LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication

Volume 28, Number 8 • November 2013

Same-Sex Benefits

The Latest IRS Guidance

By Sarah Riskin and Morgan Holcomb

In its June 26, 2013 decision in *United States v. Windsor*, the United States Supreme Court held Section 3 of the Defense of Marriage Act (DOMA) unconstitutional under the due process and equal protection guarantees of the Fifth Amendment. In focusing on the states' historic responsibilities in defining and regulating marriage, the Court reasoned that so long as a particular state's regulation of marriage comports with constitutional standards, the state's regulation is to be respected. Congress's attempt in DOMA to single out state-recognized same-sex marriages was therefore unconstitutional.

Although the full reach of the ruling is yet to be seen, recent IRS guidance represents the beginning of what promises to be a long process of agency rulemaking in light of the *Windsor* decision.

Windsor specifically addressed federal estate tax benefits, and following the case it is clear that the IRS is obliged to treat a couple as married when the couple's state recognizes them as such, at least for federal estate tax purposes. The Court itself remarked that *Windsor* went beyond simply estate tax and is applicable to other federal tax rules, but *Windsor's* impact on areas of law outside of tax remains uncertain.

continued on page 9

Protecting Confidential Information and Trade Secrets from Defecting Employees

By Susan Guerette

In today's business world, the entirety of a company's most significant information can be uploaded to a device the size of a thumbnail and taken by a departing employee. The consequences can be devastating. With advances in technology, it is more important than ever for companies to identify their confidential information and institute measures to preserve and protect that information from employees who decide to leave the company.

Use Technology to Control Information

As a first step, companies should consider which employees need access to what information. Once the determination is made, employers should require passwords to access any company computer, and use additional passwords to restrict employees who do not need to view more sensitive company information. Some companies are even employing voice-recognition software and more advanced methods of confirming identities before allowing access to more sensitive information. In addition, businesses can consider encrypting files and folders that they do not want easily accessed.

In addition to limiting employee access to information, companies can also use loss-prevention technology to prevent employees from taking or transferring that information. For example, software is available to prevent employees from inserting USB thumbdrives into their computers to take information. Likewise, businesses can use technology to monitor e-mails and text messages so that when triggering information is sent by e-mail, the company is notified. This type of software can be particularly effective in preventing employees from e-mailing confidential information to their homes or new employers when they leave. Software is also available to monitor printing and file-sharing services. Companies need to consider how their information may be transmitted and how comprehensive they want their preventive measures to be.

continued on page 2

In This Issue

Trade Secrets

continued from page 1

Companies that allow employees to access or store confidential information on their personal devices should particularly consider protecting information through technology. Higher-end controls may be needed for documents on remote computers or mobile devices, and companies may want to contemplate requiring software on laptops and smartphones that will enable the company to remotely wipe the proprietary contents of these devices as soon as the employee resigns.

Taking these steps will serve your company well on three fronts. First, they will help to prevent employees from taking information that could benefit a competitor. Second, if an employee does take information and the company sues to prevent the misappropriation and misuse of that information as a trade secret, the company will need to prove it took steps to keep the information confidential. If reasonable steps are not taken to protect the information, trade secret protection may not apply to the information. Finally, good technological controls will also provide evidence of attempted misappropriation in the event the company decides to seek injunctive or other relief in court.

Implement Agreements

Although a company can go a long way toward protecting its information through the use of software and other technology, these methods are not fullproof. Therefore, companies should also institute policies affirming that company information is confidential and must be treated as such. Companies should consider what types of information they deem confidential and proprietary, and describe that information in their confidentiality agreements. Since an increasing number of employees are re-creating information once they arrive at their new employer, the company should also specify that even information retained in memory is confidential and should not be used or disclosed other than to conduct business on behalf of the company.

The policy should require that information not be taken, used or disclosed, but also that if it is in the employee's possession when he resigns, it should be immediately returned. In order to determine exactly what the employee took and what he may have done with the information, policies should be clear that any information in electronic format should be preserved and the company is permitted to review and delete that information.

Confidentiality agreements should also specify that the company has the right to inspect the employee's personal devices if it suspects that they contain confidential information. In fact, if a company decides to allow employees to use their own personal devices to conduct business on behalf of the company, it is advisable to require them to sign a specific Acceptable Use Agreement. This agreement should outline the acceptable uses of company information and make it clear that employees are responsible for keeping company information secure. This is a good place for the company to make it clear that use of the personal devices for company business is conditioned upon the installation of remote wiping software.

Companies should not forget about independent contractors, vendors and other business partners when assessing measures to safeguard their confidential information. Any information disclosed to such entities should likewise be protected by an appropriate agreement.

Disseminate a Social Media Policy

Many companies encourage employees — particularly those involved in sales and marketing — to use social media sites to increase their contacts and communicate with customers. Yet, this social interaction, which is very beneficial while the employee is working to promote

continued on page 11

Susan Guerette is a partner in the Philadelphia office of Fisher & Phillips. She can be reached at sguerette@laborlawyers.com.

Third-Party Litigation Investing And Attorney-Client Privilege

By David A. Prange

Civil litigation is potentially expensive, and achieving lucrative outcomes is not without risk. In recent years, companies with viable claims have looked to diversify their risk by partnering with third-party investors. Successful investment relationships require substantial due diligence and communication. This communication may include claim-holder materials that are subject to the attorney-client privilege or that are considered attorney work product.

A claim-holder's communications with its investors, or potential investors, introduces the risk of privilege waiver and the potential exposure of sensitive information to an adverse party in later litigation. An attractive discovery subject for any defendant may be the materials shared between the plaintiff and its investor. The plaintiff's evaluation of its claims would provide good information for cross-examination. Thus, the issues of privilege and work product protection arise when a plaintiff shares otherwise protected information.

