IDENTITY THEFT AND DATA BREACH WHITEPAPER

Autumn 2016

EQUIFAX®

Contents

All figures, unless otherwise stated, are from YouGov Plc.

1 http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/filew

2 http://www.telegraph.co.uk/news/2016/06/26/police-force-website-hacked-by-football-loving-albanian-group/

3 Total sample size for questions regarding company data breaches was 2037 adults. Fieldwork was undertaken between 17th-20th June 2016. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18+). Total sample size for questions regarding personal identity theft concerns and online protection such as multiple passwords was 2060 adults. Fieldwork was undertaken between 6th – 7th June 2016. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18+).

4 Cifas 2016 Fraudscape Report

5 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/01/your-reputation-is-at-risk-if-you-don-t-keep-data-safe-ico-warns/

6 Excluding 25th/26th December

The growing issue of identity theft and fraud

With the financial gains possible, it is unsurprising that fraudsters continually find new ways to get hold of consumers' personal information. Yet, worryingly, consumers' awareness of scams and how to protect themselves, particularly online, is still low.

Making the problem worse – and the fraudsters' ride easier – is that there are still too many examples of companies that hold consumer data not doing enough to protect the information they have. This not only puts the consumer at risk of becoming a victim of identity fraud, but also threatens the reputation of the company. Even long standing loyal customers could lose faith and seek alternative providers for their goods and services.

A recent report from the National Crime Agency (NCA)[1] observed that law enforcement bodies were losing the 'cyber arms race' with criminals. It highlighted a need for a stronger partnership between authorities and businesses to better fight online crime.

And it's not just private companies risking the safety of consumers' identities. The public sector is equally vulnerable. For example, in June 2016 a breach of the South Yorkshire Police Force's website potentially put confidential data at risk. The hackers did state that they had only uploaded a false home page to run images, videos and text relating to the Euro 2016 football tournament. But the potential for further damage was extensive.[2]

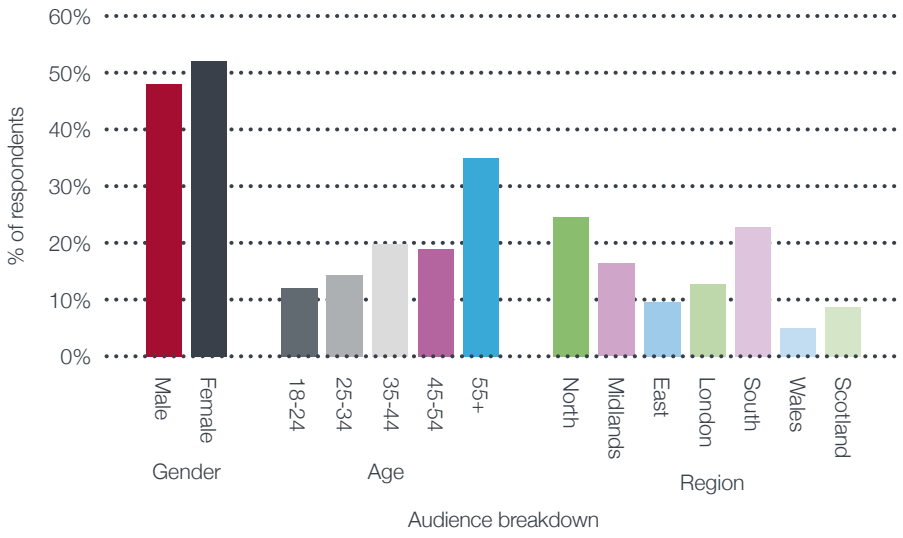
To assess what consumers understand about identity theft and fraud and the actions they take to protect themselves, as well as find out how consumers feel about companies that experience data breaches, Equifax commissioned YouGov to undertake an in-depth study.

