Cyberspace Law

Message from the Chair

Michael Fleming
Chair, Committee on Cyberspace Law

As we approach the second of our Committee's major meetings during the bar year, the Business Law Section's Spring Meeting, it seemed a good time to reassess the services we can provide to our committee members who, for whatever reason, are not always able to join us at the physical meetings.

Frankly, even as we get well into the twenty first century, and even for a bar group dedicated to the use of technology to communicate and do business, we still find that the face-to-face meeting is one of our most important means to generate enthusiasm and participation. I think of our Winter Working Meeting and its famously wonkish long sessions of friends talking deeply about the topics we love, the Spring meeting with its focus on the business of technology and the interplay with our Section's other committees, and the Annual meeting during the dog days of summer often accompanied by members' families finding a way for a vacation around the bar activities.

But, those of us who are fortunate enough to regularly attend the face-to-face meetings must not forget the nearly ninety percent of our membership that is not so lucky. The dictates of time in the practice of law make attendance difficult for some, and the costs of travel, especially in the recent economy, can be daunting. While we will still encourage those who can to join us, the committee needs to address the needs of those who cannot.

And, we are beginning to address those concerns, albeit in baby steps. This newsletter is one example—By going out to the entirety of the membership, we help to ensure that each of the members are up to date on the committee's activities, and offer a forum for members who would like to write short pieces for distribution to the committee and often to the Section as a whole.

The Committee's program work product over recent years can be found on the Section's web site—The organization and user interface could be a bit better, but the wealth of materials produced by our hard-working members and the guests we've invited to join our Programs continues to be the among the best of legal resources for Cyberspace Law issues. Our former chair Vince Polley produces a fantastic resource that he shares every few weeks with the entire committee membership—The MIRLN newsletter is a must read for all of us.

The Section is experimenting with tools for members to be able to participate remotely with those at the face-to-face meetings, such as webinar or other teleconferencing tools. We hope to have a more fleshed out description of what those tools will be in the coming months, and we will share what we know about them as the details become available.

We experiment with interactive tools and social media, sometimes on an unofficial basis and sometimes within tools being set up by the ABA such as the Legally Minded social networking tool. We Tweeted on Twitter about Winter Working Meeting 2009, and even dedicated a new 'hash tag' (#WWM09) just for our Twitter users to quickly find information about our meeting. And, we will continue to look for more tools to collaborate electronically with our members.

These baby steps are still not enough. The Committee, and bar associations in general, need to continue to look for new ways to maintain the presence of their members in a rapidly changing world. We believe this committee, with its mix of
smart technology users (dare we say - the legal geeks?), is well positioned to experiment with these ideas. More importantly, we are also well positioned to explain these tools to the other members of bar groups as well as the firms and institutions we work for. Lawyers are often the among the last to adopt to the changing technologies, but adopt we must—And will.

About the author: Michael F. Fleming is a shareholder at Larkin Hoffman Daly & Lindgren, Ltd., Minneapolis, Minnesota USA, where he practices in commercial and technology transactions, regulatory analysis and compliance, intellectual property and electronic commerce. He can be reached at mfleming@larkin hoffman.com.

Message from the Newsletter Director

Alan S. Wernick  
Newsletter Director

The Committee on Cyberspace Law explores a wide range of rapidly changing legal disciplines including electronic commerce and contracts, consumer protection, intellectual property, cyber security & privacy, jurisdiction, internet governance, and online financial activities. This CCL eNewsletter provides our members with an opportunity to help advance members’ awareness and understanding of these evolving and dynamic legal issues. Our goal is to make it a useful addition to your practice by helping to make you aware of some of the developments impacting your practice and your clients' businesses, and what these developments mean. This newsletter also serves as a virtual bulletin board of the many activities of the various CCL committees and sub-committees, so committee chairs are encourage to share the news about the interesting activities of your committee. Please contact me if you are interested in submitting short articles or committee news for publication in this eNewsletter, or if you have any constructive comments or suggestions concerning this newsletter. My e-mail is ALAN@WERNICK.COM.

Thanks to our contributors for this issue: Michael Fleming, Francoise Gilbert, Sarah Jane Hughes, and Phillip Schmandt.

