ABA SECTION OF ANTITRUST LAW

ABA ANTITRUST SECTION

INSURANCE AND FINANCIAL SERVICES COMMITTEE NEWSLETTER

Prepared for the Members of the Antitrust Section

American Bar Association | Fall 2009 | Section of Antitrust Law

EDITOR'S NOTE

By Renata B. Hesse

This marks the first edition of the newsletter of our newly-formed committee. We are excited to have a stand-out edition to mark the occasion, with articles that provide a unique focus on issues of importance to the insurance and financial services industries. The articles in this edition cover three topics of current interest for practitioners. The first article, by Matt Staples of Wilson Sonsini, is on the FTC's Red Flag Rules, and provides an overview of the rules with a particular focus on providing practical tips on determining whether a business is covered and, if so, on implementing the rules. This article—along with the one that follows it—brings to the newsletter a bit of perspective on the consumer protection issues that are currently facing businesses in the insurance and financial services industries. The second article, by Daniel Edelman of Crowell and Moring, provides an overview of the new proposed Consumer Financial Protection Agency. This new agency—assuming its formation is approved by Congress—will be of acute interest to those of us who work with financial services clients and is at the center of the Obama Administration's efforts to reform financial regulation. We will all be watching Congress later in the Fall for word on the agency's fate. Finally, Logan Breed and Leigh Oliver from Hogan & Hartson provide an update on the on-going legislative activity relating to credit card interchange fee legislation. Their article provides a fact-filled summary of the legislative activity in this area and the positions of the various constituencies with interests in the legislation. We hope that you all find the newsletter interesting and informative.

CO-CHAIR'S REPORT

By Suzanne E. Wachsstock

When we last published our newsletters in the Spring, we represented two separate committees -- the Insurance Committee and the Financial Services Committee. Today, our newly-constituted joint committee offers one-stop shopping for issues of interest in both the insurance and financial services sectors. Stemming from this merger, our first request to our joint readership is in the form of a contest: Help us come up with a more creative name for the "Insurance and Financial Services Committee," and we'll give you a year's free subscription to our newsletter!

While you are working hard on that task, we wanted to give you a preview of some of the programs we have in the works for the upcoming year. We have brown bags and teleseminars planned on such diverse issues as perspectives on the proposed Consumer Financial Protection Agency and the Credit Card Fair Fee Act of 2009, both previewed in this newsletter; current developments relating to board interlocks under Clayton Section 8, a newly hot topic in light of the Google/Apple investigation; the EC Insurance Block Exemption Regulation; antitrust immunities; non-discrimination rules; and a multi-part series on antitrust issues that arise in the trading, settling and clearing of complex financial instruments. We are also working on streamlining and expanding our website in light of our expanded membership and offering new opportunities for on-line discussion.

As always, we are looking for eager new members to help us plan and execute each of these programs, as well as to write articles for our upcoming newsletters and grow our listserv, so step up if you are interested in getting involved in any way. We welcome all suggestions to help us make the committee and its activities relevant and interesting for each of you. Please don't hesitate to contact any of us at the numbers or email addresses listed on the right. We look forward to hearing from you.

Committee Co-Chairs:

Suzanne E. Wachsstock
American Express Company
200 Vesey Street
New York, NY 10285
Phone: (212) 640-8159
Suzanne.E.Wachsstock@aexp.com

William M. Katz, Jr.
Thompson & Knight LLP
One Arts Plaza
1722 Routh Street, Suite 1500
Dallas, TX 75201
william.katz@tklaw.com

Committee Vice-Chairs:

Renata B. Hesse
Wilson Sonsini Goodrich & Rosati
1700 K Street, N.W., Suite 500
Washington, D.C. 20006
Phone: (202) 973-8834
rhesse@wsgr.com

Scott A. Scheele
U.S. Department of Justice
Antitrust Division
450 5th Street, N.W., Suite 7700
Washington, D.C. 20530
Phone: (202) 616-5924
Scott.Scheele@usdoj.gov

Elai Katz
Cahill Gordon & Reindel LLP
Eighty Pine Street
New York, NY 10005
Phone: (212) 701-3039
ekatz@cahill.com

Council Liaison:

Jonathan M. Jacobson
Wilson Sonsini Goodrich & Rosati
1301 Avenue of the Americas,
40th Floor
New York, NY 10019
Phone: (212) 999-5800
jjacobson@wsgr.com

Red Flags Rules: Financial Institutions and Creditors with Covered Accounts Must Implement ID Theft Prevention Programs

By Matthew C. Staples[1]
Wilson Sonsini Goodrich & Rosati

Each year, millions of Americans are victims of identity theft. The information used to commit the crime comes from many different sources: a stolen wallet, dumpster diving, or online phishing, to name a few. Businesses also collect and hold sensitive personal information about their customers, like names and addresses, Social Security numbers, credit card numbers, and other financial account information that can be used for identity theft if it falls into the wrong hands. Government regulators and industry have responded to the threat of identity theft by adopting rules that require companies to take steps to prevent and mitigate the compromise of sensitive personal information.

