

# SHERRARD GERMAN & KELLY, P.C.

ATTORNEYS AT LAW



Report from Counsel - Insights and Developments in the Law

## Pennsylvania Adopts New Breach of Personal Information Notification Act

By: Edward G. Rice, Esquire and Kevin P. Dolan, Esquire

As businesses increasingly move into the electronic age for conducting their affairs, there is a corresponding increase in consumer and regulatory attention focused on concerns about the security of personal information maintained on computers. Concerns about "identity theft" are only amplified with every report of large-scale theft or loss of personal information, which seems to occur on a near daily basis. Federal legislation has been expected to deal with data security breaches for some time. Except for the financial services industry, however, no national laws have been forthcoming. Instead, regulatory activity has occurred on the state level - more than twenty states have passed their own legislation to deal with information security breaches and the consequences of such breaches.

Pennsylvania has now joined the fray. On June 20, 2006, the "Breach of Personal Information Notification Act" (73 P.S. § 2301 *et seq.*) ("the Act") became effective, establishing standards for assessing and disclosing security breaches to Pennsylvania residents whose personal information was or may have been disclosed due to a breach of security.

**Scope of the Act.** Generally, the Act establishes a new notification requirement in the event of a breach of the systems which house personal information on individuals. The Act applies to any entity

that maintains such personal information as part of a database of multiple individuals. Coverage is broad under the Act, and includes individuals, businesses, governmental agencies and political subdivisions. It also expressly includes financial institutions (and their parents and subsidiaries) organized, chartered or holding a license or authorization certificate under the laws of Pennsylvania or any other state or nation. The Act does not apply to breaches that took place before June 20, 2006 (the effective date of the Act).

**Applicability: Assessing the Need to Disclose.** As an entity determines whether a breach has occurred such that the Act's disclosure requirements are triggered, the definitions of "personal information" and "breach of the security of the system" are of fundamental importance. "Personal information" protected under the Act means a person's first name (or initial) and last name, in combination with any of the following other data elements (which are not encrypted or redacted): (1) a social security number; (2) a driver's license number or other state-issued identification number; and (3) a financial account number or a credit or debit card number, combined with any required security code, access code or password that would permit access to an individual's financial account. The terms "encrypted" and "redacted" are important in this analysis. "Encryption"

Peter Y.  
Herchenroether

### Congratulations

Peter Y. Herchenroether has been elected to a four year term on the Board of Trustees of Westminster College in New Wilmington, PA. A shareholder of the firm, Mr. Herchenroether received his BA in History, summa cum laude, from Westminster College in 1976 and received his JD from Vanderbilt University School of Law in 1979. He is currently serving as a member of the Probate and Trust Law Section Council of the Allegheny County Bar Association. His practice focuses on personal estate planning and estate administration and he serves as counsel to several non-profit charitable organizations.

Susan J.  
Messer

### Announcement

Susan J. Messer was elected to the Board of Directors of Variety Children's Charity of Pittsburgh Young Professional's Board. Mrs. Messer is a shareholder of the firm and received her BA from Duquesne University in 1989 and her JD from the University of Pittsburgh, School of Law in 1992. Mrs. Messer is a member of the firm's Corporate and Financial Services Groups.



## Pennsylvania Adopts New Breach of Personal Information Notification Act ... *continued*

is the transformation of data into a form where there is “a low probability of assigning meaning” without using a confidential process or key. “Redact” means truncation of an identification number or account number such that only the last four digits are accessible as part of the data (as, for example, on an ATM receipt). Thus, when determining its obligations, an entity must first consider the nature of the data in question - encrypted or redacted information is not considered “personal information” under the Act, except where encrypted information is accessed in unencrypted form.

