



TABLE OF CONTENTS

BUSINESS LAW 1

Federal Law Requires Businesses to Properly Dispose of Sensitive Consumer Information..... 1

Business Friendly Changes to Bankruptcy Law..... 2

TECH FRONTIER 3

Businesses must Assist Pennsylvanians in Protecting Against Identity Theft..... 3

ACQUISITIONS CORNER..... 5

Seller Beware: Surety Obligations can Remain after Sale of Business 5

Buyer may Implicitly Assume Lease..... 6

ESTATE CORNER..... 7

Positive Changes to Federal Estate Tax..... 7

POTPOURRI..... 7

Good News/Bad News: Pennsylvania Enacts Health Savings Account Legislation..... 7

Pennsylvania Streamlines Collection of Delinquent Realty Transfer Tax..... 8

KKAG SPEAKING OUT..... 9

BUSINESS LAW

reports. This requirement, known as the “Disposal Rule”, was established and is enforced by the Federal Trade Commission (“FTC”) pursuant to the Fair and Accurate Credit Transactions Act of 2003, which amends the Fair Credit Reporting Act (“FCRA”). Businesses that use consumer reports for a business purpose are subject to the requirements of the Disposal Rule.

For purposes of the Disposal Rule, a consumer report is any written, oral or other communication of information from a consumer reporting company and bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which information is used, or is expected to be used, to determine a consumer’s eligibility for insurance, credit or employment. In addition, under the Disposal Rule, a consumer report includes any personally identifiable information about a consumer which is derived from such records. Consumer reports include consumer credit reports, credit scores, employment background checks, insurance claims, tenant histories, medical histories or check writing histories.

To comply with the Disposal Rule, businesses using consumer reports for business purposes need to adopt policies that provide for reasonable disposal of consumer reports. The policies need to be appropriate to prevent the unauthorized access to or use of the information contained in the reports. The FTC recognizes that businesses need flexibility to determine which destruction practices will be reasonable for them, depending on the nature of the business, the

Federal Law Requires Businesses to Properly Dispose of Sensitive Consumer Information

Beginning on June 1, 2005, businesses must properly dispose of sensitive information contained in or derived from consumer



sensitivity of the information and the cost of destruction. Taking those variables into account, the FTC identifies the following as reasonable measures to dispose of consumer report information:

- Implementing and monitoring compliance with policies and procedures requiring the burning, pulverizing, or shredding of papers so the information cannot be read or reconstructed;
- Implementing and monitoring compliance with policies and procedures requiring the destruction or erasure of electronic files or media so the information cannot be read or reconstructed; or
- Hiring a document destruction contractor to dispose of information consistent with the Rule, provided that the business conducts due diligence on the contractor - such due diligence should include, but is not limited to, reviewing an independent audit of a disposal company's operations or its compliance with the Rule, obtaining information about the disposal company from several references, requiring that the disposal company be certified by a recognized trade association, or reviewing and evaluating the disposal company's information security policies or procedures.

Businesses that violate the Disposal Rule are subject to the penalties established under the FCRA. Specifically, a business that engages in a willful violation may be subject to a private lawsuit for actual damages not to exceed \$1,000, punitive damages, costs and attorneys fees. Negligent violations will subject businesses to actual damages, attorneys' fees and costs. Further, the FTC is

authorized to bring enforcement actions that could result in prison time for violators and fines of up to \$2,500 per violation.

Business Friendly Changes to Bankruptcy Law

With the enactment of the Bankruptcy Abuse Prevention and Consumer Act of 2005, Congress in some ways made the Bankruptcy Act friendlier towards businesses. Among the changes to the Bankruptcy Code that will be beneficial to businesses, when they are a creditor in a bankruptcy are the following:

- In preference actions, which are actions where a creditor is asked to give back money to the debtor because the payment was within ninety days of the bankruptcy, the Act makes the standard of proof for the creditor's position easier to meet.
- The Act prohibits preference actions where the aggregate value of the property in question is less than \$5,000.
- The Act requires that preference actions to recover debts of less than \$10,000 against non-insiders can only be brought in the district court where the defendant resides.
- The Act gives a supplier a priority expense claim for the value of any goods received by the debtor within twenty days of the commencement of the bankruptcy. Additionally, the Act has increased the period of time that a supplier may reclaim goods from ten days to forty-five days.