The study comprised two detailed consumer surveys, one focusing on company data breaches and the other on how consumers protect themselves against identity fraud, and how much of an issue they believe it to be.[3]

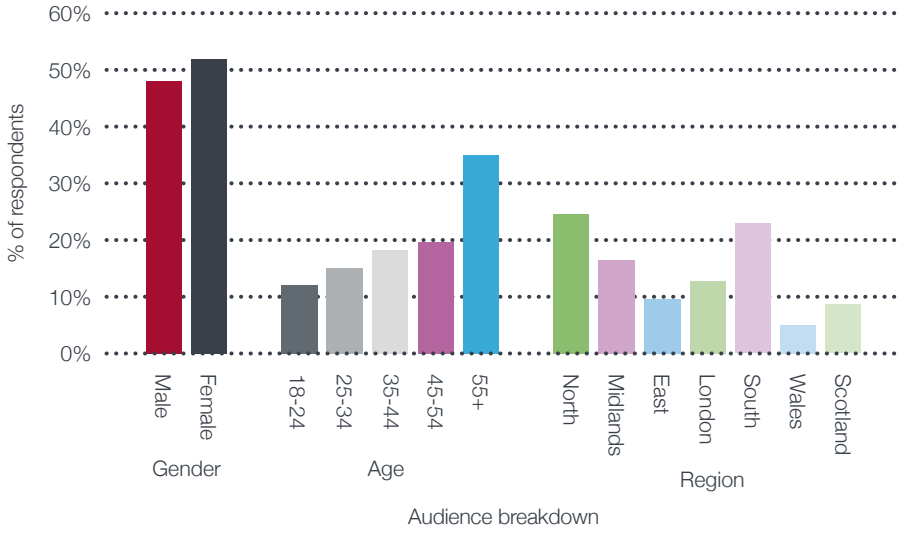
Demographics

Over 2,000 consumers took part in each online survey. All areas of England, Wales and Scotland were represented.

Respondent breakdown for company data breaches survey



Respondent breakdown for personal identity fraud concerns and online protection survey



Executive summary: the expert view

More than half of consumers surveyed claimed they are worried about identity fraud and account takeover. But with CIFAS, the fraud prevention organisation, reporting a 16% annual increase in fraud[4], it is clear that more consumer awareness is essential to tackle to the growing problem. Encouragingly, 88% of respondents within the Equifax research did agree that sharing personal information on social media sites increased their risk of falling victim to identity fraud, but again this should be even higher to ensure consumers are protecting themselves.

"...whilst consumers are doing little to protect themselves, they have high expectations of companies..."

High expectations

However, when it comes to companies that hold their personal data, consumers are less relaxed. Most would not use a company for the first time if they knew they had previously experienced a data breach, and 61% would expect financial compensation if their details were misused as a result of a data breach. It appears, therefore, that although consumers are doing little to protect themselves, they have high expectations of companies and rely on them to look after their information securely and protect them from fraud.

Of course, it is not just consumers who expect companies to look after their data and act quickly if anything compromises their privacy. The Information Commissioner's Office (ICO) demands the same. Companies of every size have legal obligations under the Data Protection Act to look after any data they hold, and can expect fines if they don't act appropriately to keep the data secure.

In January 2016, the Information Commissioner at the time, Christopher Graham, reminded companies that their reputations are at risk if they do not keep consumer data safe:

"Companies that play fast and loose with people's personal information risk the wrath of the ICO and that means fines of up to £500,000. A heavy fine is bad enough, but the time, energy and money it takes to rebuild customer confidence can be as severe a punishment as the fine itself.

"…people care about what happens to their personal information. Getting it right is not only an obligation under law, but it should be central to an organisation's reputation management."[5]

Over half concerned about account takeover fraud

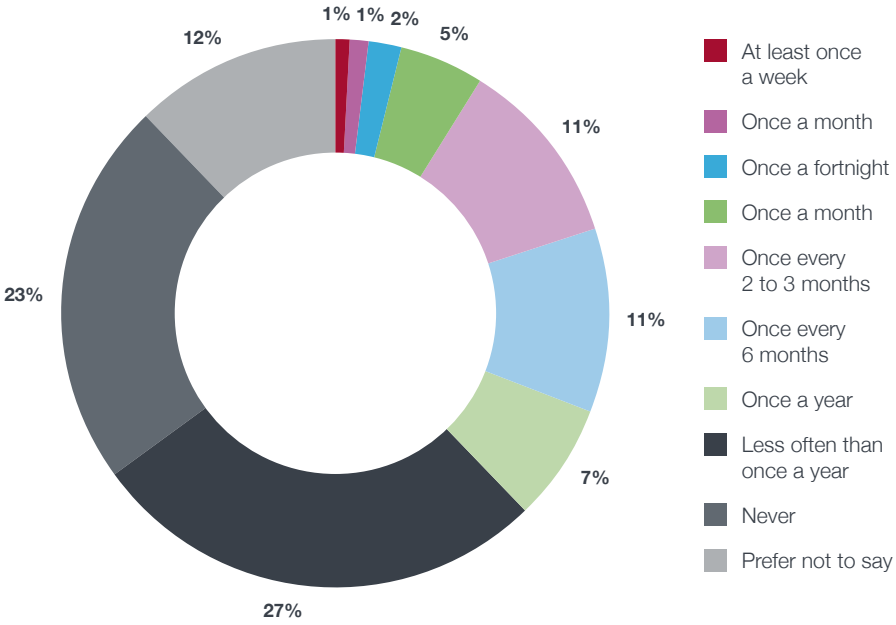
55% of GB adults who responded to the survey are worried about identity theft – defined as the act of obtaining the personal or financial information of a real person with the intent of assuming their identity.