Case law addressing whether these communications destroy the privilege is limited and inconsistent. Courts are divided on whether the claimed commonality in such a relationship — a financial interest — is enough to preserve privilege. Still, the claim-holder will need to communicate some information to an investor to obtain investment in the prosecution of its claims. This article considers recent case law addressing privilege challenges and third-party investment relationships, and provides suggestions on how to minimize the risk of destroying any privilege through the provision of sensitive information in such relationships.

David A. Prange is a senior associate with Robins, Kaplan, Miller & Ciresi LLP. The author gratefully acknowledges **Becky Thorson**, a partner of the firm, for discussion and review on the topics of this article. Prange may be reached at DAPrange@rkmc.com.

The Attorney-Client Privilege and Work Product Doctrine

The attorney-client privilege applies to communications (oral or written) between a client and an attorney when the attorney is acting to provide legal advice. The privilege may also extend to communications between agents of the client and the client's attorney. The communicating parties must intend for the communication to be confidential. There are limited exceptions to the privilege, such as the crime-fraud exception, that may compel disclosure, but absent application of an exception the privilege protects any disclosure of the attorney-client communication. The privilege does not prevent the disclosure of underlying facts, but a fact cannot be obtained if only available through a protected communication. The privilege of an attorney-client communication can be waived by the client, but not by the attorney.

Separate from the attorney-client privilege is the attorney work product doctrine. This is broader in scope than the attorney-client privilege because the doctrine protects materials prepared by attorneys and their agents in the anticipation of litigation that may not be communicated to the client. The litigation need not be active for the doctrine to apply; the doctrine may also cover materials developed before a lawsuit is filed. Work product may cover materials where the client has no direct involvement. The work product doctrine is intended to shield the opinions of counsel from discovery to allow for case preparation.

Interplay of the Common Interest Doctrine

The separate "common interest doctrine" appears in opinions considering whether disclosure of otherwise attorney-client communications or attorney work product (collectively "attorney-associated information") to a third-party investor resulted in a waiver. Sometimes mislabeled as a separate "privilege," the common interest doctrine is a rule for determining whether a privilege is preserved when materials are shared between non-related parties. It is not, in itself, a distinct form of privilege.

A common interest may exist if the parties to the communication share a common interest, the disclosing party has a reasonable expectation that the communication would remain confidential, and the disclosure is reasonably necessary. In the context of third-party investors, courts have identified two separate common interests — a common legal interest to a claim and a common financial interest in the outcome of prosecuting a claim. Courts disagree about whether a financial common interest alone satisfies the common interest requirement. Courts have also addressed whether the disclosing party, invariably the claim-holder/plaintiff, had a reasonable expectation that the information would remain confidential.

Case Law

Courts are mixed on whether disclosure of attorney-associated information to a third-party litigation investor waives the privilege. In an early opinion on the subject, a Delaware federal court in *Leader Technologies, Inc. v. Facebook, Inc.*, held that the plaintiff waived its attorney-client privilege on certain documents that it shared with litigation financing companies during the companies' evaluation of the investment opportunity. 719 F. Supp. 2d 373, 376-77 (D. Del. 2010). The defendant moved to compel the production of the attorney-associated information exchanged between the plaintiff and its financing companies. The plaintiff argued that there was no privilege waiver because the subject documents were only exchanged after a finance company and itself established a common interest. The argued common interest was the financing company's interest in funding the litigation. The court disagreed, finding that a

continued on page 4

Privilege Waiver

continued from page 3

common interest arising from only a commercial relationship was not sufficient to allow the common interest exception to waiver to apply. The court compelled the plaintiff to produce the subject documents.

In contrast to *Leader Technologies* is *Mondis Technology, Ltd. v. LG Electronics, Inc. et al.*, where a Texas federal court held there was no waiver when the plaintiff shared similar types of information with prospective investors. 2011 U.S. Dist. LEXIS 47807 (E.D. Tex. May 4, 2011). The shared information included litigation and licensing strategy and financial returns from implementing the strategy. On a defendant's motion to compel production of this information, the court held that the materials created for potential investors were work product, and that the sharing did not waive the protection. Significant to the court's holding was the existence of nondisclosure agreements in place between the plaintiff and potential investors before the plaintiff shared the information. The court reasoned that the plaintiff had a reasonable expectation of confidentiality based on the nondisclosure agreements. The disclosure would not "substantially increase the likelihood that an adversary would come into possession of the materials." *Id*. at *16-17. The court did not consider whether a financial interest between the plaintiff and the potential investors was sufficient to find that there is a common interest.

In *Devon IT, Inc. v. IBM Corp.*, a Pennsylvania federal court reached a similar conclusion. The court held that the disclosure of attorney-associated information to a potential investor did not waive any privilege because a separate common interest and nondisclosure agreement existed between the parties. 2012 WL 4748160, *1 n.1 (E.D. Pa. Sept. 27, 2012). The plaintiff moved for a protective order and to quash a third-party subpoena served by the defendant on third parties who had received the information from the plaintiff. The latter had provided the information subject to the nondisclosure agreement, but before executing a funding agreement. The court granted the plaintiff's motions, holding that the information was work product or attorney-client privileged. The court further held that the common interest doctrine prevented waiver in view of the existing common interest agreement. The common financial interest in the case outcome, and that there was no other recognized interest between the parties, was sufficient for the common interest doctrine to apply.

Two federal courts in Delaware have also considered the issue of privilege waiver for documents shared with third-party consultants. In *Walker Digital, LLC v. Google, Inc.*, the court held that attorney-associated information exchanged between the plaintiff and its patent monetization consultant was protected under the common interest doctrine. Civ. No. 11-309-SLR, ECF No. 280 (D. Del. Feb. 12, 2013). The court relied on an agreement between the plaintiff and the consultant providing for a common interest between them. The opinion is not specific on the timing of the communications and exchange of information, for example whether the disclosure was before or after execution of the agreement.

