



STATE OF NEW YORK  
OFFICE OF THE ATTORNEY GENERAL

ERIC T. SCHNEIDERMAN  
ATTORNEY GENERAL

DIVISION OF ECONOMIC JUSTICE  
BUREAU OF INTERNET & TECHNOLOGY

**BY EXPRESS MAIL**

September 14, 2017

Brian J. Cassin  
CEO, Experian plc  
Newenham House  
Northern Cross  
Malahide Road  
Dublin 17, Ireland

Craig Boundy  
CEO, Experian North America  
475 Anton Boulevard  
Costa Mesa, CA 92626

**Re: Data Security for Private Consumer Data at Credit Reporting Agencies**

Dear Messrs. Cassin and Boundy:

The unprecedented data breach experienced by Equifax Inc. that affected 143 million Americans – including more than 8 million New Yorkers – has raised serious concerns about the security of private consumer information held by the largest consumer credit reporting agencies. The breach is also imposing costs on consumers who wish to protect themselves and their access to credit from criminals who would misuse the breached data. We write to inquire about steps Experian is taking in light of the Equifax breach, both to ensure that sensitive consumer information in Experian's possession remains safe and to assist consumers who wish to implement additional protections through Experian.

As the chief law enforcement officer for New York State, Attorney General Eric T. Schneiderman enforces laws that protect consumer privacy, guard against fraud and deceptive practices, and require businesses to inform their New York customers, and our office, about breaches of sensitive consumer data. Our office has been granted broad authority to protect these consumer interests from privacy invasions, identity theft, financial loss, and other economic harms, but also from unauthorized disclosure or unfair use of more intimate details that could cause consumers public embarrassment, harassment, or discrimination. Our office has – both

independently and in coordination with other State AGs' offices – used such legal authority to protect consumer privacy in the internet age.

We opened an investigation immediately after learning of the Equifax breach, to learn what happened and who is responsible. We also put out a consumer alert to New Yorkers, advising them of take steps they could take to protect themselves, including by placing a credit freeze on their files. And our office is responding to a barrage of questions and complaints from New York consumers who reasonably fear further harm.

With that work underway, we now turn to ensuring that consumer data at other major credit reporting agencies is safe from attack and provide further assistance to consumers. Accordingly, we ask that Experian address the following questions:

1. What security measures did Experian have in place to ensure the safety of private consumer information before it learned of the Equifax breach, including but not limited to administrative safeguards, technical safeguards, and physical safeguards, as well any best practices or certifications of compliance with any data security regulations or leading standards?
2. What steps has Experian taken since learning of the Equifax breach to ensure that Experian has not already suffered any similar intrusions?
3. What steps has Experian taken since learning of the Equifax breach to ensure that it does not experience breaches going forward? Please address steps to prevent both malicious hacking as well as breaches caused by employee negligence.
4. What steps has Experian taken since learning of the Equifax breach to help consumers implement additional protections for their private data in Experian's possession?
5. Will Experian consider waiving any fees it currently charges for New York consumers who wish to implement and manage a credit freeze for their files through Experian?

We ask that you provide the requested information on or before September 21, 2017, and that an Experian executive who is knowledgeable about the requested information meet with us at our offices in New York City on or before September 28, 2017. Should you have any questions, please feel free to contact me at (212) 416-8196 or via email at [kathleen.mcgee@ag.ny.gov](mailto:kathleen.mcgee@ag.ny.gov). We appreciate your prompt attention to this matter.

Sincerely,

A handwritten signature in blue ink, consisting of a stylized initial 'K' followed by a long horizontal line.

Kathleen McGee  
Bureau Chief  
Bureau of Internet and Technology



STATE OF NEW YORK  
OFFICE OF THE ATTORNEY GENERAL

ERIC T. SCHNEIDERMAN  
ATTORNEY GENERAL

DIVISION OF ECONOMIC JUSTICE  
BUREAU OF INTERNET & TECHNOLOGY

**BY EXPRESS MAIL**

September 14, 2017

James M. Peck  
President & Chief Executive Officer  
TransUnion  
555 West Adams Street  
Chicago, Illinois 60661

**Re: Data Security for Private Consumer Data at Credit Reporting Agencies**

Dear Mr. Peck:

The unprecedented data breach experienced by Equifax Inc. that affected 143 million Americans – including more than 8 million New Yorkers – has raised serious concerns about the security of private consumer information held by the nation’s largest consumer credit reporting agencies. The breach is also imposing costs on consumers who wish to protect themselves and their access to credit from criminals who would misuse the breached data. We write to inquire about steps TransUnion is taking in light of the Equifax breach, both to ensure that sensitive consumer information in TransUnion’s possession remains safe and to assist consumers who wish to implement additional protections through TransUnion.

As the chief law enforcement officer for New York State, Attorney General Eric T. Schneiderman enforces laws that protect consumer privacy, guard against fraud and deceptive practices, and require businesses to inform their New York customers, and our office, about breaches of sensitive consumer data. Our office has been granted broad authority to protect these consumer interests from privacy invasions, identity theft, financial loss, and other economic harms, but also from unauthorized disclosure or unfair use of more intimate details that could cause consumers public embarrassment, harassment, or discrimination. Our office has – both independently and in coordination with other State AGs’ offices – used such legal authority to protect consumer privacy in the internet age.

We opened an investigation immediately after learning of the Equifax breach, to learn what happened and who is responsible. We also put out a consumer alert to New Yorkers, advising them of take steps they could take to protect themselves, including by placing a credit

freeze on their files. And our office is responding to a barrage of questions and complaints from New York consumers who reasonably fear further harm.

With that work underway, we now turn to ensuring that consumer data at other major credit reporting agencies is safe from attack and provide further assistance to consumers. Accordingly, we ask that TransUnion address the following questions:

1. What security measures did TransUnion have in place to ensure the safety of private consumer information before it learned of the Equifax breach, including but not limited to administrative safeguards, technical safeguards, and physical safeguards, as well any best practices or certifications of compliance with any data security regulations or leading standards?
2. What steps has TransUnion taken since learning of the Equifax breach to ensure that TransUnion has not already suffered any similar intrusions?
3. What steps has TransUnion taken since learning of the Equifax breach to ensure that it does not experience breaches going forward? Please address steps to prevent both malicious hacking as well as breaches caused by employee negligence.
4. What steps has TransUnion taken since learning of the Equifax breach to help consumers implement additional protections for their private data in TransUnion's possession?
5. Will TransUnion consider waiving any fees it currently charges for New York consumers who wish to implement and manage a credit freeze for their files through TransUnion?

We ask that you provide the requested information on or before September 21, 2017, and that a TransUnion executive who is knowledgeable about the requested information meet with us at our offices in New York City on or before September 28, 2017. Should you have any questions, please feel free to contact me at (212) 416-8196 or via email at [kathleen.mcgee@ag.ny.gov](mailto:kathleen.mcgee@ag.ny.gov). We appreciate your prompt attention to this matter.

Sincerely,

A handwritten signature in blue ink, consisting of a stylized initial 'K' followed by a long horizontal line.

Kathleen McGee  
Bureau Chief  
Bureau of Internet and Technology