The most recent initiative is the Red Flags Rules ("Rules"), a joint effort by the financial regulators—the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System—and the Federal Trade Commission (FTC). The Rules,[2] promulgated pursuant to the Fair and Accurate Credit Transactions Act ("FACTA"), require creditors and financial institutions that maintain "covered accounts" to develop and implement *written* identity theft prevention programs. The programs must be designed to help identify, detect, and respond to patterns, practices, and activities—termed "red flags"—that could indicate identity theft. The federal financial institution regulators have required compliance with the Rules since November 1, 2008, while the FTC has stayed enforcement of the Rules until November 1, 2009.

This article provides an overview of the Rules and discusses issues relevant to businesses facing the Rules.[3]

Applicability

The Rules apply to all *financial institutions* and *creditors* that maintain *covered accounts*, terms that are defined in the Fair Credit Reporting Act ("FCRA"). "Financial institution" includes all banks, savings associations, and credit unions, as well as any other person that directly or indirectly holds a transaction account belonging to a consumer. A "creditor" is "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of any original creditor who participates in the decision to extend, renew, or continue credit." This broad definition sweeps many businesses within the scope of the Rules, including many that ordinarily would not consider themselves "creditors." For example, permitting deferred payments for goods and services, and certain lending activities, such as permitting trades on margin, fall within the application of the Rules, as do other routine business activities, such as offering payroll cards or other pre-paid cards that permit multiple transactions and involve a continuing relationship.

Many businesses have found determining whether they are covered by the Rules to be quite challenging. In particular, many businesses have struggled with identifying and ascertaining how and whether they may be "creditors" subject to the Rules. Assessing the applicability of the Rules in light of operations is the first step toward compliance.

The Requirements – What Must be Done by Businesses with "Covered Accounts"

The Rules require creditors and financial institutions to implement identity theft prevention programs if they maintain *covered accounts*, which are accounts offered or maintained primarily for personal, family, or household purposes that permit multiple payments or transactions. Examples include a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account. Covered accounts also include any other accounts, whether personal or business accounts, where 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.

Complying with the Rules

All financial institutions and creditors with covered accounts must develop and implement a program designed to detect, prevent, and mitigate identity theft. Thus, once a business has determined that it is a *creditor* with *covered accounts*, the next step is to design and implement a program appropriate to its business operations.

The Rules employ a risk-based approach. Red flags programs, therefore, should be appropriate to the size and complexity of a business and to the nature of its operations. A business with several types of covered accounts may need a complex program, while a small, low-risk entity may be able to implement a more streamlined program.

In all cases, the program must include the following:

- ***Identification of red flags***. The business should determine relevant patterns, practices, and specific activities that are "red flags" signaling possible identity theft. For example, an alert, notice, or other warning from a consumer reporting agency regarding an account may be a red flag, as may the presentation of apparently

---

[1] Matthew C. Staples, an associate in the Seattle office of Wilson Sonsini Goodrich & Rosati, is a member of the firm's Technology Transactions and Consumer Regulatory and Privacy groups. He counsels companies in several industries regarding information privacy, data security, e-commerce, marketing, and advertising matters. He can be reached at mstaples@wsgr.com.

[2] *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule*, 72 Fed. Reg. 63718 (Nov. 9, 2007) (*available at* http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf) ("Red Flags Publication").

[3] The Red Flags Publication also contains "address discrepancy rules" that were issued jointly by the FTC and federal financial institution regulators. These rules, which went into effect on November 1, 2008, require users of credit reports to follow specific procedures upon receiving a notice from a consumer reporting agency of a substantial difference between a consumer's address that the user provided to request a consumer report and the address in the agency's file. The address discrepancy rules went into effect on November 1, 2008. Unlike the Rules, enforcement of the address discrepancy rules was not stayed by any of the responsible agencies.

forged documents when a customer requests an address change.