Similarly, in *Intellectual Ventures I LLC v. Altera Corp.*, the court upheld the plaintiff's privilege claim to patent acquisition materials shared with a third-party contractor. C.A. No. 10-1065-LPS, ECF No. 415 (D. Del. Jul. 25, 2013). The plaintiff argued that communications and materials shared between the plaintiff's employees and a contractor tasked with identifying patents for acquisition by the plaintiff did not destroy applicable privileges because there was a common interest. The court agreed. While the *Intellectual Ventures* and *Walker Digital* opinions do not address third-party investors, in view of the *Leader Technologies* opinion they may reflect a split within the district that a common financial interest, without more, may be enough for the common interest doctrine to apply.

How to Minimize the Risk Of Privilege Waiver

The small number of courts that have considered the privilege waiver issue in the third-party investing context, coupled with the split in opinions, introduces uncertainty to whether shared communications are protected from disclosure. The opinions do not present a consistent trend, and there is some gloss over the treatment of different categories of documents exchanged and the significance of nondisclosure agreements. The decisions may reflect regional preferences to preserving privilege and applicable of the common interest doctrine — the opinions originate from only two (Third and Fifth circuits) of the federal court system's 13 circuit regions.

Claim-holders and investors should be cognizant of the risk that their communications and information could be seen by an adverse party. Thus, if a claim-holder must disclose attorney-associated information to obtain investment, or to manage an investment relationship, the claim-holder can implement several practices to reduce the chance of privilege waiver.

First, attorney-client communications only between a party and its attorney are off-limits for sharing. This prohibition applies regardless of whether the investor is evaluating the opportunity or has made a commitment. In communicating with the third-party investor, neither the client nor its attorney should volunteer separate attorney-client communications.

Second, obtain non-disclosure agreements in addition to any investment agreement. Completing a non-disclosure agreement should be the first task of any investing relationship, and regardless of the final outcome of an investing evaluation. An investor will likely need to evaluate confidential business information of the party seeking investment. Absent an appropriate agreement, a disclosure may accidentally waive the confidentiality claim. Further, any agreement should i4clude within its scope statements of

continued on page 10

From A to ZIP Codes, and Beyond

By Kenneth L. Chernof and Allyson Himelfarb

An ever-increasing number of companies find themselves facing potential liability for practices concerning the use, collection, or release of consumer data. The courts are rife with class-action litigation by individuals seeking compensation in the wake of stolen or lost laptops, hacked computer networks, or data stolen through phishing scams, even in cases where the plaintiffs have not suffered any actual misuse of their own data. Recent legal developments have helped to limit the viability of these cases. Perhaps the most prominent development is the U.S. Supreme Court's recent decision in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), in which the Court made clear that plaintiffs cannot establish standing to sue based on a mere risk of future injury, and plaintiffs may not manufacture standing by taking steps to prevent the risk of future injury.

Collecting ZIP Codes

Despite — and perhaps because of — this and other positive developments, new and increasingly creative fronts in data privacy litigation and enforcement are constantly being opened. One such evolving area of potential liability impacts companies that collect ZIP code information from consumers during routine retail transactions. Many companies request and collect a customer's ZIP code at the time of a retail transaction, and they do so for various purposes: some may need the information for delivery of the purchased product; some may wish to enroll the customer in some type of rewards or other store benefits program; some may use the information to send marketing materials to the customer; and some may sell the information to third parties. Although there are many legitimate purposes for collecting ZIP code information, this practice has now borne significant scrutiny.

Pineda

One of the first cases to challenge the practice of collecting ZIP code information was heard in 2008 when plaintiff Jessica Pineda filed a putative class action against retailer Williams-Sonoma, alleging that the retailer's request for her ZIP code during a sales transaction — which she alleged the company used to send her marketing materials — violated a California statute that prohibits businesses from requiring or requesting "personal identification information" as a condition for accepting a credit card payment during a business transaction. The statute defines "personal identification information" as any information about the cardholder other than the information set forth on the credit card itself, such as a consumer's address or telephone number.

Ms. Pineda alleged that because her ZIP code constituted "personal identification information," its collection by Williams-Sonoma violated the statute. In 2011, the highest court in California agreed, reasoning that the term "address" encompasses not only a complete address, but also its components. *See Pineda v. Williams-Sonoma Stores, Inc.*, 246 P.3d 612 (Cal. 2011). According to the court, interpreting the statute to prohibit the collection of ZIP codes was "most consistent with [the] legislative purpose" of providing "robust consumer protections by prohibiting retailers from soliciting and recording information about the cardholder that is unnecessary to the credit card transaction." *Id.* at 620.

In the wake of *Pineda*, California has become something of a hotbed of activity in this area, with dozens of similar cases filed against a multitude of retailers in that state alone. Given that a violation of the California statute can subject a company to civil penalties of up to $250 per violation, the stakes for retailers doing business in California are especially high. Worse still, because the *Pineda* decision applies retrospectively, companies can still face liability even over past practices.

Tyler

A similar case was also filed against Michaels Stores in federal court in Massachusetts in 2011. In that case, plaintiff Melissa Tyler alleged that the defendant retailer illegally collected and used her ZIP code information to send her unsolicited marketing materials. Similar to California, Massachusetts has a statute prohibiting companies that accept credit cards from requiring a consumer to write any "personal identification information" that is not required by the credit card issuer on the credit card transaction form.

Massachusetts' highest state court noted that because the principal purpose of the state statute is to protect consumers' privacy — not to protect against identity fraud — a consumer need not allege that she has been the victim of identity fraud to be able to bring a claim under the statute. *Tyler v. Michaels Stores, Inc.*, 464 Mass. 492 (2013). Fortunately, even *Tyler* concludes that plaintiffs must make some showing of injury to have a viable claim.

According to *Tyler*, two types of injury that might entitle a plaintiff to seek damages under the statute include: 1) if the consumer actually receives unwanted marketing materials as a result of the collection of the consumer's personal information; or 2) if the merchant sells the consumer's personal information to a third party. The lesson to be learned from *Tyler* is that even if the consumer suffers not one penny of loss from the collection of her ZIP code information, she may still be entitled to recover statutory damages if the company acquires her personal information and uses that information "for its own business purposes."