56% stated that they are worried about identity fraud – the act of using a stolen or fictitious identity to make applications for new financial products, services or bank accounts. The biggest worry, with 57% of GB adults concerned, is account takeover fraud – that is having sufficient information to be able to use real account details to purchase products and services. Figures from CIFAS for 2015 report a 49% increase in this type of fraud from the previous year, with 86% of identity fraud committed online.

Worryingly, 7% of respondents have at some point in the past provided personal information to a company or individual over the phone, via email or through a website without initiating the contact.

10% of consumers are very diligent in protecting themselves against website breaches, by changing their online passwords at least once a month. However, 27% change their passwords less often than once a year, and 23% admitted to never changing their passwords unless specifically prompted by the website.

Approximately how often, if at all, do you change ANY of your online passwords without being asked or prompted to do so?

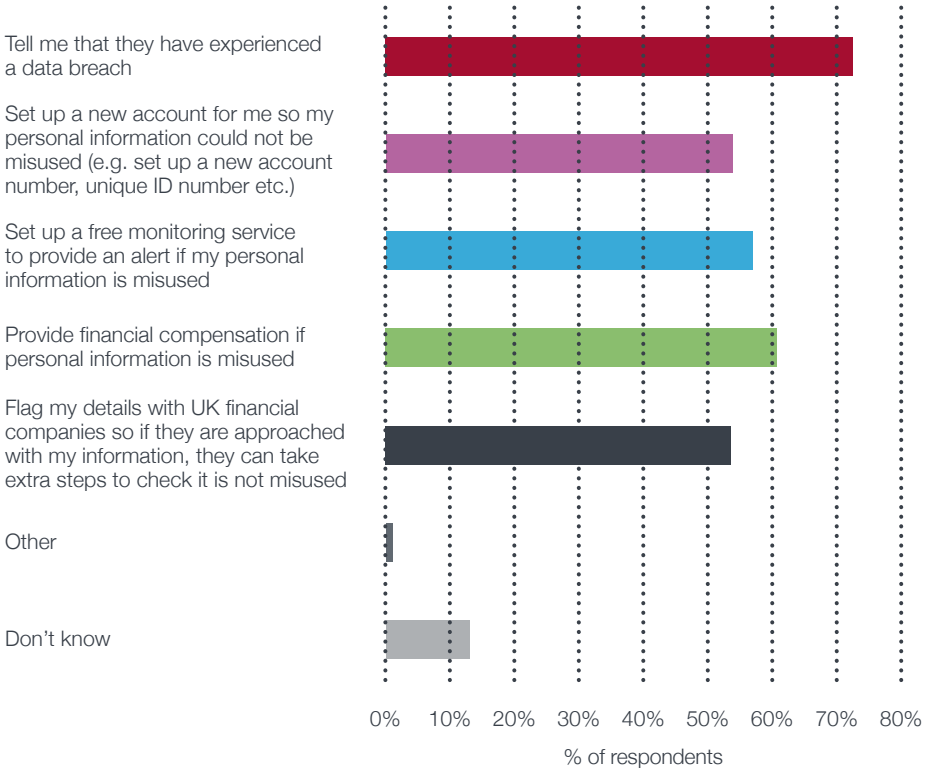


When it is possible for fraudsters to obtain online passwords through simple phishing scams, these high figures represent easy access to tens of thousands of online accounts.