- ***Detection of red flags***. The program must be designed to detect the red flags it has identified in connection with the opening of new covered accounts and the servicing of existing covered accounts. For example, companies should obtain identifying information from a person opening a new covered account in order to verify the person's identity. In the case of existing accounts, companies should authenticate customers, monitor transactions, and verify the validity of address change requests.

- ***Responses to red flags***. The program should spell out appropriate actions that the company will take when it detects red flags. The action should be commensurate to the risk posed by the red flag. For example, if a credit card account is suddenly used for a series of high-value transactions, it may be appropriate to notify the customer and, if the customer is unaware of the activities, to notify law enforcement and to re-open the account with a new account number. If suspicious documentation is presented when a person applies for a new covered account, a proper response may be to not open the covered account.

- ***Periodic review and updating***. Finally, the program should address how the company will re-evaluate the program periodically and, as necessary, update it to address new and evolving threats.

Board of Director Approval Required

Similar to the board approval requirements for information security programs issued by regulators under the Gramm-Leach-Bliley Act, red flags programs must be approved by the entity's board of directors (or a committee of the board). If the regulated entity lacks a board of directors, approval is required by an appropriate senior-level employee. Consistent with other information security best practices, an approved program must specify who is responsible for implementing and administering the program effectively.

The program also must provide for staff training and oversight of any subcontractors. Failure to comply with the Rules may result in injunctive relief and civil penalties and could lead to claims under state consumer protection laws.

Additional Considerations and Developments

Other issues are likely to emerge from the Rules as well. The ABA has urged Congress and the FTC to exempt lawyers and law firms from the Rules,[4] much like it challenged the application of the privacy provisions of the Gramm-Leach-Bliley Act to lawyers and law firms.[5] The FTC has already denied a similar challenge for exemption of health care providers from the red flags rules by the American Medical Association.[6] Though unsuccessful to date, a successful challenge by any industry group could bring other challenges to the Rules.

Additionally, insurance companies, which are exempt from most federal banking regulations pursuant to the McCarran-Ferguson Act,[7] may be covered under the Rules. The McCarran-Ferguson Act preserves the FTC Act's application to the insurance business to the extent not regulated by state law,[8] and the FTC is likely to enforce compliance with the Rules within the insurance industry.

Implications

For many financial institutions, including insurance companies, the underlying elements of a red flags compliance program will seem familiar. In particular, requirements to designate responsible individuals and to perform risk and related assessments have been around for quite some time. A significant aspect of the Rules, however, is the focus and emphasis upon ensuring that the compliance program addresses risks faced by consumers. In this regard, the Rules may be seen as the latest evolution of other information security requirements, building upon those found in regulations implementing the Gramm-Leach-Bliley Act. Regulators' experience with those regulations suggests an ongoing desire to improve compliance procedures and protocols to address consumer protection concerns rooted in the collection, use, and disclosure of personal information.

A challenge for business is how to design and implement red flags programs efficiently and in a manner that complements existing compliance activities. Avoiding duplication, leveraging existing skill sets and competencies, and mastering another set of regulations, represent some of the tasks regulated businesses face in complying with the Rules.

To assist covered entities in developing and implementing appropriate identity theft prevention programs, the regulators involved in the creation of the Rules have issued a supplement that provides examples of red flags,[9] a set of frequently-asked questions,[10] and a compliance guide for

---

[4] Statement of H. Thomas Wells, Jr., President, American Bar Association, regarding Fair and Accurate Credit Transaction Act "Red Flags Rule," June 22, 2009, *available at* http://www.abanet.org/abanet/media/statement/statement.cfm?releaseid=684.

[5] The U.S. Court of Appeals for the District of Columbia Circuit ultimately held that the FTC had overstepped its authority in seeking to apply Gramm-Leach-Bliley's privacy provisions to lawyers and law firms. *See American Bar Ass'n v. F.T.C.*, 430 F.3d 457 (D.C. Cir. 2005).

[6] Letter from Eileen Harrington, Acting Director of Bureau of Consumer Protection, Federal Trade Commission, to Director of Federal Affairs, American Medical Association, dated February 4, 2009, *available at* http://www.ftc.gov/os/closings/staff/090204amaresponse.pdf.

[7] The McCarran-Ferguson Act provides that "[t]he business of insurance, and every person engaged therein, shall be subject to the laws of the several States which relate to the regulation or taxation of such business. No Act of Congress shall be construed to invalidate, impair, or supersede any law enacted by any State for the purpose of regulating the business of insurance . . . unless such Act specifically relates to the business of insurance[.]" 15 U.S.C. § 1012.

