
- 29,188 consumers who had their driving licence number accessed (sourced from file 1)
- 637,430 consumers who had their phone number accessed (sourced from file 1)

In answer to the Committee’s general questions:
- 9,725 unique credit card numbers were contained in the data records. These numbers were partially redacted (also referred to as ‘masked’) and take the format of 123456xxxxxx1234.
- No credit account information was compromised, including information provided through data sharing schemes.
- Approximately 14.5 million records contain a combination of unique name and date of birth only. It is not possible to accurately identify how many individuals this relates to. As explained above, the data includes spurious and inaccurate records. It is not uncommon for one name and date of birth combination to correspond with zero, one or multiple addresses on the wider Equifax Ltd database. An attempt to write to these people would result in multiple consumers being contacted in error, causing unnecessary concern and risk.

What is the risk to UK consumers?

Our priority is to ensure all impacted consumers receive the appropriate advice and protection they need to safeguard their identities and minimise risk.

For the vast majority of UK consumers we are writing to, the main risk we need to protect them against is cold calling or phishing messages. To that end, we have emphasised on multiple occasions via the media that genuine Equifax Ltd correspondence will never ask for money, and if they receive such correspondence they should not respond. We have also confirmed that we will not be making any outbound telephone calls to consumers for security reasons.

The risk of identity theft is relatively low even for consumers in the highest risk category. On 10 October the National Cyber Security Centre issued advice that the 14,961 consumers who have had security details from their Equifax.co.uk membership account accessed should ensure that those details are not used on any other services or accounts. We have offered impacted individuals a range of services. These protections, especially the Cifas protective registration, have been shown to be significantly useful in detecting identity takeover and fraud and reducing the negative outcomes of such activity.

What is Equifax Ltd doing now?

Now that Equifax Ltd’s investigation has concluded, and having consulted with relevant regulators, law enforcement agencies and advisers, we are in the process of posting letters to all impacted consumers to offer them Equifax and third-party safeguards.

The letter an individual receives is bespoke to each risk category. The letter describes what data has been compromised, along with what services are available to help the consumers protect their identities. The protections include access to credit information and a monitoring system to alert them to any potential signs of fraudulent activity. The service incorporates web and social media monitoring, and alerts consumers to any publicly-available information about them. These services are free to use, simple to sign up for and will provide immediate protection for consumers. A copy of this offer to consumers is available in Annex II.

We have also set up a Freephone number which is staffed seven days a week from 8am to 8pm. This telephone line is dedicated to providing information and advice for consumers who have been – or are concerned they have been – impacted by the cyber-attack.

This guidance is also available on our website, which is regularly updated.

Crucially, we continue to invest heavily in cybersecurity. Equifax Ltd is reviewing its processes and will make improvements to minimise the chances of a security incident.
Who are Equifax?

Equifax Inc is a global information solutions business, headquartered in the United States of America in Atlanta, Georgia. Employing approximately 10,000 people across 24 countries, the business is listed on the New York Stock Exchange. The UK subsidiary, Equifax Ltd, is authorised and regulated in the UK by the Financial Conduct Authority and other regulators. Equifax Ltd employs around 800 people in the UK and Ireland. Equifax Inc and Equifax Ltd are distinct legal entities operating in different continents.

Equifax was founded 118 years ago and now serves as a source of consumer and commercial information in the world. The information helps consumers, private entities and public entities make financial decisions in a more timely and accurate way. Behind the scenes, we help millions of British citizens access credit to buy a house, car, or start a small business. We also work with a wide range of UK businesses to supply analytical and information solutions.
ANNEX II

SERVICES OFFERED TO IMPACTED UK CONSUMERS

Equifax are offering you several free services which are detailed below.

If you need any help please contact our customer care team on Freephone 0800 587 1584, they are here to support you seven days a week from 8am to 8pm.

Here is a summary of the services and each section is listed in more detail below:

1. Equifax Protect provides credit report monitoring service to alert you of any changes on your credit report.
2. Equifax WebDefend provides web monitoring services to alert you if your personal details are used on the web.
3. Equifax Postal Service provides you with a copy of your credit report by post.
4. Cifas Protective Registration is a service that reduces the risk of identity fraud. Cifas is the UK’s leading fraud protection service. Equifax will cover the cost of this service for you.
5. We have listed other companies that provide your credit report and score free of charge.

Important: We will require some information from you to set up these services but we will not ask you for any credit card details or bank account details.

1) Equifax Protect

Equifax Protect is an identity protection service that monitors your personal data, including your credit information, and alerts you by email or SMS message to potential signs of fraudulent activity. We can provide this for 12 months. If you want it for longer it will automatically extend for another 12 months free of charge.

The service takes less than ten minutes to set up via phone. It will help you track when and where your data is being used so you can identify any unauthorised activity. It consists of:

✓ Equifax WebDefend as detailed below;
✓ Regular email or SMS alerts notifying you of any significant changes to your Equifax Credit Report. This will help you identify any fraudulent activity early on.
✓ Unlimited access to your Equifax Credit Report that allows you to check that the information held on your credit report is correct.

Our Customer Care team will set this up for you in less than 10 minutes.

2) Equifax WebDefend

If you do not wish to take Equifax Protect then you can still take Equifax WebDefend.

WebDefend is a monitoring service which we can provide to you for 12 months.

It provides you with the following:

✓ Monitoring of websites used by fraudsters to trade personal information
✓ Alerts if your information is found to be at risk
✓ You can set up alerts for the following:
  • Driving licence number
  • 6 different telephone numbers
  • 6 different email addresses
  • 12 Credit / Debit cards
  • 6 Bank Accounts
· National Insurance Number

Our Customer Care team will set this up for you in less than 10 minutes.

3) Equifax Postal Services

I understand you may not wish to use the internet for services. If so we can provide you with a free copy of your credit report by post. Our Customer Care team can set this up for you in around 5 minutes.

Special Assistance - If you need larger font, audio or braille services please call us.

4) Cifas Protective Registration

Cifas Protective Registration is a service that reduces the risk of identity fraud. It is provided by a separate organisation called Cifas, which is the UK’s leading fraud protection service.

On registration, your details will be added to the National Fraud Database, which will mean that applying for products and services may take longer than usual because organisations will take further steps to verify your identity.

Equifax can apply for this service on your behalf and we will cover the cost of this service for one year. The service takes around 10 minutes to set up via phone, and we will need to provide Cifas with your name, gender, date of birth, current address, contact telephone number and email address. Call us on Freephone 0800 587 1584.

You can find more information on this service at https://www.cifas.org.uk/services/identity-protection/protective-registration

5) Other Credit Report providers

We understand that you may not feel comfortable using our service now. There are other providers that can provide your credit report and score free of charge, including:

- Noddle (part of CallCredit) www.noddle.co.uk
- ClearScore (they use Equifax data) www.clearscore.com

Useful information to protect yourself

There are several independent websites providing useful information on how to identify if fraud has taken place and actions you can take to protect yourself.

- The ICO (Information Commissioners Office) www.ico.org.uk/for-the-public/identity-theft
- Action Fraud www.actionfraud.police.uk
- UK Finance www.financialfraudaction.org.uk/consumer
- CardWatch www.cardwatch.org.uk