

SCHWARTZ & BALLEN LLP
1990 M STREET, N.W. • SUITE 500
WASHINGTON, DC 20036-3465
(202) 776-0700

FACSIMILE
(202) 776-0720

www.schwartzandballen.com

MEMORANDUM

April 22, 2005

To Our Clients and Friends

Re: Schumer-Nelson Identity Theft Prevention Bill

Senators Schumer and Nelson have introduced S. 768, the Comprehensive Identity Theft Prevention Act (the "Act"), which establishes the Office of Identity Theft (the "Office") within the Federal Trade Commission ("FTC"). The Act provides the FTC with broad authority to prevent identity theft and establish limitations on businesses that collect, maintain, sell or transfer sensitive personal information of individuals.

SCOPE OF COVERAGE

The FTC will have civil jurisdiction over all commercial organizations that collect, maintain, sell or transfer sensitive personal information. Sensitive personal information includes an individual's:

- Social security number
- Driver's license number or state identification number
- Bank or investment account number
- Credit or debit card number
- Certain medical information
- Payment history
- Other information specified by the FTC

The FTC is to promulgate regulations to enable the Office to protect consumers' sensitive personal information that is collected, maintained, sold or transferred by commercial organizations. The Act requires the Office to undertake

SCHWARTZ & BALLEN LLP

certain actions to assist consumers who are victims of identity theft to re-establish their stolen identities. These actions include:

- Establishing customer-service teams to assist consumers retrieve their sensitive personal information
- Issuing certifications to individuals who are victims of identity theft which can be used in lieu of a police report in order to access records
- Promulgating regulations that enable the Office to help consumers restore their stolen sensitive personal information quickly and inexpensively.

The Act requires the FTC to adopt rules governing the sale, maintenance, collection or transfer of sensitive personal information by commercial entities. The rules must include a requirement that entities take reasonable steps to prevent unauthorized access to sensitive personal information.

In addition, a company that maintains sensitive personal information is required to provide prompt notice to an individual and to the FTC if unencrypted sensitive personal information which was maintained by the company was obtained by an unauthorized person. A company may delay providing notice if a law enforcement authority determines that notification would impede a criminal investigation. An individual who has received such a notice may request the company to delete that person's sensitive personal information from the company's records.

A person that requests sensitive personal information from a customer intending to sell or transfer the information for value at any time is required to inform the customer that the information may be sold without the customer's additional consent. The disclosure is to appear in a clear and conspicuous box in at least 12-point type directly above the signature block on a written document or directly above the submission button on an online form.

DATA MERCHANTS

The FTC is given authority to regulate data merchants. The term "data merchant" is defined broadly as a person that engages in collecting, assembling or selling sensitive personal information in a significant manner or as a significant part of the organization's operations. As a result, many companies that share information with others may be regarded as data merchants.

The FTC's rules must require data merchants to register with the FTC. Data merchants will be required to authenticate third parties who have access to the data merchant's database and to track who has accessed what records containing sensitive

SCHWARTZ & BALLEN LLP

personal information and for what purpose. Consumers will have the ability to request a report from data merchants holding the consumer's sensitive personal information which includes what information is maintained, to whom the information was provided and the purpose of the disclosure.

Data merchants would also be required to provide a "Disclosure Box" which would alert individuals that their sensitive personal information could be sold or provided to unaffiliated parties without their additional consent.

SOCIAL SECURITY NUMBERS

The Act provides that a person may not request an individual's social security number unless it is necessary for the normal course of business and no other identifying number can be used. It also prohibits the sale, purchase or display of social security numbers to the general public.

PENALTIES AND ENFORCEMENT

The Act provides for civil penalties of up to \$1,000 per violation, depending upon the nature of the violation. The FTC and state attorneys general are authorized to enforce the Act.

A copy of the S. 768 can be found at http://www.schwartzandballen.com/whats_new.html.

If you have any questions, please call Gilbert Schwartz, Robert Ballen or Tom Fox at (202) 776-0700.