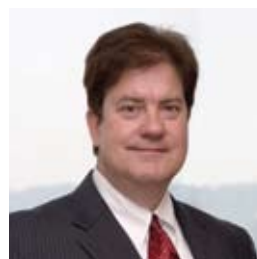
If an entity determines that the data at issue is “personal information,” it must then determine if there has been a breach. Under the Act, a breach has occurred when “unauthorized access and acquisition of computerized data ... materially compromises the security or confidentiality of personal information maintained by the entity ... and ... causes or the entity reasonably believed has caused or will cause loss or injury to any resident of [Pennsylvania].” The phrases “material compromise” and “reasonable belief” are not defined by the Act, so the entity must make its own judgment as to whether those standards have been met. The Act excludes publicly available information from the definition of “personal information.” Additionally, “breach” does not in-

clude a good faith acquisition of personal information by an employee of the entity for the entity’s purposes, so long as the personal information is used only for the entity’s lawful purposes and the information is not subject to further unauthorized disclosure.

**Notice Procedures.** Once it is determined that a breach of personal information has occurred, the entity must notify “any resident of [Pennsylvania] whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.” Notice may be provided by written notice, telephone notice, or e-mail notice where a prior business relationship exists and the entity has a valid e-mail address for the individual to be noticed. Telephone notice can only be utilized where the individual is “reasonably expected” to receive the notice. Such notice must be given “in a clear and conspicuous manner,” describing the breach in general terms. Additionally, the telephone notice must verify personal information without requiring the individual to provide personal information, and the notice must provide the customer with a telephone number to call or website to visit for further information or assistance.

In addition to written, telephone or e-mail notice, the Act also permits “substitute notice” if the entity can demonstrate

one of three things: (1) the cost of providing notice would exceed \$100,000; (2) more than 175,000 affected persons must be notified; or (3) the entity “does not have sufficient contact information.” Substitute notice must consist of all of the following: (1) e-mail notice, where the entity has e-mail addresses for the subject persons; (2) conspicuous posting of the notice on the



Edward G.  
Rice

### Identity Theft Security

Ed Rice, shareholder of Sherrard, German & Kelly, P.C., participated as a panelist in an identity theft and information security discussion at the November 6, 2006 Financial Industries Network (FIN) event held at the Duquesne Club, Pittsburgh, Pennsylvania.

The topic presented was “Identity Theft and Corporate Fraud: Recent Schemes, Solutions and Regulatory Developments.” Over 90 people attended this function to hear Mr. Rice and three other panelists from the financial services industry discuss this timely and important topic.



entity's website, if it has one; (3) notification to "major Statewide media."

The Act's notification requirements for third-party vendors who maintain, store or manage data on behalf of another entity are a bit different. Under the Act, when the vendor discovers a breach of the security system, it must notify the entity on whose behalf it maintains the information. The vendor's notification responsibilities end there, and having been so notified, it is then up to the entity to make the necessary determinations and notifications under the Act.

When an entity provides notice to more than 1,000 persons at a time, the entity must also notify, "without unreasonable delay," all of the nationwide consumer reporting agencies of the timing, distribution, and number of notices.

**Time Frames.** One of the handicaps of the Act is the absence of definitions of certain key terms (for example, "material compromise"). This is perhaps most problematic with respect to the time frames set by the Act for notice. The Act provides next to no guidance on the time period in which an entity must make the required notices, stating only that subject to the entity's need to determine the scope of the breach and restore the integrity of the data system, notice shall be made "without unreasonable delay." The Act does provide for an allowable delay if a law enforcement agency determines, and advises the entity in writing, that the notification would impede a criminal or civil investigation. Once the agency determines that the notification will not jeopardize the investigation (or national or homeland se-

curity), the notification may proceed. This provision of the Act seems incomplete in that the Act does not require an entity to notify law enforcement of a security breach; perhaps the Legislature presumed that the prudent businessperson will have taken this step as a matter of course, given the strong likelihood that a breach will have identity-theft implications. In any case, to be in a position to comply with this requirement, among other reasons, an entity should promptly consult with counsel to analyze whether it should alert local, state and federal authorities to the breach.

**Notice Exemptions; Financial Institutions.** An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information will be deemed to be in compliance with the requirements of the Act if its procedures are consistent with the Act and it notifies affected persons in accordance with those policies.