[8] McCarran-Ferguson Act, 15 U.S.C. § 1012.

[9] The *Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation* are published as Appendix A to 16 CFR Part 681. They are published on pages 63,773 and 63,774 of the Red Flags Publication.

[10] The Frequently Asked Questions document is available at http://www.ftc.gov/os/2009/06/090611redflagsfaq.pdf. It notes that the FTC plans to issue additional FAQs to answer

low-risk entities that includes a program template.[11]

Conclusion

The regulators involved in creating the Rules cast a wide net in defining the scope of entities to which they apply. Many organizations should examine whether they are "creditors" and whether their activities are subject to the Rules. Leveraging existing compliance programs, especially those focused on fraud prevention and detection, can help organizations address the Rules cost-effectively. The Rules themselves suggest the ongoing importance of sound privacy and information governance practices, as well as the need for, and value in, regular review and assessment. These practices all are familiar to compliance professionals.

A Primer on the Consumer Financial Protection Agency

By Daniel D. Edelman[12]
Crowell & Moring LLP

As part of its "New Foundation" initiatives pursuing financial regulatory reform, the Obama administration is supporting congressional approval of the "Consumer Financial Protection Agency Act of 2009" to create a new, independent regulatory agency known as the Consumer Financial Protection Agency ("CFPA"). The brainchild of Harvard Law professor Elizabeth Warren, who now also chairs the government panel overseeing TARP funds, the CFPA grew out of concerns about consumer financial losses in the credit card and mortgage industries. The White House, however, proposes using the CFPA to establish "comprehensive reform" by heightening consumer protections and imposing robust provider regulations for credit, savings, payment and other consumer financial products and services. The overall aim of the CFPA is to "instill a genuine culture of consumer protection" in the regulatory framework.

The CFPA program of comprehensive reform would be based on four principles: transparency, fairness, accountability and access. These objectives would entail making financial disclosure forms clear, simple and concise and imposing consumer communication duties that are reasonable and not just technically compliant. Specifically, the CFPA would encourage "plain vanilla"or less complex financial products.

Beyond mandating clear disclosure and straightforward products, the CFPA would be responsible for regulating and enforcing against unfair, deceptive and abusive practices concerning credit, savings and payment products and services. The proposed agency's mission would also include making financial products and services more accessible to households and communities that traditionally have had limited access to such products and providing better and more user friendly educational materials about these products and services.

If adopted, the CFPA would be funded primarily from fees assessed on covered entities and transactions subject to the agency's supervision. Like other major federal agencies, the CFPA would be run by a director and a board and supported by officers and staff. The CFPA director would also be one of the eight members of the new Financial Services Oversight Council, responsible for assessing risks to the entire financial system.

As the overarching consumer protection agency in the area of financial products and services, the CFPA would be granted the authority to promulgate rules and regulations under the various consumer financial services and fair lending statutes, including the newly-enacted Credit Card Accountability, Responsibility and Disclosure Act. Other laws that would become subject to CFPA authority include: the Truth in Lending Act (TILA), Home Ownership and Equity Protection Act (HOEPA), Real Estate and Settlement Procedures Act (RESPA), Community Reinvestment Act (CRA); Equal Credit Opportunity Act (ECOA); Home Mortgage Disclosure Act (HMDA) and the Fair Debt Collection Procedures Act (FDCPA). The CFPA would be given similar authority under any future consumer protection laws directed at the consumer credit, savings, collection or payment industries.

Private rights of action under these statutes would remain in existence. The ability of states to adopt even stricter consumer protection laws would also remain in place. The CFPA's mandate would include close coordination with state regulators in efforts to unify and strengthen standards for registering and improving the quality of financial services providers and intermediaries.

Under the proposed regulatory scheme, primary authority for financial product and service protections would be transferred from the Federal Trade Commission (FTC) to the CFPA, with the FTC retaining back-up authority for the statutes under which it currently has jurisdiction. The FTC would retain primary authority for dealing with fraud in the financial marketplace and would remain the lead federal agency on matters of data security.

The new agency would also assume consumer responsibilities currently handled by banking regulators, such as the Federal Reserve, the FDIC and Comptroller of the Currency. For example, the CFPA would set mortgage lending standards, assess the risks associated with such products and proscribe products determined to be too onerous for borrowers.