All of these changes are welcome additions for businesses that find themselves a creditor in a bankruptcy proceeding or a supplier to a now bankrupt business.



TECH FRONTIER

Businesses Must Assist Pennsylvanians in Protecting Against Identify Theft

State Law Requires Businesses to Notify Customers of Security Breaches

Following the 2005 debacle involving ChoicePoint's sale of personal and financial information of approximately 145,000 people to a criminal enterprise, state legislatures have faced increasing pressure to address the problem of identity theft. In late 2005, the Pennsylvania legislature enacted a law requiring Pennsylvania residents to be notified when their personal information was or may have been disclosed due to a security system breach. The act, known as the Breach of Personal Information Notification Act, takes effect on June 20, 2006 and applies to the discovery of security system breaches occurring after June 20, 2006.

There are several general provisions of the Act. First, any entity that maintains, stores or manages computerized data that includes personal information must provide notice of a security system breach to Pennsylvania residents whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.

Second, if the security breach is linked to a breach of the security of the encryption, or if the security breach involves a person with access to the encryption, an entity must provide notice of the breach of the security system if encrypted information is accessed and acquired in an unencrypted form.

Third, when a vendor that maintains, stores or manages computerized data on behalf of another entity, the vendor must notify such other entity of any breach of the vendor's security system. Thereafter, however, it is the entity, and not the vendor, which is responsible for making the determinations and discharging the obligations imposed under the Act.

Fourth, when an entity provides notice to more than 1,000 persons at one time, the entity also promptly must inform consumer reporting agencies of the timing, distribution and number of notices.

Fifth, an entity maintaining its own notification procedures as part of its privacy or security policies will be deemed in compliance with the Act if its policies are consistent with the notice requirements of the Act and the entity notifies subject persons in accordance with its policies in the event of a security breach.

Personal information covered by the Act includes an individual's first name or initial and last name when they are combined with and linked to any of the following unencrypted or unredacted data elements: (i) social security number, (ii) driver's license number or a state identification card number issued in lieu of a driver's license, or (iii) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. Unfortunately, the Act does not provide guidance on what constitutes the combining and linking of such information with an individual's name. Presumably, any method by which the covered information is tied together will be



sufficient to trigger potential liability under the Act. Fortunately, the Act provides helpful carve-outs to the definition of personal information, the alteration or truncation of data elements, so that no more than the last four numbers are accessible as part of the data, is considered a redaction, and therefore does not constitute personal information requiring notification in the event of disclosure. In addition, publicly available information - information lawfully made available to the general public from federal, state or local government records does not constitute personal information.

Nearly all business enterprises and governmental agencies are covered by the Act, since it applies to state agencies, political subdivisions of the state, individuals, sole proprietorships, partnerships, corporations, and other associations, whether or not for profit, doing business in the Commonwealth. In another broad sweep, the law covers individuals whose principal mailing address (as reflected on the entity's computerized data) is located in Pennsylvania. Thus, even persons who do not actually reside in Pennsylvania, but who have a primary mailing address in Pennsylvania, are protected under the Act.

The term "breach of the security of the system" is defined as the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information and that causes loss or injury to Pennsylvania residents or that the entity reasonably believes has caused or will cause such loss or injury. Excluded from this definition is the good faith acquisition of personal information by an entity's employee

or agent, where the information is used only for a lawful purpose of the entity and the information is not subject to further unauthorized disclosure.