Wide Implications

Taken together, the *Pineda* and *Tyler* decisions have broad exposure implications for retailers and other companies, not only those

continued on page 6

Kenneth L. Chernof is a partner and **Allyson Himelfarb** is an associate at Arnold & Porter LLP. The authors wish to thank summer associate **Neil Sawhney** for his contribution to this article.

ZIP Codes

continued from page 5

doing business in California and Massachusetts, but in other jurisdictions as well. That is because in addition to California and Massachusetts, similar statutes prohibiting companies from requiring or requesting certain personal identification information in connection with credit card transactions now also exist in Delaware, Kansas, Maryland, Minnesota, New Jersey, New York, Pennsylvania, Rhode Island, Wisconsin, and the District of Columbia, and more may be enacted in the coming years.

While the state statutes vary in their precise language, they generally prohibit entities from requesting or requiring customers to provide or write down personal identification information as a condition of processing credit card transactions. Many statutes provide for statutory damages ranging anywhere from $25 to a maximum of $10,000 for each violation. Moreover, many of the statutes permit individuals to pursue damages through class actions. Thus, even with statutory damages as seemingly insignificant as $25 per violation, it does not take long for those damages to add up, particularly when individual plaintiffs often seek to represent expansive classes defined as all consumers from whom ZIP code information was requested or collected in connection with a credit card transaction during a given time period. As one example, a putative class action was recently filed in federal court in the District of Columbia challenging a popular clothing retailer's collection of ZIP code information and seeking $500 in statutory damages for each member of the class — defined as all customers from whom ZIP code information was collected over a three-year period.

Exceptions

The collection of ZIP codes is not prohibited in all circumstances, however. Many of the state statutes also provide exceptions where the collection of customers' personal identification information is permissible — such as where the information is required for the shipping, installation, or delivery of the purchased product; fulfilling warranty obligations; or for some other purpose that is incidental, but related to the credit-card transaction, such as fraud prevention. In deciding whether a given practice is permissible, recent cases illustrate that the focus is on the customers' perception of the transaction, rather than on what the retailer subjectively intends to do with the requested information.

In *Pineda*, *Tyler* and many other recent cases, the plaintiffs alleged that they provided their ZIP code information under the mistaken belief that the information was necessary to process their credit-card payment. However, where a retailer "falls over itself" to inform customers that the requested information is optional and is not required to complete the credit-card transaction, courts have held that in those instances, the relevant statute has not been violated. *See Gass v. Best Buy Co., Inc.*, 279 F.R.D. 561 (C.D. Cal. 2012).

Based on this reasoning, retailers who wish to continue collecting ZIP code information for their own business purposes may start posting signs or otherwise explicitly notifying customers that provision of their personal information is optional, is in no way required to complete their credit-card transaction, and explain how the retailer intends to use that information. The bottom line: When it comes to customers' data, transparency is paramount.

Are Relevant Statutes Necessary for Litigation?

Even in states where no such laws are on the books or where the relevant statutes do not permit private rights of action, the possibility for litigation still remains. This has already been seen in New Jersey. There, because the state law prohibiting the collection of personal information in connection with credit-card transactions is limited to enforcement by the state Attorney General, plaintiffs are forced to find a work-around. Thus, plaintiffs sought to challenge the practice of ZIP code collection under the state's more general consumer protection law, the Truth-in-Consumer Contract, Warranty and Notice Act. That statute prohibits sellers from entering into any written consumer contract that violates a "clearly established right of a consumer." Plaintiffs argued that the relevant "established right" was provided for in the state statute governing the collection of personal information during credit card transactions.

These attempts have so far been largely unsuccessful. In the two cases filed in federal court, the court dismissed the complaints, holding that plaintiffs were unable to allege any "written consumer contract," and thus could not state a claim under the statute. *See Feder v. Williams-Sonoma Stores, Inc.*, 2011 WL 4499300 (D.N.J. Sept. 26, 2012); *Darocha v. Wal-Mart Stores, Inc.*, No. 11-7583 (D.N.J. May 9, 2012) (unpublished). Despite these two decisions, the state of personal identification information law — and therefore the likelihood of additional class action lawsuits — remains unsettled in New Jersey. That is because in a recent state court case, the trial judge refused to dismiss a class action arising out of ZIP code collection practices, even though the plaintiff had alleged a violation of the same New Jersey statute.

Potential exposure is not limited to private class action litigation. The FTC, the nation's top privacy watchdog, has been increasingly focused on the data collection practices of companies, admonishing in an August 2013 speech that firms that acquire and maintain large sets of consumer data must be "responsible stewards of that information" and that data security and privacy will continue to be a top enforcement priority. *See* http://1.usa.gov/1csYiga.

Indeed, on Aug. 29, 2013, the FTC filed an administrative complaint against a medical testing laboratory for the company's alleged failure to protect the security of consumers' personal data, resulting in the personal information being found in

continued on page 8

Liabilities

By Michael Goldman

This article is the seventh installment in an ongoing series focusing on accounting and financial matters for corporate counsel.

Liabilities are what a company owes. They are also the offsetting part of the transactions that are the primary source of cash (the others being profits, equity infusions, or liquidation of assets). Very often, a quick study of the liabilities of a company will tell you much of what you need to know about its operations, health, and financing.

Liabilities are usually listed on the balance sheet in order of when they come due — the sooner they are due, the higher up they are. They are classified as Current (expected to be paid within one year) or Long-Term (not expected to be liquidated within the next 12 months).

Current Liabilities

Accounts Payable

Accounts payable are generally incurred for the purchase of supplies, inventory, materials, services, utilities, etc., and generally due within 30-90 days of incurrence of the obligation. When reviewing accounts payable, some of the key things to pay attention to are the ages of the outstanding payables and the vendor concentration. Are you dealing with a few powerful vendors, or are the company's obligations diffuse and scattered?