Company data breaches

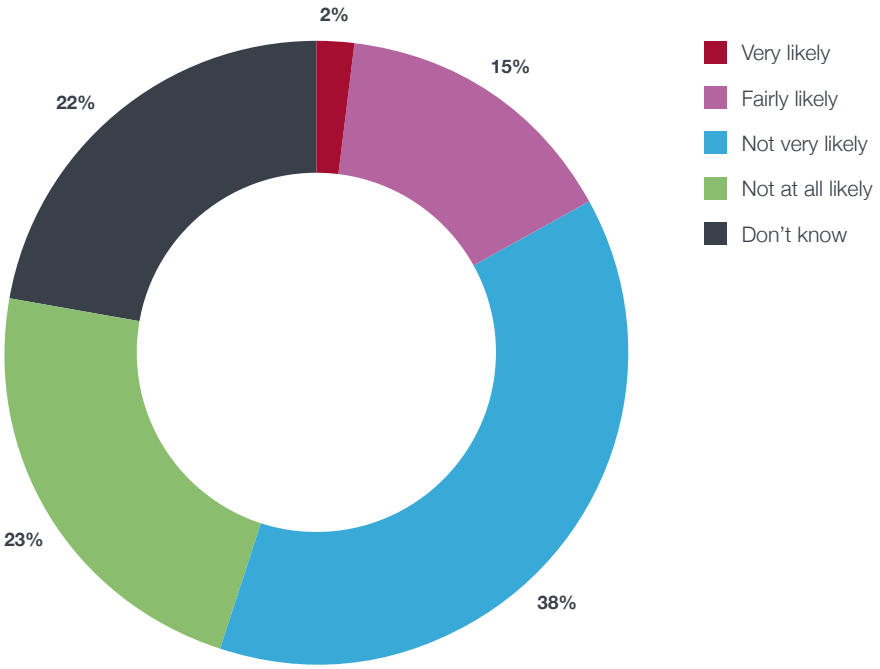
Almost three quarters (73%) of GB adults think that companies should tell them that they have experienced a data breach, and 63% of respondents would expect that notification to come within hours. A further 21% would expect to hear on the same day. To meet these high expectations, companies must ensure they have processes in place to manage such a crisis efficiently and effectively.

Which, if any, of the following do you think the company should to do for you as a result of a data breach?



If a company experienced a data breach, 61% of GB adults would be unlikely to purchase goods or services from them if they had not previously been a customer. This clearly demonstrates the importance of data security for companies of all sizes – the potential loss of business could be catastrophic.

In general how likely, if at all, do you think you would be to purchase goods or services from this company in the future, if you were required to provide personal information?



Taking a closer look: the results in detail

The generational differences

There is a clear difference in the attitudes of different age groups, regarding the sharing of personal information on social media websites. The youngest group, 18-24, a large proportion of whom will have grown up with access to the internet and using social media sites daily, appear to be more relaxed. Just 40% believe sharing personal info on their pages could present a risk of identity fraud. However 60% of the 55 and over group felt this was a risk.

Regionally, those living in the Midlands and Scotland are the most wary of sharing details on social networks, with 55% and 56% respectively, strongly agreeing that this posed a risk.

Consumer concerns

In terms of consumer concerns about identity fraud, theft and account takeover, the same applies. The 18-24s appear far less concerned – 36% worry about identity theft, 41% about identity fraud and 42% about account takeover.

Contrasting with this are the 45-54 year olds, who are far more concerned – 63% for identity theft, 64% for identity fraud and 62% for account takeover fraud.

