BRACEWELL
&GIULIANI

Texas
New York
Washington, DC
Connecticut
Seattle
Dubai
London

Glen A. Kopp
Partner

+1.212.508.6123 Office
+1.800.404.3970 Fax

glen.koppbgllp.com

Bracewell & Giuliani LLP
1251 Avenue of the Americas
New York, New York
10020

MEMORANDUM

TO:	Environmental Working Group
FROM:	Glen A. Kopp
DATE:	September 16, 2015
RE:	FACT Act and Privacy Risk

On January 26, 2015, Representative Blake Farenthold (R-Tex) introduced H.R. 526, the Furthering Asbestos Claim Transparency (FACT) Act.[1] The stated intent of the FACT Act is to prevent false claims being made against asbestos trusts. According to its sponsor:

> When attorneys and their clients bring false or exaggerated claims to trusts, they take assets from deserving victims. The FACT Act will discourage this kind of abuse by shining light on the trust system, as sunlight is often the best disinfectant. Our bill strikes the right balance between transparency and privacy—and I am proud to have the Committee's support on something that is going to help victims of asbestos exposure get the financial support they need and deserve.[2]

Notwithstanding Representative Farenthold's statement, however, the FACT Act presents significant privacy concerns as it is currently drafted.[3]

Background

The text of H.R. 526 (2015) is identical to that of the previously introduced H.R. 982 (2013). A detailed description of the background behind the harmful effects of asbestos exposure as well as the form and function of the asbestos bankruptcy trusts are contained within the "dissenting views" that were filed at the time that H.R. 982 was considered.[4] Like H.R. 982,

---

1 H.R. 526, Furthering Asbestos Claim Transparency (FACT) Act of 2015, 114th Congress (2015-2016).

2 Farenthold Press Release, "House Judiciary Committee Approves Rep. Farenthold's Fact Act," (May 21, 2013).

3 On February 4, 2015, Senator Jeff Flake (R-AZ) introduced a parallel Senate bill, S. 357. The two bills are practically identical, so the below analysis applies equally to both.

4 Dissenting Views, H.R. 982 (2013).

H.R. 526 amends 11 U.S.C. § 524(g) to require asbestos trusts to file reports no more than 60 days after each quarter's end describing each demand that the trust received from any claimant and the claimant's name and exposure history.[5] The only privacy-related limitations on this report are that the trust must "not include any confidential medical record or the claimant's full social security number."[6] The trust must also provide to any party, upon written request and payment, information related to payments and demands for payments from the trust.[7]

Privacy risks

According to the Federal Trade Commission, identity theft has been "the FTC's top consumer complaint for the last 14 years."[8] The Bureau of Justice Statistics estimates that 16.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2012, resulting in $24.7 billion in direct or indirect losses.[9] Identity theft largely results from the compromise of personal identification information, which identity thieves can use for any number of illegal purposes, including bank fraud, credit card fraud, and health care fraud.

Based on the sparse limitations contained in H.R. 526, information for each claimant that may be made publicly available could include the following: name; address; phone number; email address; date and/or year of birth; last four digits of a social security number; employer; asbestos exposure history[10]; and claim amount.

Several of these pieces of information – namely those related to names, date and/or year of birth, and social security numbers, constitute forms of sensitive personal identification upon which a federal prosecution for identity theft and/or misuse may be predicated.[11] On the other

---

5 H.R. 526, Furthering Asbestos Claim Transparency (FACT) Act of 2015, 114th Congress (2015-2016), 2:4-2:14.

6 *Id.* at 2:15-2:17.

7 *Id.* at 2:18-2:26.

8 Prepared Statement of Edith Ramirez, Senate Commerce Committee (Mar. 26, 2014).

9 Bureau of Justice Statistics, Victims of Identity Theft, 2012 (Dec. 2013).

10 While "confidential medical records" themselves are excluded, it does not appear that information that would otherwise be contained in a confidential medical record is similarly protected. As such, exposure history may include previous employers and places of employment.

11 18 U.S.C. § 1028(d)(7) ("the term 'means of identification' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual ….").

hand, all of this information is that which federal, state, and private entities recommend be kept away from any form of public disclosure. For example:

- From the Federal Trade Commission: "Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites."[12]

- From Fairport Savings Bank: "Find out who has access to your personal information and verify that it is handled securely."

- From UC Berkeley School of Law: "Reduce the amount of personal information that is 'out there.' … Have your name and address removed from the phone book and reverse directories."

- From Industrial Federal Credit Union: "Protect your Social Security Number. … Knowing your full name, address and full Social Security Number, or even the last 4 digits, can let a thief assume your identity."

- From Identity Theft Resource Center: "Don't give out Personal Identifying Information (PII) unless absolutely necessary."