The CFPA would be authorized to collect information through data collection statutes, such as the Home Mortgage Disclosure Act. The agency would create a research and statistics unit to analyze and study the full range of consumer protection, fair lending and community development finance issues. The proposed legislation identifies the possible abuse of arbitration clauses in financial services' contracts and documents as one important area for study. The CFPA would determine the extent to which and in what contexts such arbitration clauses promote fair adjudication and effective redress.

The CFPA would also become the central location for consumer complaints about financial services, products and institutions. The agency would have subpoena power to inquire about business practices and enforce CFPA rules and regulations as to particular financial institutions.

The House Financial Services Committee is currently reviewing a draft of the legislation and expectations are that the bill will go to the Senate in the Fall.

---

questions specific to entities under FTC jurisdiction.

[11] The FTC's general compliance guide is available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf. Its template compliance program for low-risk businesses is available at http://www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf.

[12] Mr. Edelman is a partner in the antitrust and commercial litigation practices in Crowell & Moring's New York office. He was previously a Vice Chair of the Financial Services Committee.

The Proposed Credit Card Fair Fee Act of 2009

By Logan M. Breed and Leigh L. Oliver[13]

This summer, Congressman John Conyers (D – MI) and Senator Richard Durbin (D- IL) resurrected interchange fee legislation that failed to get much traction last year. The proposed legislation, the Credit Card Fair Fee Act of 2009 (the "Act"), would provide antitrust immunity for joint negotiations between merchants and providers of Electronic Payment Systems (EPS) over the interchange fees that those merchants must pay for credit and debit card transactions. The House version, H.R. 2695, was introduced by Congressman Conyers on June 4, 2009, and was immediately referred to the House Judiciary Committee, which is chaired by Congressman Conyers. The Senate version, S. 1212, was introduced by Senator Durbin on June 9, 2009, and was referred to the Senate Judiciary Committee.

These bills are based on the Credit Card Fair Fee Act of 2008, which was introduced by Congressman Conyers in March 2008, but never reached a vote on the House floor. The House Task Force on Competition Policy and Antitrust Laws held a hearing on Conyers' bill in May 2008 at which representatives from MasterCard, Visa, and organized merchant groups testified. The House Judiciary Committee marked it up in July 2008, and it was reported out by the Committee in October 2008. Senator Durbin introduced similar legislation in the Senate in June 2008, but it was never reported out of the Judiciary Committee.

Now Congressman Conyers and Senator Durbin are back, hoping to pass legislation that will enhance merchants' bargaining power vis-à-vis large providers of EPS. Both pending bills propose to allow for joint negotiations by merchants with large providers of EPS over the fees charged to merchants for routing credit card transactions through the EPS. Although both bills aim to standardize fees and terms in merchant-EPS provider agreements, the mechanics of doing so vary between the two bills. Here is how the key provisions of the bills line up:

	S. 1212 (Durbin Bill)	H.R. 2695 (Conyers Bill)
Coverage	Applies to EPS providers of 10% or more of all credit card/debit card payments in U.S.	Applies to EPS providers of 20% or more of all credit card/debit card payments in U.S.
Antitrust Immunity	Merchants who have or are seeking access to a covered EPS and the providers of a single EPS are permitted to jointly negotiate with respect to fees and terms of access.	Same as S. 1212.
Overseeing Authority	A three-judge panel (EPS Judges) appointed by the U.S. Attorney General and Chairman of FTC.	The U.S. Attorney General (AG).
Rate Setting Authority	EPS Judges can set rates based on decision-making guidelines, e.g., rates must "most closely represent[ ] the fees and terms that would be negotiated in a hypothetical perfectly competitive marketplace . . . ."	The AG cannot set rates, but must report to Congress and make a recommendation regarding how Congress should respond to rate negotiations.
Filing Requirements	All Voluntarily Negotiated Access Agreements (VNAAs) between merchants and EPS providers and supporting documentation must be filed with EPS Judges within 30 days of execution. In addition, there is an extensive and elaborate discovery process.	All VNAAs and supporting documentation must be filed with the AG within 30 days of execution. In addition, the 10 largest issuers, acquirers, and merchants for each covered EPS must file itemized costs and agreements (associated with provision of/access to EPS) with the AG.
Public Disclosures	All VNAA filings will be made public.	Same as S. 1212.

Just as was the case in the proposed 2008 legislation, powerful groups are aligning on both sides of the issue. Supporters of the legislation include retailers such as the National Restaurant Association, the National Association of Convenience Stores, and the National Retail Federation. Opponents include financial institutions, electronic payment systems, card networks, and many members of the antitrust bar.