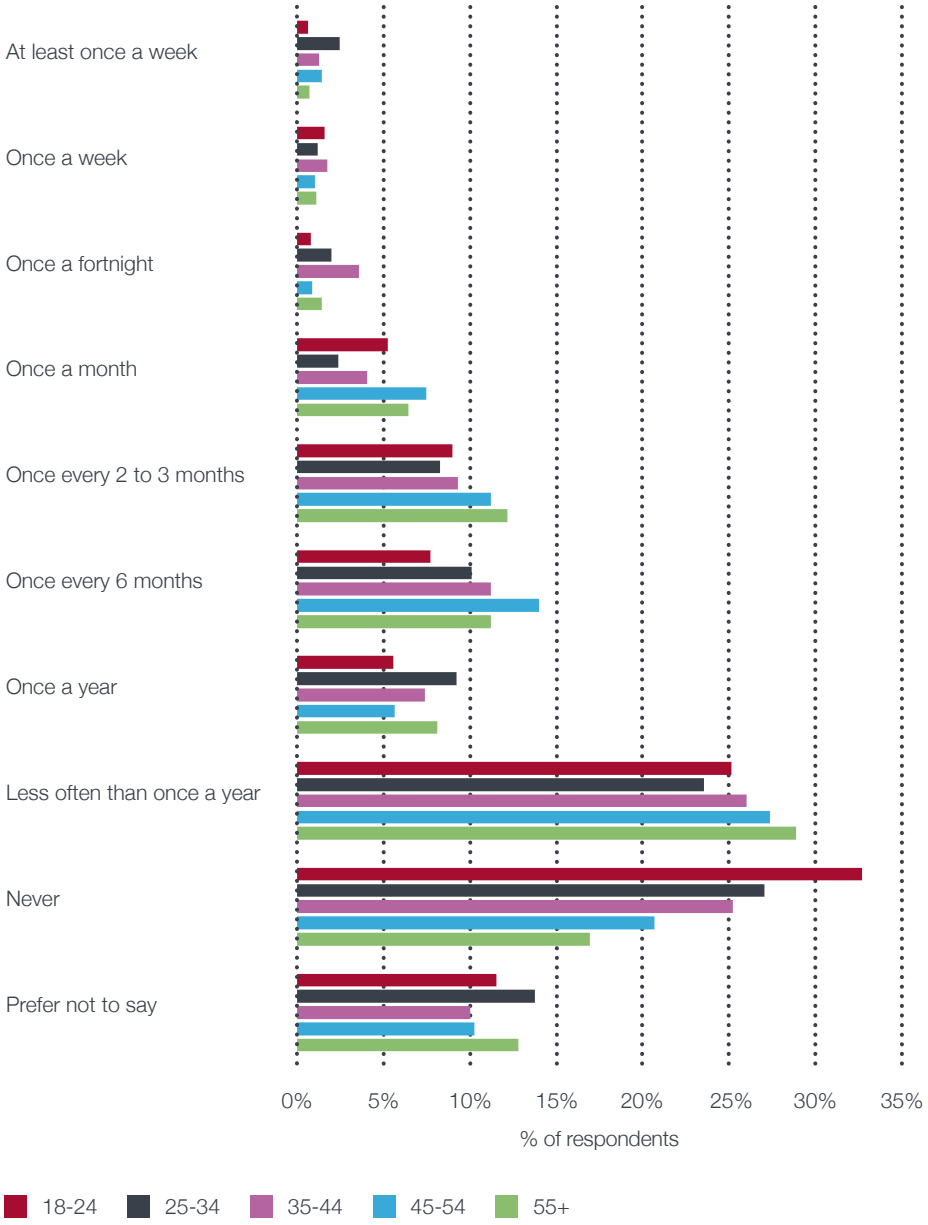
Women appear to be more concerned than men, with 17% vs 11% concerned about identity theft and similar figures for the other types of fraud – 16% vs 11% for identity fraud and 13% vs 17% for account takeover fraud.

People living in Wales appear to be consistently the most concerned region (18% identity theft and fraud, 17% account takeover), with Londoners most worried about account takeover (18%) and those living in the South of England generally far less worried – 10% for both identity theft and fraud.