An ABA Business Law Section Special Presentation - April 16, 2009, Vancouver, BC

The EU Payment Services Directive - What it Means for US and Canadian Businesses

The Banking Law, UCC, and Cyberspace Committees of the Business Section will host a special presentation entitled "The European Union's Payment Services Directive and What It Means for the United States and Canada" on Thursday, April 16, 2009, in connection with the Business Section's Spring Meeting in Vancouver, BC. The presentation will cover the European Union's Directive on Payment Services and the Single Euro Payments Area. The session will run from 10-11 a.m. PDT.
EU Commission Proposes New Rules Streamlining Use of Electronic Invoices in Europe
Phillip Schmandt

Overview

On 28 January 2009 the Commission of the European Union proposed an overhaul of the 2006 EU Directive on Invoicing (Directive 2006/112/EC). If approved, this new Directive will fundamentally change how electronic invoicing is conducted in Europe and will affect all companies doing business in Europe. Interested parties are invited to submit comments to these proposed changes no later than 13 March 2009.

The proposed new Directive would make electronic invoices equivalent in all respects to paper ones. It would introduce at least two major changes to existing e-Invoice practices: first, it would eliminate the requirement that advanced electronic signatures be used in electronic invoices. Second, it would eliminate the requirement that the recipient of the invoice consent to receive invoices in electronic form.

1 The proposed new Directive (and a link to the original Directive) is available at the following URL: http://ec.europa.eu/taxation_customs/taxation/vat/traders/invoicing_rules/index_en.htm

Bankruptcy and the Software License
Alan S. Wernick

Most companies have software they license for business critical applications. What happens to the business (licensee) if the licensor of the computer software enters bankruptcy? Does the business have to stop using the software altogether or have some restrictions applied to their use? Would the business suffer if it had to stop using any business critical computer programs they currently use? And, if the business fails to immediately stop using the software, will the bankruptcy trustee for the debtor/licensor pursue the business for infringement damages?

Both in good times and challenging economic times, bankruptcy is sometimes the "exit strategy" for some businesses, including software licensors. And, once the licensor's bankruptcy petition is filed, it will only be a matter of time before the licensees feel the impact of that filing.

What Limits For Behavioral Targeting?
Françoise Gilbert
An individual uses a travel site to check hotels in New York, but does not book any hotel room. Later the individual visits the website of a local newspaper to read about the Chicago Cubs baseball team. While on the newspaper's website, the individual is served an advertisement from an airline featuring flights from Chicago to New York. The method used to develop the consumer's profile - someone interested in travelling to New York from his home base in Chicago - in order to serve target ads is named "behavioral advertising" or "behavioral targeting."

More...

"Red Flags Rule" - Will You Be Compliant or Complacent?
Alan S. Wernick

The federal "Red Flags Rule" is designed to minimize identity theft. The failure of covered entities to comply can have several consequences, including civil penalties, injunctions, annual reporting, government oversight of the non-compliant business, and loss of trust by the customers of the business.

An amendment to the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") requires covered entities to create programs which must provide for the identification, detection, and response to patterns, practices, or specific activities - known as "red flags" - that could indicate identity theft. The Federal Trade Commission ("FTC"), the federal bank regulatory agencies (including the Office of the Comptroller of the Currency, the Federal Reserve, the Federal Deposit Insurance Program, and the Office of Thrift Supervision), and the National Credit Union Administration have issued regulations concerning this Red Flags Rule (the "Rule").

More...
The EU Payment Services Directive – What it Means for US and Canadian Businesses
An ABA Business Law Section Special Presentation – April 16, 2009, Vancouver, BC

The Banking Law, UCC, and Cyberspace Committees of the Business Section will host a special presentation entitled “The European Union’s Payment Services Directive and What It Means for the United States and Canada” on Thursday, April 16, 2009, in connection with the Business Section’s Spring Meeting in Vancouver, BC. The presentation will cover the European Union’s Directive on Payment Services and the Single Euro Payments Area. The session will run from 10-11 a.m. PDT.

The Directive on Payment Services, known by the acronym “PSD,” has multiple aims. Among these are:

- establishment of a “modern and comprehensive set of rules applicable to all payment services” in the European Union;
- facilitation of cross-border payments within the European Union that are “as easy, efficient, and secure” as “national payments” within a Member State;
- improvement of competition by opening up payments markets in the European Union to new entrants in order to foster greater efficiencies and cost reductions; and
- establishment of the necessary legal platform for the Single Euro Payments Area (SEPA).

