

Monitoring the Virtual Water Cooler: Facebook and Beyond

National Public Radio recently aired a story about how employees working at IBM feel compelled to have a Facebook page. It's not just the newly-minted, tech-savvy, twenty-somethings indulging in social media on company time, either. The report stated that management "all the way up the chain" is on Facebook. With the fastest growing demographic of Facebook reportedly being users over age 35, IBM is clearly not the only company employing growing throngs of Facebook loyalists.

According to the NPR story, IBM is in the minority of businesses that have a social media culture and actually encourage their employees to use sites like Facebook during working hours to build professional networks and exchange business ideas. Instead, more than half of all U.S. companies prohibit the use of such sites at the office. One criticism of the policies banning the use of social media in the workplace is that these sites are merely the next generation of water cooler chit-chat, and companies shouldn't ban the "new age" water cooler just because the employers are afraid of it or don't understand it.

However, while social media sites can create positive networks and foster a sense of community and camaraderie among employees, such sites can also create real headaches for employers. What do you do as an employer when you learn too much about some of your employees?

Take, for example, a recent lawsuit in New Jersey federal district court against Houston's Restaurant in Hackensack, New Jersey. An employee there created a workplace

Odds are good that many forms of social media are already thriving in your workplace. As an employer in the 21st century, it is best to make a conscious decision about how to address these issues with your employees, and proactively develop a policy rather than get stuck doing damage control.

discussion group on his personal MySpace Web page. The discussion group was flagged "private" and was available by invitation only. One member of the group, a hostess at Houston's, showed the private MySpace discussion group to a Houston's manager. Other management soon became aware of the group and asked the hostess to provide her sign-in information, which she did. Management was not pleased when it saw that the discussion group included sexual comments about employees and customers, disparaging jokes about the company, and references to drugs and violence. The restaurant fired both the creator of the MySpace discussion group and a contributing employee. The terminated employees sued, claiming, among other things, that the company violated the federal Stored Communications Act and invaded their privacy. The restaurant claimed it had no liability because the hostess voluntarily consented to Houston's management accessing her private account for the online discussion group. The plaintiffs contended that the hostess was coerced into providing the information, fearing discipline if she did not cooperate.

The jury returned a verdict in favor of the plaintiffs on both the federal Stored Communications Act claim as well as the claims for invasion of privacy. The Houston case presents some unique facts, with a dispute over whether an employee was coerced into providing her log-in information. Although some states have specific

in this issue

- 1 **Monitoring the Virtual Water Cooler: Facebook and Beyond**
- 2 **The FTC Red Flags Rule: Temporary Reprieve but No Exception (Yet) for Service Providers**
- 6 **Whoops, We Lost Your Employees' Social Security Numbers**
- 8 **EFCOA's 'Card Check' Provision is Dropped, but Employers Should Not Drop Their Guard**

statutes regarding employee privacy and off duty conduct, generally speaking, nothing would prohibit employers from taking adverse employment action against at-will employees for this type of online conduct. With so many employees using these sites, it is likely that some employees will invite management to join their Facebook pages or blogs – perhaps without realizing the full consequences. Suppose if instead of making some disparaging jokes about the company, an employee posts explicit pictures from her moonlighting as an exotic dancer, or uses his or her Facebook page to tout Neo-Nazi sentiments or white supremacist ideas? Might the manager be inclined to terminate the part-time stripper on the basis of those pictures? Would the employer arguably be obliged to terminate the Neo-Nazi once it is aware of the employee's racist and violent views?

Before your company crafts its policy on social networking, consider if your business is in a heavily regulated industry (such as pharmaceuticals) or an industry that requires a particularly high level of confidentiality. The added legal complexities in those industries may weigh in favor of being extremely cautious about embracing social media as a company culture. If you do decide to foster a culture of social media in the office, at a minimum, you should make clear to all employees that they have a duty not to disclose confidential company information or trade secrets, including on any social networking site they may deem to be “personal.” It may also be wise to warn employees that they cannot defame the company or its employees. Be clear that any violation of the policy will result in discipline – up to and including immediate termination.