Protecting themselves

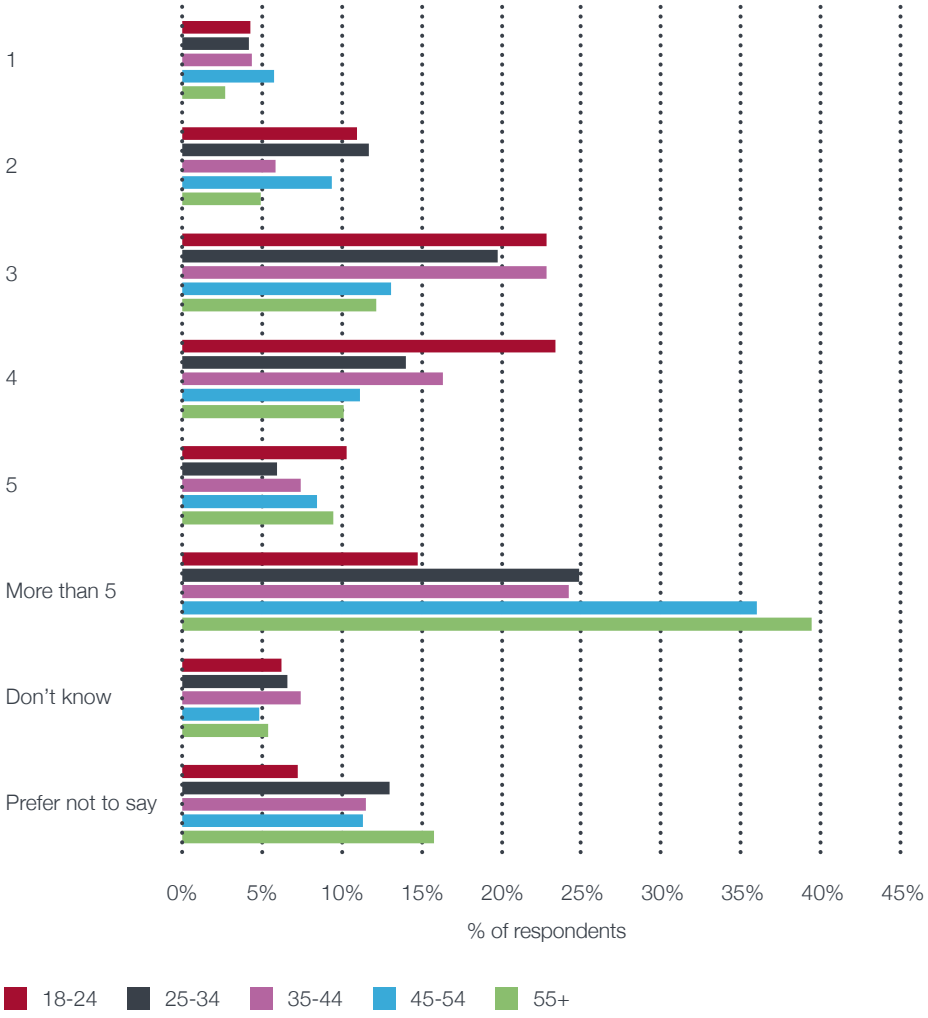
Regularly changing passwords is crucial to make it harder for fraudsters to get into people's accounts. But it seems that although the 18-24 year olds are the most switched on to the online world, they are also the most lax and least likely to change passwords regularly.

Approximately how often, if at all, do you change ANY of your online passwords without being asked or prompted to do so?



There is little difference between men and women with 21% men and 24% women never changing their passwords. So although women appear to be more concerned about identity theft and fraud, and account takeover, they are changing passwords less frequently.

Approximately how many unique passwords do you have for your online accounts (e.g. email, online banking, social media websites etc.)?



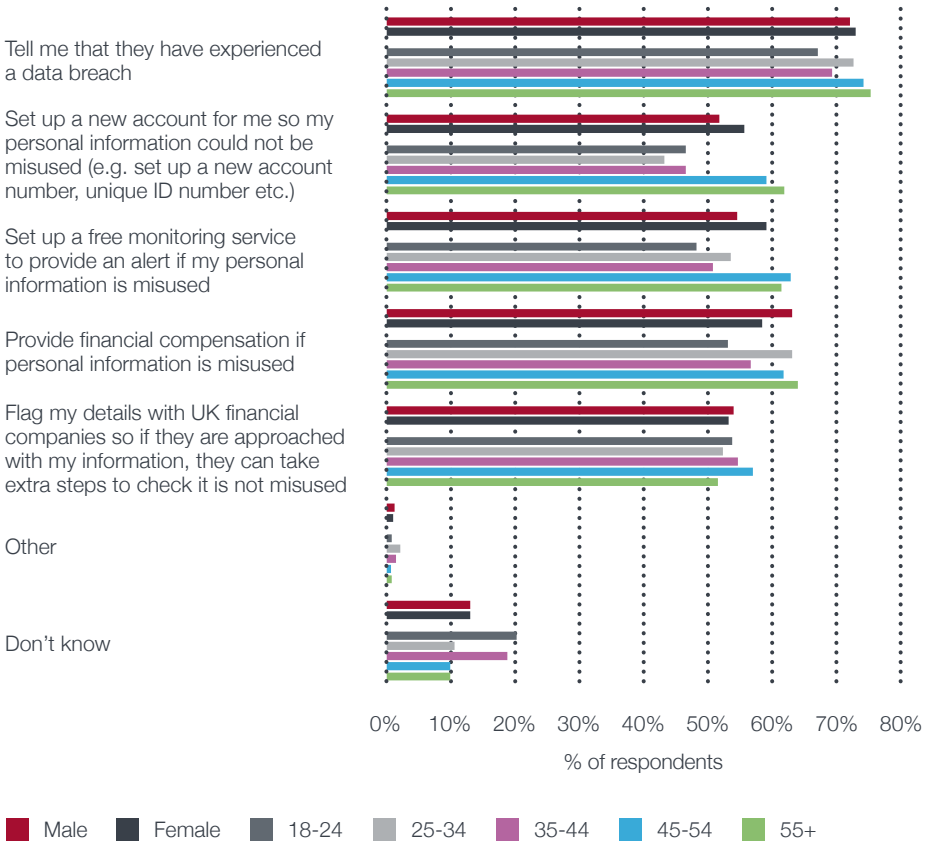
10% of 35-44 year olds and just 4% of 45-54 year olds have provided personal information to a company or individual over the phone, via email, or over the internet without machining the initial contact with the company. Therefore, they are providing their personal information without being sure of the initial source.

