

Data Breach Response:

Helping organisations to notify, manage enquiries and offer credit monitoring to the people affected.

The below data breach scenario has been created to illustrate how we can help and support businesses. It is based upon a number of live breach incidents to ensure we maintain client confidentiality.

Scenario

A financial services client suffered a Data Breach which, compromised personally identifiable information, affecting 50,000 customers.

Who was affected?

Customers across a broad range of services were affected, including loans, savings and mortgage services. All customers were based in the UK, however not all people were current customers of the client. Customers who had requested a loan/mortgage application were affected meaning the client was not confident that all the address information would be current.

What information was lost?

The information compromised included name, postal address, email, date of birth, telephone number, account sort code and number. The client could not confirm exactly what data had been compromised for each person only that potentially all the personally identifiable information for the affected people may have been taken.

What did the client do next?

The client contacted the Experian Breach Response Team through a Law Firm specialising in Data Privacy and Breach Remediation. The Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA) were notified and they were keen for the people affected to be notified of the data breach as quickly as possible.

Challenge

The client wanted to notify those people affected by letter as they were concerned if they sent an email communication people may believe it was a phishing attack. The client normally communicates with their customers by post, so sending an email may have created fears that the client had changed the way in which they interact with their customers and create concern.

The client was also aware that their contact database was not accurate and data was not in a consistent format. In addition, the client did not have the expertise or resources to send a large, urgent letter communication fulfilment to affected customers and needed help to achieve this.

The client on assessing resources was unable to stand up a large employee pool that would answer any potential incoming calls from customers who required further information and reassurance. Due to the nature of the data breach across their product range they knew they would need at least three different telephone lines as customers knew the company under different brand names.

Finally, the client wanted to offer a credit monitoring service to those people affected to mitigate the risk of identity theft as the client could not be sure the information compromised would not be placed for sale on the "dark web".

Data Breach Response

Solution

Notification letters to individuals detailing the data breach and information compromised

Experian provided a postal notification service, which included three tailored letter templates personalising the message to the different groups of people. This was based upon the services they used and associated loss of personal data.

A Data Cleansing service was provided, finding and updating forwarding addresses for those affected so notification communications would arrive at the customers current address. A mortality check was also conducted and data removed appropriately.

Finally, the list of customers was checked to remove duplicate entries and where customers took several products, the most significant data loss notification details were provided.

The letters were despatched five days after receiving the original proofs, name and address information. A returns postal service was also provided for letters 'returned to sender' so the client could assess and take further appropriate action.

Contact Centre Support to manage enquiries and provide reassurance

Experian provided customer contact centre support on behalf of the client.

The support provided included a pre-agreed frequently asked questions (FAQs) service and was managed across three different telephone lines through a pre-briefed team of call centre experts. The FAQs were tailored to the different products and data breach scenario and the client requested to have call numbers tracked and reported back.

The contact centre operated for a total of three weeks following the letter notification delivery. In addition to the FAQ support, Experian also provided a complaints escalation process in line with the Financial Ombudsman Service (FOS) requirements.

Credit Monitoring Service to help customers keep a check on credit applications

Experian provided the credit monitoring service called ProtectMyID.

This service provided customers with a voucher code for complimentary access to Experian's credit monitoring service for 12 months. The service provided access to the users Experian Credit Report as well as sending alerts to the individual when certain changes to their Credit Report occurred. In addition, product support was also provided through specialist Victim of Fraud case workers at Experian.

Conclusions

- ✓ The data breach remediation for this client was carried out successfully.
- ✓ The letter notification was implemented within the agreed timescales and due to the improved accuracy of contact data there were very low levels of additional remedial work required.
- ✓ The customer call centre received calls from approximately three percent of the affected group. In the main customers were looking for additional information about how the event had occurred and what action was being taken to stop it from happening again in the future.
- ✓ Complaint calls were very low and managed by the client directly within the required timescales.
- ✓ The monitoring service was taken up by approximately 15% of the affected base. This was broadly in line with expectation.

Data Breach Response

About Experian Data Breach Response Services

Know your

[Threats](#) | [Vulnerabilities](#)

Our proven business consultants will work with you to determine the right approach and help you to prepare a tailored consumer data breach response plan.

Prepare your

[Plan](#) | [Resources](#) | [Processes](#) | [Data](#)

Our proven experts will align the right resources tailored to your business scenario and create pre-determined communications which are stored ready for a live incident.

Recover your

[Reputation](#) | [Trust](#)

When a live incident occurs we work with you to finalise and activate the notification fulfilment, call centre support and web/ credit monitoring services to affected individuals.

About Experian IdentityWorks Global

Our global dark web monitoring service enables you to provide a remediation service to your customers/employees following the theft, loss or disclosure of their personally identifiable information (PII). This is an important step in illustrating the importance the organisation places on such an incident and its commitment to taking reassuring action.

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

E: breachresponse@experian.com
www.experian.co.uk/databreach

© Experian 2018.

Experian Ltd is authorised and regulated by the Financial Conduct Authority. Experian Ltd is registered in England and Wales under company registration number 653331.

The word "EXPERIAN" and the graphical device are trade marks of Experian and/or its associated companies and may be registered in the EU, USA and other countries. The graphical device is a registered Community design in the EU.

All rights reserved.