Sample Talking Points – Equifax Data Breach

Use the following talking points to respond to media inquiries and develop other communication materials.

It's important to clarify Equifax is a credit bureau, not a bank.

- Equifax is one of three major credit reporting agencies and handles the data of 820 million consumers and more than 91 million businesses worldwide.

On Sept. 7, Equifax announced that the records of approximately 143 million Americans were breached between May & July of this year.

- Those records contained names, birth dates, addresses, Social Security numbers and some driver's license numbers. At this time, it appears hackers did not gain access to full credit reports.
- In addition to the personal information accessed, 209,000 credit card numbers were obtained.
- Equifax has indicated that debit cards were not exposed – therefore criminals are unlikely to have the ability to withdraw funds from a checking account.
- The biggest risk posed by this breach is the threat of identity theft.

Consumers should visit Equifax's website to determine whether their information was compromised and to enroll in its free credit monitoring program, TrustedID Premier.

- Equifax is offering free credit file monitoring and identity theft protection to all U.S. consumers for one year following the breach.
- You do not need to provide credit card information to enroll.
- Consumers who sign up for the program will not be automatically enrolled or charged at the end of the year.

Internet banking is your friend here. Monitoring your accounts and credit report for unauthorized transactions is critically important.

- When the bank and customer work together, we can better prevent fraud.
- Banks use a combination of safeguards to protect your information, such as employee training, strict privacy policies, rigorous security standards and encryption systems.
- In addition to using Equifax's TrustedID Premier, consumers can check their credit reports from Equifax, Experian and TransUnion – for free – by visiting annualcreditreport.com. Unfamiliar accounts or activity could indicate identity theft.
- If you suspect you are a victim of fraud, you should alert your bank right away.

Be wary of e-mails that come from Equifax.

- Criminals often take advantage of breaches and craft sophisticated phishing e-mails encouraging consumers to provide personal information.

- Due to the high number of victims, Equifax is only notifying the 209,000 consumers whose credit card information may have been affected via postal mail.

In the event of a fraudulent transaction, consumers are protected against losses.

- When a customer reports an unauthorized transaction, the bank will cover the loss and take measures to protect your account.

- The banking industry is committed to continuing its tradition of safeguarding confidential financial information.

Equifax has agreed to waive all credit freeze fees for the next 30 days for people who want to freeze their Equifax credit files.

- It's important that consumers understand the pros and cons to credit freezes and consider their personal situation.

- Renting an apartment, getting quick credit in an emergency, taking advantage of a one-time offer, or even getting a cell phone, all require quick access to your credit report which is restricted during a freeze.

- Fraud alerts are an alternative for people who are concerned about identity theft. It gives consumers added protection without limiting access to credit.

- A fraud alert puts a red flag on your credit report which requires businesses to take additional steps, such as contacting you by phone before opening a new account.

To understand your rights as a consumer if your personal information was compromised in the breach, visit equifaxsecurity2017.com.