Consumers' expectations

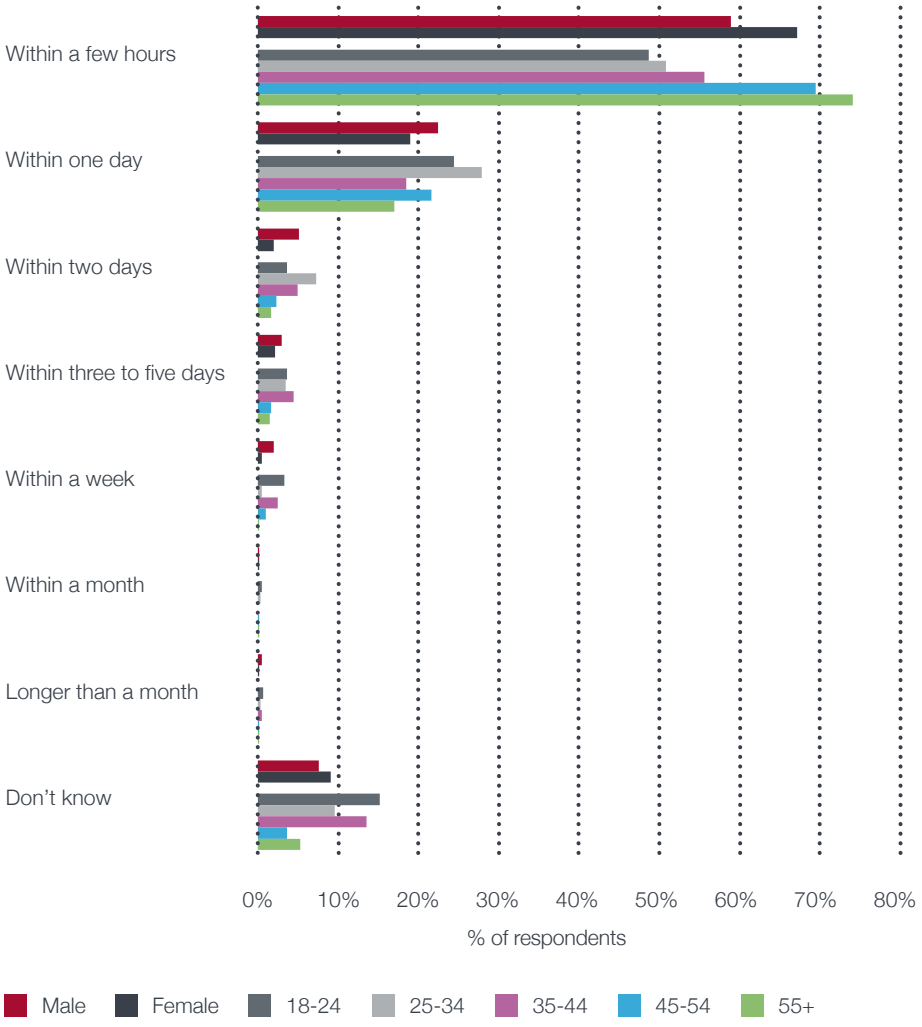
Almost three quarters (73%) of GB adults online think that companies should tell them that they have experienced a data breach. Breaking this down by age group, we can see that the older generation is more demanding in terms of companies being open about data breaches – 75% of over 55s, compared to 67% of 18-24s felt a company should tell them about any breach.

Nearly two thirds of all respondents (61%) believe that financial compensation should be provided if personal information has been misused. But there is a split between men and women, with men more expectant of financial compensation – 63% of men and 58% of women. The younger groups are again less demanding, with 53% of 18-24 compared to 64% of over 55s expecting to receive financial compensation. The regional divide is also interesting, with 65% of those living in Southern England expecting compensation, compared to just 55% of Scottish residents.