Although the law is sweeping in its breadth, businesses have some flexibility in terms of the types of notice it may provide. Specifically, the following types of notice are permissible:

- Written notice to the last known home address for an individual.
- Telephonic notice, if the customer can reasonably be expected to receive the notice and the notice is provided in a clear and conspicuous manner, describes the security breach in general terms, verifies personal information without requiring the customer to provide personal information and includes a phone number or internet website to contact for more information or assistance.
- E-mail notice, if a prior business relationship exists and the entity has a valid electronic mail for the individual.
- "Substitute notice" if the entity demonstrates one of the following: (a) the cost of providing notice would exceed \$100,000, (b) greater than 175,000 persons are affected by the breach, or (c) the entity does not have sufficient contact information. To qualify as substitute notice, the entity must provide recipients with all of the following: e-mail notice when the entity has an e-mail address for the subject persons, conspicuous posting of the notice on the entity's internet website, if any, and notification to major statewide media.



The required notice must be provided without unreasonable delay, taking into account the time necessary to take measures needed to determine the scope of the breach. Notice also may be delayed if the entity is notified in writing by a law enforcement agency that the notice will impede a criminal or civil investigation.

The Act supersedes and preempts all local and municipal rules and ordinances covering matters set forth in the Act. Willful and knowing violations of the Act are considered to be unfair or deceptive acts or practices contrary to Pennsylvania's Unfair Trade Practices and Consumer Protection Law and are enforceable by the Pennsylvania Attorney General.

ACQUISITIONS CORNER

Seller Beware: Surety Obligations Can Remain after Sale of Business

In a case of first impression, the Pennsylvania Superior Court upheld a lower court judgment against a former business owner whose personal obligation to pay a corporate vendor survived the sale of his business. The case of Fessenden Hall of Pa., Inc. v. Mountain View Specialties, Inc., 863 A.2d 578 (Pa. Super 2004), appeal denied, 882 A.2d 479 (Pa 2005), concerned a dispute between a vendor of Mountain View Specialties, Inc. ("Mountain View") and Mr. Lafferty, the sole shareholder of Mountain View. Early in the relationship between Mountain View and the vendor, Mr. Lafferty had signed a personal guarantee in favor of the vendor as a condition of the vendor extending credit to the corporation. Five years into that relationship, Mr. Lafferty sold all of the assets of the corporation, including its name, to a new owner. After the sale, Mr. Lafferty dissolved the corporation whose assets were sold and whose indebtedness to vendor he had personally guaranteed. The new corporation, using the old name "Mountain View", continued to do business with the vendor.

Unfortunately, Mr. Lafferty failed to inform the vendor of the sale or the change in the business structure or ownership and he never renounced the written guarantee. Moreover, after the sale, Mr. Lafferty continued to work at Mountain View, remained the vendor's point-of-contact person at Mountain View, and the "new" Mountain View used the same address and purchase order forms as its predecessor. The parties stipulated to the fact that nothing would have alerted the vendor that the "new" Mountain View had undergone a change in ownership.

The "new" Mountain View defaulted on its credit obligations with the vendor. Thus, the vendor sought recovery against Mr. Lafferty, individually, as a corporate guarantor. The trial court found Mr. Lafferty liable as the guarantor despite his claim that the debt defaulted upon was incurred by a corporation which was different from the one he had owned. In affirming the trial court, the Superior Court cited the doctrine of equitable estoppel, which is applicable whenever a party intentionally or negligently induces another to believe certain facts and the other



party justifiably relies and acts upon that belief. Where the relying party suffers damages because of such reliance, the other party is prevented from denying the facts or repudiating his statements or conduct. Applying this doctrine to the case at hand, the Superior Court reasoned that Mr. Lafferty was obligated to the vendor because: (i) there was a valid, written guarantee holding Mr. Lafferty responsible for the debts of Mountain View, (ii) Mr. Lafferty failed to inform the vendor of the corporate changes, (iii) Mr. Lafferty was the exclusive contact between the vendor and Mountain View after the asset sale, and (iv) the vendor would not have extended the line of credit to Mountain View without an individual guaranty.

This case illustrates the need for business owners to notify creditors of changes arising out of the sale of their businesses, to renounce their personal guarantees (in writing) and to obtain written releases of their personal obligations.