The lines between personal space and the workplace continue to blur. Odds are good that many forms of social media, such as Facebook and Twitter, are already thriving in your workplace. Who knows what technology is next? The way employers are choosing to respond to these technologies continues to evolve, and the laws certainly cannot keep pace. As an employer in the 21st century, it is best to make a conscious decision about how to address these issues with your employees, and proactively develop a policy rather than get stuck doing damage control – and perhaps become the latest talk heard ‘round the virtual water cooler.

Author:

*Heather A. Hoyt
610.640.7833
hoyth@pepperlaw.com*

The FTC Red Flags Rule: Temporary Reprieve but No Exception (Yet) for Service Providers

Many consumers and businesses face the problem of financial identity theft – the theft of identifying information, which is then used to open new accounts or misuse existing accounts. Medical identity theft causes not only financial difficulties but has the potential to cause physical harm to its victims. As described by the World Privacy Forum:

Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity – such as insurance information – without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.

Regulations, jointly issued by the Federal Trade Commission (FTC) and five other federal financial and banking oversight agencies (collectively, the “agencies”), require financial institutions and creditors with covered accounts to develop and implement a written Identity Theft Prevention Program (Program). The Program must include policies and procedures to detect patterns, practices or specific activities that indicate the possible existence of identity theft, otherwise known as Red Flags.

The regulations referred to as the Red Flags Rule were issued on November 9, 2007 (72 Federal Register 63718 accessible at <http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf>), and were promulgated under the authority of the Fair and Accurate Credit Transactions Act of 2003, which amended the Fair Credit Reporting Act. While they have not received as much attention as the Program requirements, the Red Flags Rule includes two other sets of regulations beyond the scope of this article: (1) requirements for credit and debit card issuers to assess the validity of change of address notifications,

and (2) guidance on policies and procedures for users of consumer reports when receiving a notice of address discrepancy from a consumer reporting agency.

Who Must Implement an Identity Theft Prevention Program?

Although the Red Flags Rule was issued a year-and-a-half ago, many service providers (including health care providers) only recently realized that these regulations apply beyond the financial sector. These regulations apply to service providers and institutions through the broad definitions of “creditor” and “covered account” adopted in the Red Flags Rule. The rule’s requirement to develop and implement the written Program applies to financial institutions and creditors that offer or maintain covered accounts. In determining whether the Red Flags Rule applies, service providers and institutions must conduct a two-step analysis that determines (1) if the provider is a financial institution or a creditor, and (2) if the provider offers or maintains covered accounts. If both answers are yes, the provider is required to develop and implement a Program and otherwise comply with the requirements of the Red Flags Rule.

Step One: Are You a ‘Financial Institution’ or a ‘Creditor?’

Most service providers (including health care providers) and institutions will not fit into the definition of a “financial institution,” which includes banks, savings and loan associations, mutual savings banks, credit unions and certain other lenders. However, the broad definitions of “creditor” and “credit” likely capture many service providers.

Creditor is defined to include:

- any person who regularly extends, renews or continues credit
- or any person who regularly arranges for the extension, renewal or continuation of credit
- or any assignee of an original creditor who participates in the decision to extend, renew or continue credit.

Credit means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment.

On July 29, 2009, the FTC announced its third enforcement delay until November 1, 2009. In its latest press release, the FTC committed to “redouble” its efforts to educate and assist small businesses and other entities about compliance with the Red Flags Rule.

The Red Flags Rule specifically refers to banks, finance companies, automobile dealers, mortgage brokers, utility companies and telecommunications companies. There are few references, or discussion of the rules’ applicability, to professional service providers. For example, although health care providers are not included in the list, and medical identity theft is mentioned only one time in the more than 50 pages of regulations and related discussion, these broad definitions appear to include any entities that provide services or products that are not paid for in full at the time the product is provided or the service is performed. As typical health care billing practices include billing insurers before billing patients, setting up payment plans and not collecting payment at the time of service, many health care providers will realize that they are creditors under this broad definition. Similarly, billing practices for other types of service providers may cause them to be creditors under the Red Flags Rule.