Which, if any, of the following do you think the company should do for you as a result of a data breach?



Approximately when would you expect the company to FIRST contact you after they learned they had experienced a data breach?



63% would expect to be notified of a breach within hours, with expectations varying dramatically across the age groups – from less than half of young people (49% of 18-24 year olds) increasing with age, up to 74% of over 55s.

61% of GB adults online would be unlikely to purchase goods or services from a UK company that had experienced a data breach, if they were not already a customer. Younger generations and men are more forgiving, with just over half (53%) of 18-34 year olds, and 57% of men unlikely to use a company which has experienced a breach, compared to 72% of over 55s and 64% of women.

Conclusion

Consumers and companies both need to step up

The results of this in-depth study clearly show that there is some way to go for consumers in terms of learning to protect themselves, their identity and financial information – particularly online. It seems that consumers are generally trusting. Young people are being the most relaxed and therefore probably the most at risk, due to the fact that so many will have grown up with the internet, whether at home or school, unlike the older age groups.

The research also gives a clear picture for companies of how consumers expect their data to be handled, and how any data breach should be managed in terms of informing customers. As such, the findings provide a huge incentive for companies of all shapes and sizes to tighten their data protection processes in order to avoid losing significant proportions of customers and prospects due to the loss of reputation which would follow a data breach. It is clear from the research that organisations need robust plans in place to meet these customer expectations.

Protecting personal information is the responsibility of both the consumer and any company acting as custodian of consumer data. One cannot be fully effective without the other playing its part.

Fraudsters are continually evolving their methods, and whilst organisations tracking and stopping them do have high success rates, the financial incentive for fraudsters to invent new techniques means they often stay one step ahead of those out to stop them.

It is vital, therefore, that consumers and businesses do all they can to prevent fraudulent access to personal information, and that their job is not made easy by careless sharing of personal details on social media pages or elsewhere online or over the phone.

As our lives move online more and more, the amount of data available is growing exponentially, and the opportunities for those looking to misuse the information for personal gain grow with it. This of course increases the appeal of online fraud. We are, therefore, likely to see the fraud figures continue to rise over the coming years, unless both companies and individuals take responsibility and put into place the necessary measures to stop fraudsters gaining access to this valuable information.

React swiftly with Equifax Protect

Equifax is ideally placed to help businesses if they experience a data breach. We have one of the largest sources of detailed consumer data in the UK.

Equifax Protect enables businesses to offer their customers and employees a range of tools so that they can react fast and take appropriate action to reduce the risk of fraud.

The benefits of Equifax Protect

DETAILED INFORMATION TO SPOT FRAUDULENT CREDIT ACCOUNTS

We give individuals unlimited access to their Equifax Credit Report & Score, allowing them to take action if they see suspicious activity. Information includes:

- Credit agreements including balances
- Searches for new credit applications
- Linked addresses that may not be their current home

ALERTS TO RESPOND TO NEW THREATS, QUICKLY

We'll notify individuals of changes and new information we find enabling them to take measures against potential fraud:

- Automatic alerts of new credit accounts, credit searches performed and other key changes to their Equifax Credit Report
- Optional monitoring of websites where personal information is known to be exchanged and traded by fraudsters

UNDERSTAND AND TAKE ACTION AGAINST SOCIAL MEDIA RISKS

While social media sites can be a great way to connect with others, they're also an opportunity for identity thieves to gather personal data.

Equifax Social Scan enables individuals to search around 100 social media sites for public information about themselves, understand the fraud risk associated with it and where to take action.

RAPID DEPLOYMENT, COMPREHENSIVE SUPPORT

We know responding fast is essential. Our service can be set up within three business days and includes template communications to help you contact affected customers or employees with the right message.

For end-users we provide support 7 days a week[6] by phone, online help and FAQs, with victims of fraud specialists on hand should the individual need them.

A GLOBAL LEADER IN INFORMATION

Equifax Ltd is part of Equifax Inc., one of the world's leading credit referencing agencies. Founded in 1899 in Atlanta, Georgia, today Equifax Inc. operates globally, with bases or investments in 21 countries.

Businesses throughout the world trust Equifax to help them reduce fraud and manage their credit risk. Equifax manages data on more than 800 million consumers and 88 million businesses worldwide.

Find out more today. Talk to one of our data breach team on 0800 085 4156 or email ukbreach@equifax.com

EQUIFAX®