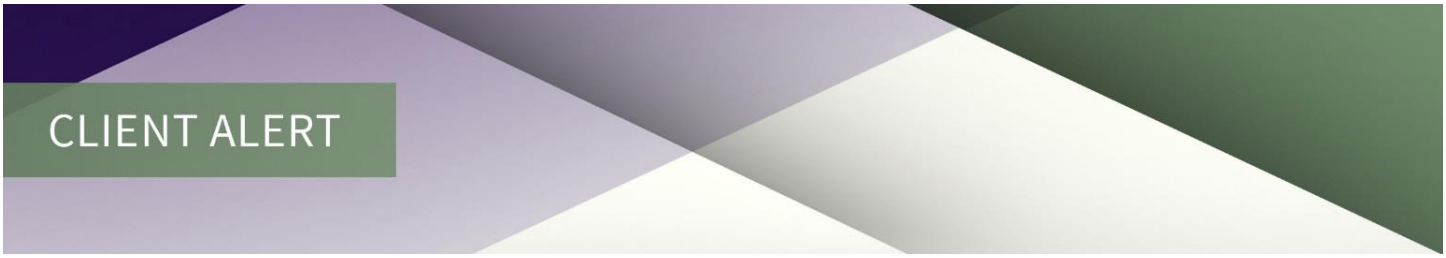

Federal Trade Commission Releases Staff Perspective on Informational Injuries Arising from Privacy and Data Security Incidents

October 24, 2018

AUTHORS

Elizabeth J. Bower | James C. Dugan | Daniel K. Alvarez | Philip F. DiSanto
Alex J. Moyer | Jill Guidera Brown

Introduction

On October 19, 2018, the Federal Trade Commission ("FTC") released a staff perspective (the "Staff Perspective") on "informational injuries" arising out of unauthorized access to or use of personal, medical, or financial information exposed by a security incident. The Staff Perspective is based on a December 2017 FTC workshop concerning informational injuries and discusses, among other things, specific types of informational injuries that consumers may suffer, and factors that governments should consider before intervening to address such injuries. The Staff Perspective is not binding and does not specify when the FTC will intervene to address informational injuries, but provides important insight into the FTC's continued focus on privacy and data security matters.

FTC's Remedial Authority for Privacy and Data Security Matters

The FTC, alongside and often in partnership with state attorneys general, has been increasingly active in shaping the privacy and data security enforcement landscape. The Staff Perspective should therefore be read in the context of the FTC's other recent pronouncements on its privacy and data security agenda. In August 2018, for example, the FTC published a notice in the Federal Register seeking public comment on potentially expanding the FTC's remedial authority

to deter unfair and deceptive conduct in privacy and data security matters, the potential consumer welfare implications of new technologies (*e.g.*, artificial intelligence), and the intersection of privacy, big data, and competition.

The scope of the FTC's authority in connection with privacy and data security matters is in flux following the Eleventh Circuit's recent decision in *LabMD v. FTC*, which questioned the FTC's authority to declare a cybersecurity practice to be "unfair" based solely on the likelihood of "substantial consumer injury." The Staff Perspective appears mindful of the potential for regulatory overreach by observing that while entities should be held responsible for their conduct, characterizing any "risk of injury" as an "injury" could render "literally everything" actionable.

FTC Staff Perspective's Guidance on Informational Injuries

The Staff Perspective sets forth three questions that governments should ask before deciding to intervene in a privacy and data security matter to address informational injuries.

1. **How sensitive is the data at issue?** If the data compromised or misused is highly sensitive personal information (*e.g.*, medical or financial information), more protection may be necessary and the likelihood of actual harm may increase.

2. **How will the information be used?** If the information compromised or misused was collected for an expected internal purpose, then the government's interest in intervention may decrease. By contrast, if information is used in a way not reasonably anticipated by the consumer (or, perhaps, if unexpected information is collected), then the government's interest in intervention may increase.

3. **Is the information anonymized or identifiable?** The FTC recognizes that the government may want to encourage certain analyses or data-sharing practices that involve anonymized information. For example, where anonymized data is shared for medical research, the government may have a more limited interest in intervention.

In addition to discussing general factors that governments should weigh in deciding whether to initiate an enforcement action or take other remedial measures, the Staff Perspective identifies and discusses several categories of "informational injuries" that are increasingly common and concerning:

- **Medical Identity Theft**: Theft of personal medical information may result in both financial and serious health and safety consequences for the consumer whose information was compromised.

- **Doxing**: "Doxing" is the distribution of private information about an individual without consent, often with the intent of harassing or injuring the individual. Anyone can become a victim of doxing, though the practice was traditionally targeted at public figures and individuals in the gaming or online hacker communities. While doxing

may involve financial consequences and risk of identity theft, it also frequently results in other injuries, such as reputational harm and threats of violence.

- **Disclosure of Personal Information**: Disclosure or misuse of particularly sensitive personal information, such as information about medical conditions or sexual orientation, may also result in consumer injuries distinct from the financial consequences of personal information being disclosed or misused.

- **Erosion of Trust**: Privacy and data security incidents may also erode consumer trust in the businesses or institutions that are responsible for protecting personal information, resulting in unintended negative effects on businesses and competition.

Preventing and Mitigating Informational Injuries

As the FTC circles in on its approach to addressing informational injuries, companies can take proactive steps to prevent potential harms to consumers while bolstering their users' trust in the way they collect, use, and share consumer data. Willkie's Cybersecurity & Privacy Practice Group is available to help navigate the legal, business, and technical considerations of developing and maintaining robust privacy and data security controls.

If you have any questions regarding this client alert, please contact the following attorneys or the attorney with whom you regularly work.

Elizabeth J. Bower
202 303 1252
ebower@willkie.com

James C. Dugan
212 728 8654
jdugan@willkie.com

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Philip F. DiSanto
212 728 8534
pdisanto@willkie.com

Alex J. Moyer
202 303 1280
amoyer@willkie.com

Jill Guidera Brown
202 303 1217
jgbrown@willkie.com