Business Acquisitions: Buyer May Implicitly Assume Lease

Purchasing a business requires careful consideration of many issues. If purchasers are not careful in their due diligence and structuring of the acquisition, they may become vulnerable to liabilities of the seller. Therefore, purchasers and their counsel routinely review liens, taxes and other successor liability factors to gain comfort that the purchaser is only assuming the liabilities that it intends to assume.

In a recent case, a purchaser who temporarily operated the purchased business out of the seller's leased property was held to have

assumed the lease even though the purchaser never executed any written assumption of the lease and the landlord never agreed to the assignment of the lease to the purchaser. In the case, the lease required the tenant to obtain the landlord's consent to any assignment of the lease. The purchaser and the landlord could not work out the terms of the assignment prior to closing, and therefore the transaction closed without any assignment or assumption documentation by any party. The purchaser used the leased property for eleven months. During that time, the purchaser and the landlord unsuccessfully continued to attempt to negotiate the terms under which purchaser would lease the property. In the end, no consent to assignment was given by the landlord and no new lease was finalized.

After the purchaser moved out of the property, the landlord sued the purchaser for rent. The court held that the purchaser had impliedly assumed the seller's lease, despite the absence of any written assumption. Important to the court were the following facts: (1) the purchaser occupied the property for eleven months; (2) the purchaser continued the same activities as the seller; (3) the purchaser paid the rent and utilities during the eleven months in its own name – it did not leave the utilities in seller's name; and (4) the purchaser maintained the property and installed fire extinguishers as required by seller's lease.

In conclusion, business acquisitions can be complex. The parties, especially the purchaser, need to carefully review areas where liabilities may be assumed, intended or not.



ESTATE CORNER

Positive Changes to Federal Estate Tax

Starting January 1, 2006, two significant changes occurred automatically to the federal estate tax. First, the estate tax applicable exclusion increased from \$1.5 million to \$2 million for each person. Thus, married couples with estates under \$4 million should not owe estate tax with proper planning. To take advantage of this increase, married couples who have done bypass trusts should review the assets in each spouse's name to be

sure each spouse has at least the exemption equivalent in their name.

Second, the annual gift exclusion amount increased from \$11,000 to \$12,000. The annual gift exclusion is the amount of annual gifts a person may make to another without using any of their lifetime exemption amounts. Using annual exclusion gifts is a highly effective estate planning tool. If an annual exemption is not used in a calendar year, it is gone – unused exclusions do not accumulate year to year.

POTPOURRI

Good News/Bad News: Pennsylvania Enacts Health Savings Account Legislation

Made effective under federal law in 2004, Health Savings Accounts are becoming a popular health insurance option for small businesses faced with rising health care costs. Health Savings Accounts, or "HSAs", have the potential to provide employers with health care cost savings because HSAs are used in tandem with high deductible health insurance plans, which generally cost less in premium dollars than those with lower deductibles. HSAs can be funded by either or both of employer and employee contributions, and they provide covered insureds with access to funds needed to pay for qualified medical expenses falling below the plan's deductible limit. Of course, federal law and regulation limit the amount of annual contributions that

may be made to HSAs, set maximum annual out-of-pocket spending limits, establish the minimum annual policy deductible and impose other complex requirements.

For purposes of federal law, the tax treatment of deposits made to an HSA is similar to the treatment of deposits made to a qualified 401(k) retirement plan. Contributions made by an employee, and contributions made by employers on behalf of employees, are excluded from federal income tax (and payroll taxes) and the earnings on contributions made to HSAs accrue free from federal income tax. Even withdrawals from HSAs are tax-free if they are used to pay for qualified medical expenses. Employees need not deplete their HSA fund balances annually. Rather, federal law permits fund balances to carry over from year to year, enabling



employees to establish portable health care nest-eggs.