A lot can be learned about a company's operations and health by looking over the list of who it owes money to and who it is paying. Is it dependent on key vendors, is it churning vendors due to inabilities to pay, does it have enough market power to be able to stretch its vendors beyond traditional terms, is it constantly taking deductions from payments to vendors? What does it need to buy and how frequently does it replenish?

Accrued Expenses

Accrued expeses are costs that have been incurred, but for which invoices usually are not received (if an invoice had been received, the liability would be an Accounts Payable). Examples of commonly accrued expenses are wages, taxes, commissions, employee vacations, warranty expenses, and interest. In a distressed situation, most of the initial attention is focused on accounts payable, but once a transition to bankruptcy is made, many accrued expense items get a higher priority than the unsecured trade debt does.

Loans and Notes Payable

These are short-term borrowings from banks or other commercial transactions

Current Portion of Long-term Debt

This refers to the principal payments of longer-term debt instruments that must be paid within the next 12 months (following the date of the balance sheet).

Unearned Revenues

Unearned revenues are payments received by customers for products or services not yet provided, such as subscriptions, retainers, maintenance agreements, and insurance premiums.

Income Tax Payable

This is technically an Accrued Expense, but profitable companies usually show this amount separately. Unprofitable companies do not have to worry about it.

The Importance of Current Liabilities

Current liabilities are an important indicator of the company's financial health. One of the definitions of "insolvency" is "an inability to pay obligations as they come due." Since the current liabilities are the first obligations to come due, this is one of the first places to look in any solvency evaluation.

Long-Term Liabilities

Long-term Liabilities include the non-current portions of notes payable, bonds payable, and mortgage obligations. When a lease is considered to be a secured financing agreement, these obligations are also treated as long-term liabilities.

When a company is operating well, long-term creditors seem to have the worst positions of any of the stake holders. They do not get the constant attention (and payments) that short-term creditors receive, and they do not have the upside potential that excites equity holders. Long-term creditors usually take what they hope is minimal risk in exchange for earning a fixed rate of return. As a company spirals deeper and deeper into financial trouble, however, the significance of the long-term creditor usually strengthens, and in extreme situations it is often the long-term creditors that end up owning or deciding the fate of the company.

Deferred Taxes

These are long-term liabilities that arise out of timing differences between GAAP accounting and tax accounting. When Congress has allowed certain tax benefits, such as faster depreciation write-offs for tax purposes than the deciders of GAAP allow, these differences create accelerated expense write-offs and lower (than GAAP) taxable income in early years. The tax deferral is from a GAAP standpoint only — the company has paid the proper tax according to tax law. The theory is that eventually these timing differences between tax law and GAAP will reverse, and in later years this deferred tax liability will be paid back when GAAP catches up to reality. During the past few years, Congress has been trying to stimulate capital investment, and depreciation allowances have become increasingly accelerated and liberal, which has caused many companies to record larger and larger deferred tax liabilities. If the company continues to grow and replace assets, or if Congress continues to tinker with tax law, or if the company becomes

continued on page 8

Michael Goldman, MBA, CPA, CVA, CFE, CFF, is principal of Michael Goldman and Associates, LLC in Deerfield, IL. His qualifications include Insolvency, Financing, Planning, Turnaround Management and Business Valuation. He may be reached at michaelgoldman@mindspring.com.

Liabilities

continued from page 7

insolvent, these "liabilities" may never actually be "paid back."

Pension Plan and Retirement

Pension plan and retirement liabilities used to receive little attention, but have been very prominent in the news during the current economic cycle. These obligations were a major component of the General Motors and Chrysler bankruptcies, and so politically sensitive that the government strong-armed secured creditors to elevate these liabilities to a much higher priority than the bankruptcy code typically provides for them. The liability shown on the balance sheet represents the unfunded amount of what an actuary has determined is the company's obligation. Governments, which generally do not follow GAAP, swept these obligations under the rug for a long time and seem to have all suddenly realized that they exist, they are huge, and they need to be dealt with.

Companies often record liabilities in the anticipation of incurring costs. For example, if a company plans a plant closure, the sale of a division at a loss, or a mass layoff, it may record a liability for what it expects the costs of those future actions to be. Some companies recorded huge liabilities when "Obamacare" was passed in 2010, even though the costs of that legislation are not expected to become actual cash outflows until 2014 and beyond. Remember one of the cardinal rules: Debits have to equal credits, and the corollary is that for every debit there is an equal and offsetting credit. The recording of these liabilities has as its equal offset a charge to the income statement that correspondingly reduces reported net income.

Contingent Liabilities

Contingent liabilities may or may not develop into real liabilities, depending on which side has the better lawyer. In addition to lawsuits, contingent liabilities can also arise from warranty obligations, noncompliance with government regulations, accidents, or self-insurance programs. If the impairment of an asset or incurrence of a liability is "probable" and the amount can be "reasonably estimated," then this will be reflected on the balance sheet and income statement as a known item. If the contingent liability is only "reasonably possible" or the amount cannot be "reasonably estimated," then the contingency gets disclosed in the footnotes to the financial statements, but does not appear on the financial statements themselves. "Reasonableness" is in the eye of the beholder, or in this case, of the accountant.

Transfer of Non-Current Assets

In the weird and wacky world of accounting, a liability that will be satisfied in the very near future (within 12 months) with the transfer of noncurrent assets is not considered a current liability. For example, if you had 10 years left on your mortgage, typically the principle that would be paid in the next 12 months is "current," and the rest of the principle is "long-term." However, if you were in default and the entire mortgage was subject to acceleration, the entire mortgage would be shown as "current" whether the lender had actually accelerated it or not. On the other hand, if your plan is to satisfy the mortgage in full by giving the building back to the bank, since the building is a fixed asset, none of the mortgage is considered "current."

Legally Enforceable Debt

The fact that a liability appears on the balance sheet does not mean that it is a legally enforceable debt, or that it will liquidated for the amount shown on the financial statements. For example, a liability for repairs under warranty is not an actual debt to an actual customer — it is an estimate based on historical patterns of what product returns may be. At the time warranty costs and liabilities are recorded, it is not known which customers, if any, may be bringing a product back to the company. If product quality has increased or decreased, or customers have gotten more or less finicky, the real obligation for warranty repairs may be significantly less than or greater than what is recorded on the balance sheet.