Step Two: Do You Maintain ‘Covered Accounts?’

Even if a service provider is a creditor, the analysis is not complete until the provider determines whether or not it maintains covered accounts. An account is a continuing relationship between a creditor and a person to obtain a product or service for personal, family, household or business purposes. Accounts include extensions of credit (like purchasing property or services using a deferred payment) and deposit accounts. A covered account is either:

- (i) an account that a financial institution or creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account or savings account, or

(ii) any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

For example, financial and billing accounts maintained by many health care providers permitting multiple payments will cause health care providers to be considered creditors maintaining covered accounts. A question remains whether medical records will fall under this definition, but current thinking suggests that medical records would only be considered covered accounts if they are combined with financial accounts.

Note that the Red Flags Rule requires each creditor to “periodically” determine whether it offers or maintains covered accounts. This determination is to include a risk assessment taking into account (1) the methods the creditor provides to open accounts, (2) the methods it provides to access accounts and (3) previous experience with identity theft. Even if a creditor initially determines that it does not have or maintain covered accounts (and therefore is not required to develop a Program), the Red Flags Rule requires the creditor to periodically reassess this determination.

Establishing an Identity Theft Prevention Program

Creditors who offer or maintain covered accounts must develop and implement a written Program. The Red Flags Rule specifically provides that the Program must be appropriate to the size of the creditor. In the preamble to the final rules, the agencies note that the rules are designed to provide flexibility for the entities developing and implementing the Program. When implementing a Program, creditors are required to consider the guidelines attached as Appendix A to the final FTC regulations (Guidelines) and include in their Program those Guidelines that are appropriate. The Guidelines elaborate on the required Program elements and the administrative requirements.

Program Core Elements

When developing a Program, service providers and institutions should integrate, as applicable, HIPAA privacy and security compliance programs and other identity theft policies and procedures already in place. Each Program also

must include reasonable policies and procedures on these four required elements:

1. *Identifying Red Flags.* Creditors are required to identify Red Flags for their covered accounts and incorporate those flags into the Program. In identifying flags, the FTC Guidelines list four risk factors that should be considered: the types of covered accounts the creditor offers or maintains, the methods the creditor provides to open and access its covered accounts and the creditor’s previous experience with identity theft. In a supplement appended to the Guidelines, the FTC includes 26 examples of Red Flags organized into these five categories:

- alerts, notifications or warnings from a consumer reporting agency, such as a fraud alert included in a consumer report or a notice of credit freeze
- presentation of suspicious documents, such as a forged driver’s license or health insurance card, or if the information on the identification card is inconsistent with information provided by the person presenting the identification or with information readily accessible by the creditor
- presentation of suspicious personal identifying information, such as a Social Security number or insurance number that is the same as one submitted by other persons opening accounts, or the person opening an account fails to provide all of the required personal identifying information (e.g., the person provides a health insurance number but no card)
- suspicious activity on an account, such as unusual billing patterns, the patient notifies the provider that it is not receiving account statements, or records showing that medical treatment is inconsistent with patient’s medical history
- notice from the patient, law enforcement or others about possible identity theft.

In identifying other Red Flags specific to a particular service provider, creditors and institutions should consult materials and guidance prepared by trade organizations and professional organizations focused on the problems of identity theft in the provider’s industry.

2. *Detecting Red Flags.* Policies and procedures implemented through the Program should address detecting Red Flags both in connection with opening new covered accounts and maintaining existing covered accounts. The Guidelines provide some examples of detection, such as by verifying the identity of individuals

opening covered accounts and authenticating customers and monitoring transactions.

3. *Responding to Red Flags.* A critical element of any Program will be the creditor's response policies and procedures regarding the detected Red Flags. The regulations require an "appropriate" response to prevent and mitigate identity theft. In the Guidelines, the agencies note that the determination of an appropriate response should consider various aggravating factors that could heighten the risk of identity theft. The Guidelines also note, in a non-exclusive list of 10 possible responses, that no response may be warranted.