The PSD contains numerous features of interest to payments and other transactional lawyers in the United States and Canada as well as those inside the European Union. These features include:

- regulation of cross-border payments in Euros in terms of
  - regulation of equality of charges for payments, and
  - regulation of information on the payer accompanying transfers of funds;
- e-invoicing pursuant to an interim report issued on January 27, 2009; and
- e-signatures and e-identification pursuant to an action plan approved on December 2, 2008.
This presentation will provide an overview of the PSD and SEPA and will highlight topics of concern to payments lawyers in the United States and Canada whose clients send and receive payments to Europe.

Attendees will hear a distinguished, multi-national panel of experts, including Tom Brown of O’Melveny & Myers (San Francisco), Robert Burns of MacRoberts LLP (Glasgow, Scotland), Joe Alexander of The Clearing House Association (New York City) whose expertise includes the Clearing House’s new International Payments Network, and Peter Moller Jensen of Visa Europe (Brussels) (invited but not confirmed as of February 27th). The panel organizers thank Lisa Lifshitz, Partner, Gowlings (Toronto) & Co-Vice Chair, Cyberspace Law Committee (lisa.lifshitz@gowlings.com), and Broox W. Peterson, Esq. (Sandwich, MA) & Member, Cyberspace Law Committee (broox@bwplawyer.com), for their assistance in recruiting Messrs. Brown, Burns, and Jensen to join us in Vancouver.

Please join us for what promises to be an exceptional panel on topics that relatively few US lawyers may have focused on and that presents a potential model for other cross-border payments.

Stephen T. Middlebrook & Sarah Jane Hughes
Co-Chairs, Electronic Payments & Financial Services
Cyberspace Law Committee

Sarah Howard Jenkins & Karen Nash-Goetz
Co-Chairs, UCC Payments Subcommittee
UCC Committee
EU Commission Proposes New Rules Streamlining Use of Electronic Invoices in Europe
By: Phillip Schmandt

Overview

On 28 January 2009 the Commission of the European Union proposed an overhaul of the 2006 EU Directive on Invoicing (Directive 2006/112/EC).1 If approved, this new Directive will fundamentally change how electronic invoicing is conducted in Europe and will affect all companies doing business in Europe. Interested parties are invited to submit comments to these proposed changes no later than 13 March 2009.

The proposed new Directive would make electronic invoices equivalent in all respects to paper ones. It would introduce at least two major changes to existing e-Invoice practices: first, it would eliminate the requirement that advanced electronic signatures be used in electronic invoices. Second, it would eliminate the requirement that the recipient of the invoice consent to receive invoices in electronic form.2

Timing

The Commission’s goal is to have new legislation implemented by the member states by 1 January 2013.

One day before the EU Commission made this announcement, the EU’s “Expert Group” on e-Invoicing issued its Mid Term Report on e-Invoicing (27 January, 2009).3 The Expert Group on e-Invoicing was established by the European Commission on 31 October 2007. Its task is to issue a final report on establishing a European Electronic Invoicing Framework by the end of 2009.

The Mid Term Report points out that individual member states are already implementing measures to accelerate adoption of electronic invoices in those states: In Spain, all suppliers of
the government, regardless of size or turnover, must submit electronic invoices to the Public
Administration by November 2010. The Finnish Government has announced that it will accept
only e-Invoices from 1 January 2010. And in Italy, e-Invoicing for the supply of goods and
services to the public sector has started to become mandatory under a phased timetable.

The Mid Term Report estimates that currently only 3% to 12% of invoices in Europe are
transmitted electronically.

**Advanced Electronic Signatures No Longer Required**

The Expert Group based its recommendations on its finding that it is the member states’
disparate requirements for advanced electronic signatures that has created significant
obstacles to the adoption of electronic invoices. The Expert Group observed that the
requirement for advanced electronic signatures, while well intentioned, has resulted in an
anachronistic requirement for a “seal” for an original electronic document, much like the
former wax seals of paper documents. Not only is a “seal” uniquely required for electronic
invoices, but the requirements for that seal vary among the member states, resulting in great
practical difficulties in cross border invoicing. The Commission now wishes to harmonize
member state requirements for electronic invoices by, among other things, abolishing the need
for invoices to include advanced electronic signatures.