Similarly, changes in market conditions from what the actuary used in the pension plan assumptions (such as interest rates being 1% instead of 8%) can significantly change the pension liability shown on the balance sheet.

Conclusion

Liabilities are subject to courts, negotiation, commercial practices, and economic reality. The old saying that "nothing is certain except for death and taxes" is for the most part true, except that in today's political environment there is less and less certainty regarding what tax policy will be. Accountants do their best in all this to record and classify liabilities as they expect them to be paid. Some liabilities are more certain than others, but at the end of the day, the only way to truly know what the amount and terms of an obligation were is when the check that satisfies that obligation clears the bank.

—❖—

ZIP Codes

continued from page 6

the hands of identity thieves. As a word of caution, the FTC was quick to point out that this latest action was "part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers' personal data." *See* http://1.usa.gov/1hWe2ss.

Conclusion

Although data privacy exposure is a rapidly evolving field, what should be clear is enterprising plaintiffs' attorneys are likely to challenge the practice of ZIP code collection through alternative avenues — whether under the state's broader consumer protection statute or through some other yet-to-be-seen theory. Given the latest trend in consumer privacy litigation along with the possibility for heightened government scrutiny, corporate counsel should be mindful of statutory and decision law developments in each state where they

continued on page 12

Same-Sex Benenfits

continued from page 1

That reach, however, is vitally important for employers and employees, especially considering that "marriage" pervades federal statutes and regulations (upwards of 1,000 federal benefits and burdens are keyed to marital status). The impact of the *Windsor* decision on same-sex married couples in areas including social security, housing, and employment has yet to unfold, and federal agencies have just begun the massive undertaking of determining how the *Windsor* decision impacts their own rules and regulations.

What Employers Should Know

A fundamental question *Windsor* left open is whether a couple validly married in a state that recognizes same-sex marriage but residing in another state will be considered married for federal purposes. This question has been answered, at least for federal tax purposes, by a highly anticipated IRS Revenue Ruling. In Revenue Ruling 2013-17 (issued Aug. 29, 2013) the Service ruled broadly in favor of recognizing same-sex marriages.

The Revenue Ruling explicitly provides that all marriages — regardless of the sex or gender of the individuals who are married — are accorded all of the same federal tax benefits. Most significantly, the Ruling specifies that a marriage is defined by the jurisdiction where it is celebrated, not the couple's state of residence. This is referred to as the "state of celebration" rule, in contrast to a "state of residence" rule. Therefore, the IRS will recognize the marriages of couples even in states that do not recognize same-sex marriage so long as the marriage was legally contracted in another state or foreign jurisdiction. (We note that the IRS's guidance in Rev. Ruling 2013-17 is in tension with federal regulations applicable to the Family Medical Leave Act (FMLA).

In 29 C.F.R. § 825.122, "spouse" is defined as "a husband or wife as defined or recognized under State law for purposes of marriage *in the State where the employee resides*, including common law marriage in States where it is recognized." (Emphasis added). In a post-*Windsor* Fact Sheet, the Department of Labor (DOL) reiterated this definition without discussing its continuing vitality in light of *Windsor*. However, the DOL's Technical Release No. 2013-04, dated Sept. 18, 2013, expressly adopts the state of celebration rule for employee benefit plans, leading to predictions that the DOL may reverse course on the FMLA definition in time.

Federal Taxes

In addition to embracing the state of celebration rule, Rev. Ruling 2013-17 also provides that same-sex couples will be treated as married for all federal tax purposes, including income, gift, and estate taxes. Married same-sex couples now enjoy the benefits, and in some cases burdens, of marriage for all federal tax purposes. As one important example, same-sex couples are now entitled to file their returns jointly, or they may elect to use the married filing separately status. Same-sex couples are no longer permitted to file singly and in most cases they no longer have the option of filing using "head of household" status.

Some couples will find that their new joint filing status will result in a larger tax burden because of the marriage penalty, while other couples will see their tax liability reduced; all couples in recognizing states will find their tax compliance burden lightened. For many couples, however, the intangible value in being able to check "married" on the federal form might well be the most meaningful consequence of the Ruling.

Health Insurance

The benefit of providing such benefits tax-free is best illustrated by looking at health insurance, which is one area that has caused considerable trouble to employers and employees alike. Same-sex couples now have the ability to insure their spouses through employer-provided health insurance without being made to include the value of that insurance in their income. The Revenue Ruling addresses in summary fashion employer-provided health coverage benefits as well as fringe benefits provided under sections 106 (accident and health plans); 117(d) (qualified tuition reduction); 119 (meals and lodging); 129 (dependent care assistance programs); 132 (excluding value of various fringe benefits including de minimus and employee discounts). Additional guidance has subsequently been provided in the form of a Q&A, as well as Notice 2013-61.

Typically, health insurance is a significant benefit that is not taxable to the employee. For married couples, employer-provided insurance coverage for the employee's spouse is also tax-free. However, under DOMA, this was not a tax-free event for same-sex couples. Specifically, employees who received coverage for their same-sex spouses were treated as receiving income in an amount equivalent to the amount of the benefit — this is often referred to as "imputed income." For example, if an employee received health coverage for herself and her same-sex spouse, and the value of the spousal coverage was $1,000 per year, the employee would have an additional $1,000 of taxable income.

This "imputed income" could result in significant tax liability for the employee, but no additional actual income with which to satisfy the tax liability. This hardship led some employers to offer what has been coined the "gay gross-up." These employers compensated LGBT employees at a higher rate to account for the imputed income. In other words, the employer "grossed up" the employee's income to cover, or at least mitigate, the additional tax the employee faced. Immediately post-*Windsor*, employers lacked guidance on whether they should continue imputing income for the cost of coverage — Revenue Ruling 2013-17

continued on page 10

Sarah Riskin is an attorney with Nilan Johnson Lewis in Minneapolis. **Morgan Holcomb** is Associate Dean and Associate Professor at Hamline University School of Law. Reach them at sriskin@nilanjohnson.com and mholcomb01@hamline.edu, respectively.