4. *Periodic Updating.* Effective Programs, to reflect changes in risks to patients and to the safety and soundness of the creditor against identity theft, must include procedures for periodic updates, including re-determinations of which Red Flags are relevant.

Program Administrative Elements

In addition to the four core elements, the Red Flags Rule includes requirements for Program administration:

1. *Program Approval.* The initial written Program must be approved by either the company's Board of Directors or an appropriate committee of the Board of Directors.

2. *Program Oversight.* The board, an appropriate committee or a designated member of senior management of the company must be involved in the oversight, development, implementation and administration of the Program. Oversight activities include assigning responsibility for Program implementation, reviewing staff reports regarding compliance with the Red Flags Rule and approving material changes to the Program. Note that if oversight activities are delegated to senior management, material changes to the Program would not need to be approved by the board (or applicable board committee).

3. *Training.* The creditor must train staff, as necessary, to implement the Program. For a Program to be successful, the company's employees and staff will be instrumental in detecting and responding to Red Flags, thereby preventing and mitigating identity theft. A well-designed Program will be useless if company personnel are unfamiliar with the company's identified risk areas and/or the policies and procedures adopted to detect and respond to the Red Flags.

The FTC released an interactive template intended to help covered entities with a low risk for identify theft to comply with the Red Flags Rule and to develop an identity theft prevention program.

4. *Oversight of Service Providers.* The Red Flags Rule also requires that covered entities exercise "appropriate and effective oversight" of those who provide services in connection with covered accounts. While creditors can require service providers to comply with their Program (such as through the service agreement or a business associate agreement), the agencies note in the preamble that if the service provider has adopted its own identity theft program it can follow that program, if it meets the requirements of the Red Flags Rule.

Compliance and the FTC's Enforcement Delays

The Red Flags Rule was effective on January 1, 2008, but the mandatory compliance date was set for November 1, 2008 because the agencies recognized that some covered entities would require more time to respond to the rule. Two weeks before the compliance deadline, on October 22, 2008, the FTC suspended enforcement of portions of the Red Flags Rule until May 1, 2009, in order to provide additional time for covered entities to develop and implement their Programs. In announcing the six-month delay the FTC explained that it decided to grant the delay after learning, through their outreach, that some industries were unaware of the rule's application. It is important to note that this delay only affects the FTC's own enforcement activities – creditors may have liability exposure if they are not yet complying with the Red Flags Rule's requirements.

On April 30, 2009, the FTC announced that it would again delay enforcement of the Red Flags Rule for an additional three months until August 1, 2009. In connection with the announcement of the second delay, FTC Chairman Jon Leibowitz said, "Given the ongoing debate about whether Congress wrote this provision too broadly, delaying enforcement of the Red Flags Rule will allow industries and associations to share guidance with

their members, provide low-risk entities an opportunity to use the template in developing their programs, and give Congress time to consider the issue further.”

Shortly after announcing the second enforcement delay, the FTC released a template program (available at <http://www2.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm>). The interactive template is intended to help covered entities with a low risk for identify theft to comply with the Red Flags Rule and to develop an identity theft prevention program.

On July 29, 2009, the FTC announced its third enforcement delay until November 1, 2009. In its latest press release, the FTC committed to “redouble” its efforts

to educate and assist small businesses and other entities about compliance with the Red Flags Rule.

It remains to be seen whether any modifications to the Red Flags Rule will materialize, either from the FTC or from Congress. In the meantime, it is advisable for service providers and institutions to continue (or begin) developing and implementing a written identity theft prevention program in time for the November 1, 2009 deadline.

Author:

*Rebekah A. Z. Monson
215.981.4031
monsonr@pepperlaw.com*

Whoops, We Lost Your Employees' Social Security Numbers

Imagine this — you've contracted with a vendor to enter your employees' personnel data into a new computer system. You give the vendor confidential information regarding your employees, including their Social Security numbers, addresses, names of dependents, health records, and bank account routing numbers. During its engagement, the vendor notifies you that much of your employee data in its custody was somehow stolen or lost from the vendor's facility. What do you do?