In the original 2006/112/EC Directive on VAT Invoicing, Title XI, Chapter 3, Section 5 governed
the use of electronic invoices.

Article 232 of the original directive allowed enterprises to use electronic invoices only if the
recipient consented to receive electronic invoices.
Article 233 required electronic invoices to assure integrity of content and authenticity of origin by means of either an advanced electronic signature, EDI or “other electronic means allowed by the Member States.”

The proposed new Directive would amend Article 232 to say that invoices can always be sent by paper or “made available” electronically, thus deleting the requirement of recipient consent. The new directive would delete Article 233 and the requirement to use advanced electronic signatures entirely.5

In adopting this proposed new Directive, the Commission announced:

“The proposal aims to end any legal barriers to e-invoicing contained in the VAT Directive by treating the transmission of an invoice, whether by paper or by electronic means, equally. Thus, references to the fact that the e-Invoice should be by advance signature or by EDI are removed.

“At the same time it is important that best practices develop so that standards, business requirements and all legal requirements converge towards a common approach. In this sense the VAT Directive can only play a part in helping to remove the obstacles that currently exist in terms of VAT legislation and here work of the Expert Group on E-invoicing will be useful.”6

**Goal: A Pan European Framework of Interoperability**

The Mid Term Report suggests that the Expert Group will recommend adoption of a pan European “overarching framework for interoperability, in which trading parties and their service providers could interoperate with each other across Europe in an open and standardised way”.7

The recommend “framework” would include, among other things:
1. Full harmonization of national/tax requirements among EU Member states regarding e-Invoices;
2. A single “semantic data model” for e-Invoice content standards (as opposed to recommendation of a single content standard), with a recommendation that UN/CEFACT and ISO be the two global standards organizations that should collaborate to develop an e-Invoice content standard that satisfies the overall Business Requirements identified by the Expert Group. This would constitute the core reference semantic model for the European e-Invoicing Framework;
3. A business requirement of reducing manual work for the sender/receiver, while remaining technology neutral and accessible to all trading partners with or without ERP systems. This aspect of the framework could have significant implications if it is interpreted to prohibit the practice of large buyers or suppliers requiring all of their trading partners to manually enter data onto a unique web based system;
4. A method of ensuring “trustworthiness and data protection.” While invoices do not typically include personally identifiable information of individuals, the Expert Group emphasized that commercial data is nonetheless worthy of protection: “Privacy and data protection should be ensured at all levels in the end-to-end process. Invoice data is critical to any enterprise and important information about the trading parties and their supply chains are an integral part of the transmitted data.”;
5. Replacing digital signatures for ensuring authenticity of origin and integrity of content with auditable internal business control processes. While not fully formulated, these internal business processes might involve a Code of Practices along the lines of the Good Practice Guidelines developed by the CEN Workshop on Electronic Invoicing available at the following URL: http://www.e-invoice-gateway.net/knowledgebase/eInvoiceBestPractice. Those best practices may be enforced through audit guidelines issued at a pan European level or through bilateral agreements among trading partners or with service providers, with the understanding that in the final analysis each trading partner is responsibility for the integrity of its own control systems.
Practical Considerations

Practitioners should note that the devil will be in the detail of the “auditable internal business control processes.” Under current legislation, both the integrity of the invoice (assurance that the content has not been modified) and its authentication (assurance of identity of the sender) is assured by the use of an advanced electronic signature. Under the proposed new regime, an electronic signature would only provide authentication and possible a much lower level of authentication than provided by advanced electronic signatures. Precisely how the integrity of the document and equivalent protection of authentication will be ensured through auditable business processes will of course be of interest to all enterprises in Europe.

If the proposed new directive is adopted, trading partners will have the right, but not the obligation, to use advanced electronic signatures. Trading partners choosing to forego the security of advanced electronic signatures for the ease of transmission, will need to consider the effect of Directive 1999/93/EC on a Community Framework for Electronic Signatures and national legislation issued pursuant thereto by the member states. Under Article 5(1) of that Directive, advanced electronic signatures based on a qualified certificate and which are created a secure signature device are required to be afforded the same treatment as a handwritten signature and must be admissible as evidence in legal proceedings. Electronic signatures without such an advanced electronic signature fall under Article 5(2) of that Directive, which provides the weaker level of protection of not being denied legal effectiveness “solely on the grounds” that they are in electronic form or not based on a similar advanced electronic signature.
The proposed new Directive (and a link to the original Directive) is available at the following URL:


The Mid Term Report of the European Commission Expert Group on e-Invoicing is available at the following URL:
http://www.epractice.eu/document/5425


See Mid Term Report of the European Commission Expert Group on e-Invoicing at Pages 25-26, Section 5.3.
See Mid Term Report of the European Commission Expert Group on e-Invoicing at Page 8, Section 2.2.
See Mid Term Report of the European Commission Expert Group on e-Invoicing at Page 11, Section 2.6

About the Author: Phillip Schmandt is a Partner and Chair of the Technology Practice Group at McGinnis, Lochridge & Kilgore in Austin, Texas (www.mcginnislaw.com). He can be reached via e-mail at pschmandt@mcginnislaw.com.
Bankruptcy and the Software License
By Alan S. Wernick

Most companies have software they license for business critical applications. What happens to the business (licensee) if the licensor of the computer software enters bankruptcy? Does the business have to stop using the software altogether or have some restrictions applied to their use? Would the business suffer if it had to stop using any business critical computer programs they currently use? And, if the business fails to immediately stop using the software, will the bankruptcy trustee for the debtor/licensor pursue the business for infringement damages?

Both in good times and challenging economic times, bankruptcy is sometimes the “exit strategy” for some businesses, including software licensors. And, once the licensor’s bankruptcy petition is filed, it will only be a matter of time before the licensees feel the impact of that filing.

The drafter of a software license agreement must look ahead in the transaction and consider where the parties want to be in the event of bankruptcy, and then properly weave those considerations into the fabric of the agreement. In the event of the licensor’s bankruptcy, the licensee must act precisely and without hesitation to fully avail itself of the benefits of Sec. 365(n) of the Bankruptcy Code.

Under Sec. 365(n) of the U.S. Bankruptcy law (11 U.S.C. Sec. 365(n)(1)), a licensee has the option of (a) terminating the license agreement, if rejection by the trustee amounts to such a breach as would entitle the licensee to treat such contract as terminated by its own terms, applicable non-bankruptcy law, or an agreement made by the licensee with another entity, or (b) retaining the licensee's rights (including the right to enforce any exclusivity provision of such license agreement, but excluding any other right under applicable non-bankruptcy law to specific performance of such contract) to the computer software, subject to the limitations set
forth in Sec. 365(n). The license agreement should address the rights the licensee will have in the event of the licensor’s bankruptcy. However, when the license agreement is silent on the issue of the licensor’s bankruptcy, there may be other provisions of the agreement or other documents that will impact the analysis and the outcome as to whether or not the licensee may continue to use the software in some manner or another for the licensee’s business. One such other document is the source code escrow agreement which when properly drafted (and the escrow properly maintained) may, in the event of the licensor’s bankruptcy, provide both legal and practical remedies to the licensee.

When an owner of certain types of intellectual property comes under the protection of the Bankruptcy Court, the rights of licensees are at risk with regard to that intellectual property (including trade secret, invention, process, design, or plant protected under U.S.C. Title 35; patent application; plant variety; work of authorship protected under U.S.C. Title 17 -- such as computer programs; or mask works protected under U.S.C. Title 17; to the extent protected by applicable non-bankruptcy law). In the past, that risk might clearly have been that the licensee would lose its license rights to the licensed technology, as was the case in \textit{Lubrizol Enterprises Inc. v. Richmond Metal Finishers, Inc.}, (4th Cir. 1985).

However, Congress addressed the \textit{Lubrizol} problem by enacting the “Intellectual Property Bankruptcy Protection Act of 1987 -- An Act to Keep Secure the Rights of Intellectual Property Licensors and Licensees Which Come Under the Protection of Title 11 of the United States Code, The Bankruptcy Code.” But, as seen in \textit{In Re El International} (U.S. Bankruptcy Court for the District of Idaho, 1991), a licensee of computer software failed to retain its rights to licensed software when its licensor went into bankruptcy. Thus, even though Sec. 365(n) exists in the bankruptcy statutes, the licensee may still lose, or have limitations placed upon, its licensed rights to the technology.