Same-Sex Benenfits

continued from page 9

relegates imputed income (for these purposes, at any rate) to history.

Social Security and Medicare Taxes

The Ruling and subsequent guidance also clarify that employees and employers have the option to amend three years' worth of returns or otherwise claim refunds for inclusion of imputed income (for employees) and overpayment of Social Security taxes and Medicare taxes paid on benefits (for employers). In conjunction with the Service's adoption of the state of celebration test, the ability to amend reaches to couples in states that did not in previous years (and do not currently) recognize same-sex marriage, provided the couples were lawfully married in another jurisdiction at the time.

With this IRS Revenue Ruling, which took effect Sept. 16, 2013, employers have initial guidance on how to treat the taxation of employee benefits. Employers with employees in multiple states particularly stand to benefit from these administrative explanations, as they can implement universal federal tax policies applicable to every employee, regardless of residence. Employers should discontinue the practice of imputing income to those employees who cover their same-sex spouses on health insurance plans and the employees' benefits should otherwise be administered the same as those benefits of employees in opposite-sex marriages. Further, employers should apply these federal rules across the board, regardless of jurisdiction.

Analysis

By applying the "state of celebration" test, rather than a "state of residency test," the IRS has started a slow (or perhaps it's actually a lightning-fast) crawl toward full federal recognition of marriage equality. For instance, under the Ruling, a couple that lives in Alabama is now free to marry in Minnesota, where same-sex marriage became legal on Aug. 1, 2013, and enjoy a full panoply of federal tax benefits back home.

The Service justified its decision by the necessity of uniformity, and certainly the decision is beneficial for the administration of federal benefits. As the DOL described in its Sept. 18, 2013, Technical Release, adopting the state of residency test would have required employers to track, at all times, both the employee's and the employee's spouse's state of domicile to determine whether the marriage would be recognized to properly administer benefits. By adopting the state of celebration test, the agencies were hoping to reduce the employers' burden in this way.

However, in some ways, the agencies' objective to reduce administrative burdens has failed. Prior to *Windsor*, employers in the states that recognized same-sex marriage had a two-track system where employees were considered married under state law but not for federal law. But what was a headache for employers and individual taxpayers in the small number of states with marriage equality has now become a headache in the remaining 37 states. Now, in the majority of the country, employers have (or at least have the potential to have) employees who

continued on page 12

Privilege Waiver

continued from page 4

recognition that the parties have a common interest in the outcome of the litigation. It is easier to argue that a claim-holder has a reasonable expectation that sensitive information will not be disclosed if there is a supporting agreement.

Third, a party should plan that information shared with an investor is information that would be responsive to a fact discovery request in litigation. Underlying factual information cannot be shielded from an adverse party. It is likely that the adverse party will at least ask for any factual information that formed that basis of the investing relationship. Thus, a party's written communications accompanying disclosures to an investor should be sensitive to this issue. The communications may also be subject to production.

Fourth, if a party is sharing information with an investor, and before any investment agreement is reached (potentially the most risky of positions), limit disclosures to necessary information. Limit or altogether avoid casual electronic communications and other writings about the disclosed information. These casual communications may be produced in later litigation, and such communications may be used and misinterpreted by an adverse party.

Fifth, assume that any attorney-associated information that is shared with an investor may at least be seen by a judge. An aggressive opponent will challenge privilege claims by a motion to the court. The party asserting privilege has the burden to establish that the communication is privileged. To resolve the challenge the judge may examine each document individually to evaluate if the document contains privileged information, or if the document must be produced. Regardless of whether the privilege challenge is successful, the information may still influence the evaluating judge. This influence may not be beneficial to the privilege-claiming party as the case progresses, or it may leave the court with the desire to level the field on a different motion.

Conclusion

The task of obtaining third-party litigation funding presents unique privilege preservation issues to a claim-holder when sharing information with an investor. Through some simple steps, however, the claim-holder may mitigate the risk of an unintended waiver. Privilege preservation is only one of several related challenges in third-party funding relationships. Other challenges are also present, including attorney representation ethics and practical management of client/investor relationships. Claim-holders should address these challenges with advanced planning and attorney consultation.

—❖—

Trade Secrets

continued from page 2

the company's interests, can also be used to divert information and customers once the employee resigns.

By allowing employees to link in with customers or other confidential contacts, the company may be destroying the legal protection afforded this information. This is a particular challenge with regard to customer and prospect information. While companies want their employees to be able to communicate with customers through increasingly popular social media sites, they also have a legal obligation to protect the confidentiality of that customer information. As discussed above, if a company wants its confidential information to be protected when an employee leaves, it needs to show that the information was not publicly available and that it took steps to keep the information private. If an employee posts customer names and other information on a social media site, a court could conclude that the information was publicly available — even if only a limited number of people could view the information. If the court concludes that the company put the information in the public domain or failed to take steps to protect the confidentiality of the information, it may decide that the information was no longer confidential or entitled to trade secret protection.

Social media sites can also enable employees to thwart contract provisions that prevent them from initiating contact with, or soliciting customers when they resign. Many companies take great pains to implement employment agreements that contain these types of restrictive covenants. However, if the company has permitted the employee to link in with customers during his employment, the employee simply has to update some aspect of his profile, such as his employment, and each of his contacts will get an automatic notification that the employee has updated that information and the new information will be provided.

The employee can then continue to ping customers by tweaking different aspects of his profile, causing additional notifications to be sent to the company's customers each time he does so. Courts are facing an increasing number of lawsuits alleging that an employee's communication with a contact on a social media site was a solicitation. At least one court has indicated that if a company wants to prevent that type of conduct, it should provide a definition of "solicit" that specifically includes that type of activity. *Enhanced Network Solutions Group, Inc. v. Hypersonic Technologies Corp.*, 951 N.E.2d 265 at fn. 1 (Ind. Ct. App. 2011).