Unfortunately, this scenario is not uncommon. According to the Privacy Rights Clearinghouse (www.privacyrights.org), a nonprofit, consumer information and advocacy organization, more than 262 million records have been breached since January 2005. The Federal Trade Commission estimates that nine million Americans have their identities stolen each year (www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html). A class action complaint was recently filed in the United States District Court for the Eastern District of Pennsylvania (*Allison v. Aetna, Inc.* C.A. No. 2:09-2560) by employees and applicants of Aetna who allege that Aetna failed to adequately protect their personal information, which was stored on Aetna's Web site; the site was accessed by a computer hacker.

If your company is faced with this situation, you should consider taking the following steps:

Investigation. As soon as possible after the incident occurs, insist that a thorough investigation be conducted to determine what went wrong and whether the vendor was negligent in its management of the employee data or the security of its network or facilities. The investigation should be performed by an outside firm not connected to the vendor or to your company.

Notification of Employees. Most states, including Pennsylvania, have laws governing the form and type of notification that must be provided in the event of a security breach. In addition, the Health Information Technology for Economic and Clinical Health (HITECH) Act, signed into law on February 17 as part of the American Recovery and Reinvestment Act of 2009, established a federal rule for notification of security breaches involving personal health records. You should make sure that the vendor sends the legally required notifications to your employees. Consider sending a separate communication to the affected employees so that they know that you were not responsible for the breach and that you are taking steps to determine what happened.

When should employees be notified that their personal information has been taken? Normally, the best course is to tell the truth and tell it fast. In this context, however, there is a tension between sending a notification before there has been an opportunity to investigate and gather the relevant

data, which is likely to frustrate employees who want answers, and delaying notification, which also is likely to upset employees. The plaintiffs in the *Allison v. Aetna* case allege that Aetna was negligent in not timely disclosing the security breach at issue in that case. It is important to keep your employees informed about developments in the matter, and to be sensitive to their concerns about their missing information.

Actions Against Vendor. In a situation like that described above, where a third party is responsible for the data loss, what courses of action are available to an employer to protect its employees and itself?

- You should try to have the vendor agree to pay for any damages caused by the breach and to indemnify you and your employees in any legal action.
- You should also insist that the vendor cover the cost of providing identity theft protection for at least three years. According to a study by the General Accounting Office, stolen data may be held for a year or more before being used to commit identity theft, and could then be used for several years. There are several identity theft monitoring services that scrutinize the use of personal information and scan public databases and Internet sites to detect potential identity theft before it occurs. For example, identity theft monitoring services can determine whether individuals' credit cards or bank account numbers have been compromised.

Proactive Steps to Minimize Risk. Your contract with the vendor should include language that will minimize the risk of a data breach, as well as the risk of liability to you and harm to your employees if such a breach occurs. For example:

- You should obtain the vendor's contractual commitment to limit the number of individuals who will handle the data, to ensure that the data is encrypted, to maintain the data in a secured location, and to manage any transmission of the data in a controlled, protected manner. If your company has policies addressing data security, the contract should obligate the vendor to comply with those policies.
- The vendor contract should specify that the vendor will notify you of any data lost within a certain number of days, and should commit the vendor to comply with all applicable federal and state laws on notification of security breaches.

- The contract also should provide that the vendor is legally responsible for any data breach that occurs during its engagement, and that it will indemnify the employer and its employees for any actions arising from such a breach. Not surprisingly, vendors are often reluctant to include that type of language in their contracts. Employers who are tempted to sue the vendor for negligence or other causes of action should know that courts will often dismiss actions brought before the harm has occurred. In other words, it is difficult to pursue an action for potential identity theft.
- Ideally, the contract should obligate the vendor to pay any damages resulting from the data loss no matter when they occur.
- As more vendors perform services offshore, controlling risk becomes more difficult. Not only does that structure implicate international laws and enforcement practices, but it also presents practical difficulties in managing the security of remote data and understanding the ability to enforce security requirements in different countries. You should negotiate contract language that requires the vendor to obtain your approval before moving work offshore. Also, because offshore work is likely to be less costly for the vendor, you should seek the vendor's agreement to pass that cost savings on to you.