Appropriate language for addressing the bankruptcy issue in a software license agreement will depend upon the particular facts of the transaction. Depending on those facts, one drafting tip may be for the software license agreement to provide that “...failure by the
Licensee to assert its rights to ‘retain its benefits’ [to the intellectual property encompassed by the software], pursuant to Sec. 365(n)(1)(B) of the Code, 11 U.S.C., under an executory contract rejected by the trustee in bankruptcy, shall not be construed by the courts as a termination of the contract by Licensee under Sec. 365(n)(1)(A) of the Bankruptcy Code.”

If, on the other hand, the licensee enters into bankruptcy, the question arises as to whether or not the trustee for the debtor/licensee can assign the software license as an asset of the debtor. This analysis will depend on several things including whether or not the license is an exclusive or nonexclusive license, and how the issue of assignment is addressed in the license agreement. The few cases that have examined the issue of assignment and assumption of a software license agreement in the bankruptcy context have turned to the copyright law analysis of the issue, a discussion of which is beyond the scope of this article.

The bottom line of the licensee's failure to take appropriate action in the event of the licensor’s bankruptcy may result in the licensee's loss of its rights to the licensed technology. The licensee must not procrastinate when faced with rejection of an executory contract. Under Sec. 356(n) of the Bankruptcy Code, it must proceed promptly to assert its rights under this provision to retain its rights to the software covered under the agreement, or alternatively, pursue its monetary claims provided for in the contract.

© 2009 Alan S. Wernick. WWW.WERNICK.COM All rights reserved.

About The Author: Since 1982 Alan S. Wernick has been practicing computer law / cyberspace law / information technology law, data privacy, and intellectual property law. He has a background in computer programming and accounting. Alan is admitted to practice in IL, NY, OH, and DC. Additional information is available at WWW.WERNICK.COM. He can be reached via e-mail at ALAN@WERNICK.COM.
What Limits For Behavioral Targeting?

By Francoise Gilbert

An individual uses a travel site to check hotels in New York, but does not book any hotel room. Later the individual visits the website of a local newspaper to read about the Chicago Cubs baseball team. While on the newspaper’s website, the individual is served an advertisement from an airline featuring flights from Chicago to New York. The method used to develop the consumer’s profile – someone interested in travelling to New York from his home base in Chicago – in order to serve target ads is named “behavioral advertising” or “behavioral targeting.”

Behavioral targeting is a marketing technique that tracks a user’s online activities over time in order to build a profile of that individual and to deliver advertising that is targeted to the assumed interests of this individual. The information about a user is collected through a combination of cookies and pixel tags. It could include what searches were conducted, what pages were visited, how long she stayed on a particular page, on which links or advertisements she clicked. This information may then be combined with other information about that individual, such as her geographic location. It is then shared with advertisement networks, which serve advertisements at websites across the Internet.

Many consumers and advocacy groups are concerned about the privacy issues that are associated with such practices. For example, the manner in which the consumer information is collected is not visible to the consumer. Further, sensitive information regarding health, finances, or children could be used for unanticipated purposes.

The Federal Trade Commission has conducted studies, published reports, and presented testimony before a Committee on Commerce, Science and Transportation in Congress. In December 2007, it published proposed “Online Behavioral Advertising Privacy Principles”, indicating that it was seeking comments. In February 2009, the FTC issued a report describing its ongoing examination of online behavioral advertising and setting forth revised proposed

The report discusses the privacy concerns raised by behavioral advertising. It notes that companies must still comply with all applicable privacy laws, some of which may impose requirements that are similar to those established by the principles. The report sets forth four revised principles.

- **Transparency and Consumer Control:** Websites are expected to provide clear, concise, consumer-friendly, and prominent notice regarding behavioral advertising, and an easily accessible way for consumers to choose whether to have their information collected for such purpose. The report encourages the development of creative and effective disclosure mechanisms that are separate from their privacy policies.

- **Reasonable Security and Limited Data Retention:** Companies are urged to provide reasonable security for any data they collect for behavioral advertising and to retain data no longer than is needed in order to fulfill a legitimate business or law enforcement need.

- **Affirmative Consent for Material Changes to Existing Privacy Promises:** Before a company can use previously collected data in a manner that is materially different from the promises that the company made when it collected the data, it should obtain affirmative express consent (opt-in consent) from the affected customers.