Federal legislation authorizing HSAs does not account for the fact that some states, as a function of their regulatory oversight of the insurance industry, completely prohibit insurance deductibles or substantially restrict the deductible limits for certain medical insurance benefits. In this regard, Pennsylvania has acted in a positive direction by enacting the Health Savings Account Act, which became effective in the fall of 2005. This legislation exempts high deductible health plans meeting applicable federal requirements from Pennsylvania laws which restrict or limit deductibles for mandated minimum health insurance benefits or reimbursements.

Although the legislation has paved the way for increased marketing and use of HSAs in the Commonwealth, it fails to mirror the favorable tax treatment offered by the federal legislation. Contributions to HSAs by employers and employees are taxable for purposes of Pennsylvania state income tax. Thus, although HSAs established by Pennsylvania employers will enjoy a federal tax incentive for both contributions and earnings accrual, they will not enjoy a similar state tax incentive, since only earnings, and not contributions, are state income tax-free.

Pennsylvania Streamlines Collection of Delinquent Realty Transfer Tax

Pennsylvania legislation was enacted in 2005 to streamline the collection of delinquent local realty transfer tax. According to the Department of Revenue, the legislation is intended to establish effective and efficient local tax enforcement through the use of the

Department's resources, experience and computer systems.

Under Pennsylvania's realty transfer tax system, each of the state and local government assesses realty transfer tax in the amount of 1% of the fair market value of real property. The recorder of deeds in the county where the real property is located is responsible for collecting both portions of the tax when a taxable document is recorded. The Department of Revenue scrutinizes thousands of real estate transactions each year for realty transfer tax compliance. When the Department determines that taxpayers have recorded documents which claim improper tax exemptions or which under-report value, the Department issues notices of determination to taxpayers in order to formally assess the tax, which is then considered delinquent.

In summary, the new legislation attempts to enhance the collection of delinquent local realty transfer tax by doing the following:

- Expanding the time period for delinquent assessments from three to six years if the taxpayer underpays the tax by twenty-five percent (25%) or more, and expanding the time period indefinitely if any part of the underpayment is due to fraud or an undisclosed, intentional disregard of applicable rules and regulations.
- Authorizing the Department of Revenue to collect both the state and local portion of the delinquent and unpaid realty transfer taxes (plus fines or penalties), rather than the state portion alone.
- Extending fraud penalties to cover the local portion of the realty transfer tax.



- Expanding the coverage of tax liens imposed by the Department of Revenue to include the local realty transfer tax portion, when a combined state and local delinquent tax assessment is issued.
- Permitting tax information to be shared between state and local officials.



KKAG SPEAKING OUT...

- ◆ Mark is co-authoring the book *“Privately Held Business: Acquisition and Sale”*
- ◆ In May 2006, Mark Grimm will be giving a presentation for accountants entitled *““An Overview of Buying and Selling a Business.”*
- ◆ In the Spring of 2005, Mark Grimm gave a presentation for accountants entitled *“Entity Selection: What Do I Want to be When I Grow Up?”*
- ◆ In the Spring of 2005, Mark Grimm gave another presentation for accountants entitled *“An Overview of Buying and Selling a Business.”*

We hope you find this issue of the Business Law Watch helpful and informative. If you have any questions regarding any of the subjects covered or other business law matters, please do not hesitate to call or e-mail Mark Grimm (e-mail: grimm@kkaglaw.com), Clarence Kegel (e-mail: kegel@kkaglaw.com) or Beth Reister (e-mail: reister@kkaglaw.com) at 717/392-1100.



KEGEL KELIN ALMY & GRIMM LLP
Business Law Group
(717) 392-1100

KKAG has a substantial business law practice, representing businesses of all sizes.

KKAG advises businesses on mergers and acquisitions, business formation, general contracting and business counseling, financing, distribution and trade regulation, tax, technology law issues, as well as a full range of other legal areas faced by businesses.

D. Mark Grimm, Jr., Clarence C. Kegel, Jr. and Elizabeth A. Reister are the primary lawyers in our business law group. Other lawyers are involved in business law work as appropriate based on their areas of expertise.