Federal Trade Commission Red Flags Rule. Employers and vendors also should be aware of their potential obligations to comply with the Red Flags Rule (<http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>). The rule is in effect, but the FTC has again delayed its enforcement until November 1, 2009. The rule requires "financial institutions" and "creditors" with "covered accounts" to develop and implement written identity theft prevention programs that will outline procedures to detect "red flags" suggesting the possible existence of identity theft. The rule applies to banks, credit unions and the like, as well as a broadly defined group of creditors, which includes entities that regularly defer payment for goods and services and bill customers later. Health care providers, utility companies and telecommunications companies likely fall within this definition.

Author:

Susan K. Lessack
610.640.7806
215.981.4569

lessacks@pepperlaw.com

EFCA's 'Card Check' Provision is Dropped, but Employers Should Not Drop Their Guard

The proposed Employee Free Choice Act (EFCA)'s "card check" proposal meant, until recently, that employees could organize into a labor union when a majority of the employees in a bargaining unit sign authorization forms, or cards, stating they wish to be represented by the union. Despite recent news reports that card check has been dropped from the EFCA to facilitate the 60 votes needed in the Senate to prevent a filibuster against the proposal, employers nevertheless need to remain or get prepared for the passage of this legislation.

The card-check provision was always intended as a Trojan Horse (see Pepper Hamilton's March 23, 2009 *Pepper@Work*). Part of the compromise that replaces card check includes three incredibly powerful proposals, which will dramatically increase unions' ability to win elections:

'Quick' Elections in Five to Ten Days. Because the union controls the timing, these will be very challenging to win; unprepared employers will not be successful.

Access to Employer's Property. This raises powerful private property issues, but the proverbial bottom line is to allow union access to the workplace. This validates the union, and allows the union to communicate a message that employers will find very difficult to respond to in light of the prohibitions against "promising."

Prohibition of 'Captive Audience' Speeches. First, never use the word "captive." Never allow the other side to imprint negative language on conduct. In any event, it is always recommended that attendance be voluntary, and that has worked well. However, it is not clear how this provision will read, or how the "new" Obama labor board will interpret and enforce it.

The key to union success is the quick elections. While powerful and attractive to unions, the "access to property" and "captive audience speech" proposals could well be trade-offs in negotiation in order for unions to retain the single most pernicious amendment – mandatory arbitration.

Mandatory arbitration remains in the proposed statute, and that is the most important component. Not only does

it mandate a contract, it totally changes the educational component of campaigns, and validates the union promise of "more." It is most threatening to employers with multiple facilities. The obvious union tactic is to organize one, obtain the mandatory contract, and then use that as an organizing tool elsewhere. There is no compromise to this proposal.

It is time for employers to conduct vulnerability assessments and take appropriate action so that there are no quick elections. The election timetable is, in effect, moved up, and employees must operate at all times in election mode. Essentially, what that means is that employers should create and maintain a pro-employee atmosphere. Everyone must believe in that, and embrace that behavior and those values.

It is hard to predict when this legislation may pass, but it is clearly coming soon.

Author:

*Jonathan Kane
610.640.7803
kanej@pepperlaw.com*

Pepper Hamilton LLP

Attorneys at Law

The material in this publication is based on laws, court decisions, administrative rulings and congressional materials, and should not be construed as legal advice or legal opinions on specific facts. The information in this publication is not intended to create, and the transmission and receipt of it does not constitute, a lawyer-client relationship.

Please send address corrections to phinfo@pepperlaw.com.

www.pepperlaw.com

Berwyn | Boston | Detroit | Harrisburg | New York | Orange County
Philadelphia | Pittsburgh | Princeton | Washington, D.C. | Wilmington

© 2009 Pepper Hamilton LLP. All Rights Reserved.
This publication may contain attorney advertising.