- From the U.S. Department of Justice: "Be stingy about giving out your personal information to others unless you have a reason to trust them, regardless of where you are. … Start by adopting a 'need to know' approach to your personal data."

- From the Federal Bureau of Investigation: "But for [identity theft] to happen, the crook first needs to know your personal information. Your name, home address, and birth date provide a good start."

Maintaining the confidentiality of this kind of information is particularly important given its typical use by identity thieves. For example, phishing scams – or schemes in which criminals impersonate a legitimate business or person in order to trick a victim into giving away personal information – are often predicated on exploiting an existing relationship between the victim and the business. Current or previous employment information can provide a criminal with the lure he or she needs for such an attack. An address, email address, and/or phone number are the means to execute the attack.[13] Phone numbers are also, on occasion, used by

---

[12] The FTC also adds that "[b]efore you share information at your workplace, a business, your child's school, or a doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing."

[13] According to Experian, the credit reporting agency, phishing occurs "when a scammer sends an e-mail that appears to come from your bank or another legitimate

businesses to identify their customers or employees. In the hands of an enterprising criminal, such phone numbers can be "spoofed." Similarly, criminals can exploit email addresses which often serve as usernames for many sites, including Facebook and PayPal.

Criminals may also use low-tech methods to steal personal identification information. According to the state of New Jersey, with a physical address, thieves can "retrieve credit card receipts, bank statements, and bills from your … garbage," and can "steal from your mailbox and even complete change of address forms to divert your mail to another location." Unsolicited credit card offers are also a fertile source for identity thieves.

Bankruptcy limitations on the availability of some of this information – such as the restriction on disclosure to a birth year instead of a full birthdate – do not serve as sufficient protection against identity theft. Because identity thieves are adept at amalgamating information across platforms to construct victim profiles, even the year of birth can serve as the basis for social engineering. For example, individuals on Facebook often disclose their birthdays absent the year so as not to disclose their age, or to receive birthday wishes from friends even in the absence of a specific date listed on the site. With the year in hand and a Facebook profile, an identify thief can easily acquire the rest of the birthdate information.

Names, dates and/or years of birth, and social security numbers are usually used to verify identities for almost any kind of a business or institution. Even limiting disclosure to the last four digits of the Social Security number provides scant comfort: in 2009, Alessandro Acquisti and Ralph Gross of Carnegie Mellon University reported they had created a computer algorithm to successfully predict the first five digits of a person's Social Security number 44 percent of the time for people born after 1989. All they needed to know was when and where the person was born. IDT911, an identity protection service, also recommends against disclosure of the last four digits of a Social Security number, pointing out that "[m]any businesses have started using the last four digits of your SSN for remote identification purposes for access to online banking and telephone banking."

Finally, listing the amount of a claim in conjunction with the claimant's personal information can help a criminal prioritize targets. In other words, the higher the claim, the more appealing the target.

While each piece of information described above may separately lead to identity theft, there is a real danger to its collective use. As the Federal Trade Commission points out, "[i]f you post too much information about yourself, an identity thief can find information about your

---

company, asking you for personal information, such as your credit card or Social Security number. Phishing scams may also be conducted by telephone, with an unknown caller claiming to represent your bank or credit card issuer."

life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information." The same is equally true in situations where someone else – here, a trust – is posting that information for you.

Thus, even a proposed "fix" that purports to protect Social Security numbers in their entirety does not sufficiently address the underlying risk. It simply does not prevent the many forms of phishing attacks that are predicated on personal identification information other than possession of all or parts of a social security number.[14] Moreover, unless the collection of Social Security numbers is prohibited in its entirety, the FACT Act still requires disclosure of the last four digits of Social Security numbers to multiple parties and a wide variety of individuals with no restriction on use, disclosure, dissemination, or transmission, and without encryption.

Other privacy-related considerations

When participating in a hearing concerning the NSA's bulk collection of data, H.R. 526's sponsor, Farenthold, argued that privacy concerns outweighed security concerns related to terrorism, asking, "How is having every phone call that I make to my wife, to my daughter relevant to any terror investigation? So do I have a reasonable expectation of privacy in any information that I share with any company? My Google searches, the email I send … do I have a reasonable expectation of privacy in anything but maybe a letter I hand deliver to my wife?"

Rep. Farenthold's concerns about the bulk collection of "innocent" information that led him to oppose significant portions of NSA's surveillance authority appear to be equally on point with respect to H.R. 526's broad collection of personal information related to asbestos claims. In effect, H.R. 526 also authorizes the bulk collection of personal identification information from a wide range of individuals so that limited instances of fraudulent activity can be identified. However, fraud prevention can occur through a number of less intrusive and significantly more private means, with a vastly reduced risk of the misuse of personal identification information by identity thieves or the inadvertent disclosure of such information by others.

[14] For example, in February 2015, the Social Security Administration warned of phishing attacks designed to acquire social security numbers.