Some of these matters may be resolved through a thorough and well-promulgated social media policy that discusses the use of confidential information on social media sites, what social media can be used by employees, who they can link in with, and what happens to those connections once they resign. Designing a social media policy is not easy because employers need to navigate the National Labor Relations Act (NLRA) to make sure that their policy does not run afoul of an employee's Section 7 right to engage in concerted protected activity. Concerted protected activity extends protection to all employees (whether union or non-union) to band together for "mutual aid or protection." Section 7 is designed to ensure that employees can share concerns over common employment terms and conditions. Many companies make sweeping proclamations in their social media policies, which can make that policy run counter to Section 7. For example, the National Labor Relations Board invalidated a company policy that prohibited any posts that damage the company, its reputation, or defamed an individual, concluding that it was an overly broad restriction on employees' Section 7 rights. *See Costco Wholesale Corp.*, 358 NLRB No. 106.

Employers need to implement social medial policies that ensure that confidential information remains confidential while at the same time not running afoul of employee rights. Some of the provisions that employers can consider adding to their social media policies include: 1) Specifying that login and passcode information on sites used for business purposes are owned by the employer and must be disclosed to the employer; 2) Explaining that the company will monitor activity on social media sites that are used for business purposes; 3) Confirming that information regarding customers, prospective customers, vendor contact information and whatever other connections the company considers confidential are owned by the company; 4) Ensuring that social media information is specifically included as part of confidential information that is protected by any confidentiality or non-disclosure policies; 5) Limiting the information that can be posted on these sites (again while making sure not to violate the NLRA); 6) Requiring employees to set their social media sites to private so that their connections cannot view each other; and 7) Specifically stating that if an employee chooses to connect with customers or other confidential connections, he must either disconnect from those connections following termination of employment, or not update his profile if he does not remove confidential connections.

The last item above raises two issues. First, if the employee disconnects from an individual, some social media sites will automatically send a notification to that person stating that the connection has been terminated. This could cause the customer to call the employee to find out why their connection was terminated. If the customer calls the employee, a court may conclude that the employee is then free to talk to the customer about their new venture — thereby skirting any non-solicitation restrictions. Alternatively, if the company does not require the employee to terminate those confidential connections, then they still have access to the customer's information and it can be difficult to monitor whether they use that information in their new role. Companies need to consider which approach is best for their situation.

continued on page 12

Trade Secrets

continued from page 11

Crafting a social media policy that will protect your company's confidential information and limit communications with customers will likely be one of the most important steps that the company takes to protect itself, as the Internet and social media redefine how companies do business.

MONITOR EMPLOYEES AND CONDUCT EXIT INTERVIEWS

If the company suspects that an employee might be planning to resign, it should not wait to begin monitoring her activities. By monitoring an employee before she departs, a company can learn about activities that may be harder to detect after she leaves. For example, if employees begin printing excessive information or start carrying laptops into the office, those actions could raise red flags the company will want to ask about if the employee in fact resigns. If the company is aware that an employee is interviewing with a competitor or seems to be unhappy at the company, new technologies can allow the company to track the employee's digital activities. Software is available to record everything that occurs on company devices and provide reports on unusual activity, such as data transfers.

When employees do resign, management should conduct an exit interview to learn about the employees' new position and to remind them of their obligation to maintain the confidentiality of company information. Management should ask the employee where he is going, and what position he will be in at the new company. The employee should also be questioned about any company information he has in his possession, and be asked to immediately return it. If the employee had access to valuable company information, or there is a question about whether the employee has possession of that information, the company may want to require the employee to sign off on a statement that all information has been returned.

At the conclusion of the exit interview, the employee should be provided with either the confidentiality agreement that she signed, or a sample of the company's policy so that she is aware of her obligations. Departing employees should be told that the company expects full compliance with the agreement, and be reminded that the agreement requires employees to return all company property and information. Once the exit interview has finished, the employee should be escorted out of the office to make sure he does not take any company information.

Finally, management should quickly act to terminate the employee's access to company systems. Most businesses know to terminate the employee's access to their network and e-mail accounts. However, consider other places where the employee may be able to obtain information. For example, does the employee have a remote access connection that needs to be terminated? Also check their phone lines to see if they have changed their message to direct customers to call their new firms. Make sure that the password is changed on any phone line so that the employee cannot call in and obtain messages from the company's customers.

CONCLUSION

By following the steps outlined above, companies can take greater control over information that could be devastating in the hands of a competitor. Management should meet with their technology and legal advisers to determine what is both possible and practical in deciding whether to institute some or all of these measures.

—❖—

Same-Sex Benenfits

continued from page 10

are married under federal law but not under state law. Employers still have to maintain a two-track system.

Regardless, employers should take measures to ensure that they properly implement these changes. If heterosexual employees are not required to show a valid marriage certificate, neither should LGBT employees.

Employers should also be sensitive to the very real possibility that they have some employees who have never shared their sexual orientation at work, but who may be faced with disclosing their newly recognized marital status. Employers should train their Human Resources and other professionals accordingly.

CONCLUSION

The *Windsor* decision has far-reaching implications, many of which are yet to be known. The IRS specifically noted that it intends to issue further guidance on the retroactive application of the *Windsor* decision to other employee benefits and employee benefit plans and arrangements, so individuals and companies should stay tuned for more.

—❖—

ZIP Codes

continued from page 8

conduct business to ensure that they have taken the necessary steps to demonstrate compliance when collecting ZIP code information.

Beyond just ZIP codes, these developments should encourage corporate counsel to conduct internal reviews and assess the various kinds of data they collect, how they collect such data, and what they ultimately do with it. Given the potential exposure flowing the seemingly innocuous collection of a customer's ZIP code, you never know where the next point of exposure may lie.

—❖—