- **Sensitive Information:** Companies are urged to obtain affirmative express consent before collecting sensitive information for behavioral advertising. While financial information, information about children, health information, and Social Security numbers traditionally have been considered" sensitive information," the FTC encourages stakeholders to develop more specific standards to address this issue.

**Next steps:** In its press release accompanying the report, the FTC notes that the February 2009 document is only part of an ongoing process, and that significant work in this area remains. The FTC intends to evaluate self-regulatory programs and to conduct investigations, where appropriate, to determine whether practices violate Section 5 of the FTC Act. In his comments accompanying the updated principles, FTC Commissioner Jon Leibowitz noted that “industry
needs to do a better job of meaningful, rigorous self-regulation, or it will certainly invite legislation by Congress and a more regulatory approach by our Commission…. Put simply, this could be the last clear chance to show that self-regulation can – and will – effectively protect consumers’ privacy in a dynamic online marketplace.”

Companies need to pay close attention to behavioral targeting issues and must update their privacy statements in order to reflect their actual practices accurately. To the extent that they do use behavioral advertising techniques and collect information about their user’s behaviors, they should give them the opportunity to choose whether to have their information collected for such purpose.

Copyright 2009 Françoise Gilbert, IT Law Group, Palo Alto, CA. All rights reserved.

About The Author: Françoise Gilbert is the Managing Director of IT Law Group, www.itlawgroup.com, a law firm based in Palo Alto, California. A practicing attorney and a Certified Information Privacy Professional (CIPP), Ms. Gilbert focuses on information privacy and security, and data governance. She is admitted to practice law in California, Illinois, and France. She can be reached via e-mail at fgilbert@itlawgroup.com.

REMINDER: The Cyberspace Law Committee will present a new program on behavioral advertising issues at the Section of Business Law’s Spring Meeting. Join us on Saturday from 8:00 AM - 9:30 AM to see “A Business Lawyer's Review of Online Behavioral Advertising - A Legal Analysis of the New Technologies and Marketing Practices.” Program Chair Elizabeth Bowles is looking forward to seeing you!
“Red Flags Rule” – Will You Be Compliant or Complacent?

By Alan S. Wernick

The federal “Red Flags Rule” is designed to minimize identity theft. The failure of covered entities to comply can have several consequences, including civil penalties, injunctions, annual reporting, government oversight of the non-compliant business, and loss of trust by the customers of the business.

An amendment to the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") requires covered entities to create programs which must provide for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft. The Federal Trade Commission ("FTC"), the federal bank regulatory agencies (including the Office of the Comptroller of the Currency, the Federal Reserve, the Federal Deposit Insurance Program, and the Office of Thrift Supervision), and the National Credit Union Administration have issued regulations concerning this Red Flags Rule (the “Rule”).

In October 2008 the FTC granted a six-month delay of enforcement of the Rule requiring covered entities under its jurisdiction to have identity theft prevention programs in place. This enforcement delay was limited to the Identity Theft Red Flags Rule, and did not extend (a) to the rule regarding address discrepancies applicable to users of consumer reports, or (b) to the rule regarding changes of address applicable to card issuers. The FTC delay did not affect other federal agencies’ original November 1, 2008, enforcement date of the Rule.

May 1, 2009, marks the beginning of the FTC enforcement of the Rule. The FTC’s announced purpose for their delay in enforcement is to allow covered entities sufficient time to
establish and implement appropriate identity theft prevention programs in compliance with the Rule. Will you be ready?

What Are The Red Flags Rule And How Will You Comply With Them?

How you comply with the Rule depends on your business, the type of sensitive consumer data your business collects which is subject to the Rule, and how your business handles that data. Essentially the Rule requires you to develop a written program that identifies and detects relevant identity theft warning signs – i.e., “red flags.” Your written program must also describe your responses that would prevent and mitigate identity theft as well as set forth detailed information as to how you will update the written program. The Rule states that the written program must initially be managed by the Board of Directors or, if the business does not have a Board of Directors, by senior employees. The business must have an annual review of the program, provide appropriate staff training, and provide for oversight of any third-party service providers.

The Rule set forth numerous examples of types of red flags, which fall into five categories:

- Alerts, notifications, or warnings from a consumer reporting agency;
- Suspicious documents;
- Suspicious personally identifying information, such as a suspicious address or SSN that is listed on the Social Security Administration’s Death Master File;
- Unusual use of, or suspicious activity relating to, a covered account;
• Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts held by the financial institution or creditor.