Financial institutions will be deemed to be in compliance with the Act if they comply with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Safe harbor is also provided for an entity that complies with the notification guidelines proscribed by its primary or functional Federal regulator. For the notice requirements under these federal laws, as well as a comprehensive discussion of the other data security requirements for financial institutions, refer to the Sherrard, German & Kelly article "The War on Identity Theft," by Ed

Rice, published in the Summer 2005 issue of the firm's Report From Counsel, available on the firm website at [www.sgkpc.com](http://www.sgkpc.com).

**Penalties.** Any violation of the Act's disclosure provisions will be deemed an "unfair or deceptive act or practice" in violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law (UTPCPL). There is no private right of action for an individual under the Act;



Cynthia M.  
Morrison

## Welcome

The firm is pleased to announce that Cynthia M. Morrison has joined the firm as an associate in the firm's Litigation Services Group. Ms. Morrison's practice is focused on general civil litigation matters. Prior to joining the firm, Ms. Morrison was an associate in the litigation department of a Pittsburgh-based international law firm and served as a judicial clerk to the Honorable Elizabeth V. Hallanan of the United States District Court for the Southern District of West Virginia. Ms. Morrison received her law degree from the Ohio Northern University Pettit College of Law in 1999, where she served on the executive editorial board of the Ohio Northern University Law Review. She received her BA from the College of Wooster in 1993.

**Counseling businesses and individuals in the following areas:**

**Business Services:**

- Business formation and structure
- Mergers, Acquisitions, Reorganizations, Sales and Consolidations
- Commercial real estate transactions
- Financial Transactions
- Contract preparation
- Labor and employment matters
- Employee benefits
- Tax planning and counseling
- Intellectual Property protection, licensing and technology transfer

**Bank Services**

- Retail financial services
- Commercial, industrial and real estate lending
- Commercial credit recovery
- Consumer collection

**Individual Services**

- Residential real estate transactions
- Tax issues
- Estate planning
- Drafting of wills and trust agreements
- Probate and estate and trust administration
- Estate tax issues

**Litigation Services**

- Commercial Litigation
- Bankruptcy
- Contract disputes
- Personal injury
- Employment disputes
- Estate and trust litigation services

## Pennsylvania Adopts New Breach of Personal Information Notification Act ... *continued*

Attorney General is given sole authority to bring a UTPCPL action. The Act makes no distinction between levels of violation (e.g., negligent, willful, intentional); therefore, even a negligent violation of the Act may prompt the Attorney General to seek relief under the UTPCPL. However, a civil penalty will only be imposed for “willful” violations of the UTPCPL.

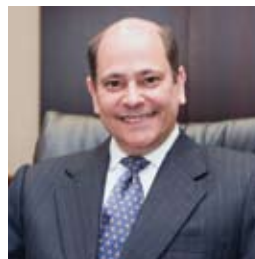
**Concluding thoughts.** As noted above, we expect federal legislation at some point in the future. When and if that legislation is passed, we hope that it will preempt state and local notification laws (as this Act preempts any applicable local laws in Pennsylvania) in order to avoid the patchwork of overlapping requirements. Until such legislation is passed, however,

entities doing business on a national (or even multi-state) level must contend with the legal mosaic of more than 20 separate state laws dealing with notification of security breaches. To the extent that an entity is not already operating under notifications prescribed by federal guidance or the regulations of an agency, Pennsylvania provides one more set of laws that must be considered in conjunction with a business’ information security processes.

• *SGK*

---

For questions regarding this article, or for additional information on privacy and information security laws, please contact: Edward G. Rice, 412-355-0200  
egr@sgkpc.com



Gary Philip  
Nelson

### Super Lawyer: Gary Philip Nelson

Gary Philip Nelson was selected as a Pennsylvania 2006 Super Lawyer. Mr. Nelson is a shareholder of the firm and his practice includes loan transactions, restructurings, litigation, and bankruptcy. Mr. Nelson is admitted to the Supreme Courts of Pennsylvania and the United States, the Third and Fourth Circuits Courts of Appeal, and the Federal Courts in the Western District of Pennsylvania, and has appeared in Bankruptcy Courts throughout the country. Mr. Nelson is a senior hearing committee member appointed by the Disciplinary Board of the Supreme Court of Pennsylvania.