In 2005 ChoicePoint, Inc., suffered a major data breach involving some 163,000 records. ChoicePoint ultimately settled with the Federal Trade Commission for $10 million in civil penalties and $5 million for consumer redress. This $15 million was in addition to the other costs (e.g., attorney fees, security consultant fees, customer notifications, etc.) incurred as a result of the breach. In the ChoicePoint situation the identity thieves set up bogus ChoicePoint accounts which they used to obtain the personal identifiable information records. If the Rule had been effective in 2005 and ChoicePoint in compliance, perhaps the data breach could have been avoided, or at least minimized both in terms of the number of records breached and the total cost to ChoicePoint resulting from the breach.

Who Must Comply With The Red Flags Rule?

The Rule applies to “financial institutions” and “creditors” with “covered accounts.” Where the enforcement net widens is in the definition of “creditors” with “covered accounts.” This is because the Rule defines a “creditor” as any entity that regularly extends, renews, or continues credit; that arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Specifically identified as “creditors” are finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies; plus non-profit and
government entities that defer payment for goods or services. Other “creditors” deferring payments on a regular basis may include retailers and hospitals.

The expanded coverage of the Rule arises in part through the definition of a “covered account.” This definition is integral to the underlying policies of the Red Flags Rule – the prevention of identity theft. A “covered account” is defined as an account used mostly for personal, family, or household purposes, and involves multiple payments or transactions. This includes financial accounts such as credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts, plus any 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.” This definition would include any account that may be vulnerable to identity theft such as a small business or sole proprietorship account. Thus, if your business is a steward of data that, if breached, presents a reasonably foreseeable risk of identity theft, then the Rule may apply.

One may argue that any new rule or regulation is overly burdensome. Nevertheless, for those businesses now leading or on track to become the leaders in their respective industries the Red Flags Rule may provide one benchmark for best practices in protecting the personal identifiable information of the customers and employees of the business. The health care services industry is already subject to a number of privacy related regulations. Two examples being the Health Insurance Portability and Accountability Act (“HIPAA”), and the American Recovery and Reinvestment Act of 2009 (“ARRA”), Title XIII – the Health Information
Technology for Economic and Clinical Health Act (the “HITECH Act”) – which indicates a new phase in the evolution of federal law governing the privacy and security of medical information. Likewise, the financial services is subject to a number of privacy related regulations, such as the Gramm-Leach-Bliley Act (“GLB”).

With medical identity theft on the rise, much of the enforcement activity in medical identity theft cases has come from the offices of the Attorney General in various states rather than through HIPAA enforcement. Since the requirements of the state data breach laws vary, the Red Flags Rule may prove less of a burden to the health care industry than might appear from a first look at the Rule, and proper and consistent compliance with the Rule may minimize the exposures that trigger the data breach laws in the first place.

What Might Happen If You Fail To Comply With The Red Flags Rule?

Typical FTC enforcement activities of the Red Flags Rule may include requesting injunctive relief, monetary damages, and increased government oversight of your business (including annual reporting of your compliance for possibly twenty years). This is in addition to the value of management’s time that will have to be focused in a crisis mode upon receipt of notice of an enforcement action, court costs, consultant fees, and attorney fees to respond to the enforcement action. But all of these costs may pale in comparison to the cost to your business resulting from a loss of trust by your customers due to a data breach, particularly when the customers are victims of identity theft traced back to your business. Which costs less: prevention or clean-up? Taking the time now to understand the data your business uses, how the Red Flags Rule apply to your business, and engaging in preventive planning to comply with
the Red Flags Rule should cost your business less. As Ben Franklin said: “An ounce of prevention is worth a pound of cure.” Ignoring the Red Flags Rule could cause your business’s bottom line to see red.

© 2009 Alan S. Wernick.  WWW.WERNICK.COM  All rights reserved.

About The Author:  Since 1982 Alan S. Wernick has been practicing computer law / cyberspace law / information technology law, data privacy, and intellectual property law.  He has a background in computer programming and accounting.  Alan is admitted to practice in IL, NY, OH, and DC.  Additional information is available at WWW.WERNICK.COM.  He can be reached via e-mail at ALAN@WERNICK.COM.