The bills' proponents argue that merchants currently have little or no bargaining power against international credit card networks such as Visa and MasterCard, and that the legislation would enable merchants to negotiate lower fees. These supporters claim that although the merchants pay the interchange fees, the merchants' customers ultimately bear the cost of these fees. Therefore, they claim that a reduction in the fees will benefit consumers.

---

[13] Logan Breed and Leigh Oliver are associates in the Antitrust, Competition, and Consumer Protection practice group at Hogan & Hartson LLP. The firm represents American Express Company in various matters.

The National Retail Federation estimates that interchange fees "cost the average household more than $400 a year and total more than $48 billion annually."[14] However, the current bills do not include provisions that would require that merchants pass-on cost savings to consumers, and merchants previously opposed such provisions. Finally, even though the legislation would permit collusive behavior that would ordinarily violate the antitrust laws, some supporters argue that the Act would stimulate competition. Conyers stated that his bill will "enhance[] competition"[15] by allowing merchants to negotiate on a more even footing with large credit card companies.

Opponents of the legislation focus on the fact that the markets for electronic payments are two-sided markets, *i.e.*, they are economic networks with two distinct user groups (merchants and consumers) that provide benefits to both merchants and cardholders. While it will reduce the costs on one group (the merchants), the legislation may also inadvertently harm consumers because the credit card companies will have to raise the fees charged to its customers to offset the lost revenue from the merchants or reduce benefits provided to consumers, such as rewards programs. If an EPS network increased fees to cardholders (or reduced benefits), fewer consumers would use credit cards; and similarly, if an EPS network increased fees to merchants, fewer merchants would accept credit cards, and consumers would have fewer opportunities to use their cards. The Electronic Payments Coalition, a lobbying organization for credit unions, banks, and payment card networks, argued that under the Act, "American families will end up footing retailers' bills when it comes to accepting debit and credit cards."[16]

Opponents note that in 2003, Australia imposed a ceiling on credit card fees. A GAO report from May 2008, evaluating the Australian example, found that the effect of regulated interchange fees was reduced costs to merchants without any evidence of cost savings to consumers. In Australia, cardholders experienced reduced benefits and an increase in annual and other credit card fees.[17]

Moreover, the legislation's opponents argue that the exemption contemplated by the Act is inappropriate because it would be much broader than any of the current exemptions to antitrust law. These exemptions typically apply only to industries that are subject to a comprehensive regulatory regime, such as agricultural cooperatives that operate under the oversight of the Department of Agriculture, or groups that operate outside the market process, such as labor unions. Opponents argue that the Act "would simply operate as naked market intervention in favor of one set of market players seeking to minimize their overhead costs, likely to the detriment of consumers."[18]

Finally, the legislation's opponents point out that industry-specific antitrust exemptions are generally disfavored because, as the Antitrust Modernization Commission noted in 2007, they tend to "harm the U.S. economy and, in the long run, reduce the competitiveness of the industries that have sought antitrust exemptions."[19] The antitrust agencies in the current administration also do not generally support industry-specific antitrust exemptions. In her Senate confirmation testimony, Christine Varney, Assistant Attorney General for the Antitrust Division, stated that "antitrust exemptions are not generally favored."[20] In 2008, both the Justice Department and the Federal Trade Commission opposed the bill.[21] As the Justice Department's letter explained, "The antitrust laws are the chief legal protector of the free-market principles on which the American economy is based. Companies free from competitive pressures have incentives to raise prices, reduce output, and limit investments in expansion and innovation to the detriment of the American consumer." The Justice Department also opposed the "price control" provisions of the bill: "The Department does not support the creation of a regulatory panel to set rates and terms of access. Generally, regulation should be confined to the fewest areas possible, and even then should be narrowly tailored to address a clearly demonstrated market failure." As the Justice Department noted, rate regulation is typically reserved for natural monopolies, such as regulated public utilities, and no one has demonstrated that EPS is an example of a market failure. However, neither the Justice Department nor the FTC has taken a position on the 2009 bills.

While the 2009 versions of the Conyers and Durbin bills still face significant opposition, the results of last November's elections and the current economic downturn have created a much different political climate in Washington as compared to a year ago. These changes have already affected credit card issuers – earlier this summer, Congress approved substantial new regulations limiting finance charges and interest rate increases to benefit consumers at the expense of the credit card industry with the Credit Card Accountability and Responsibility Act of 2009. Although the interchange fee bill raises very different issues and the abrogation of the antitrust laws may create broader unintended consequences, Congress' recent willingness to enact more

---

[14] National Retail Federation, "NRF Welcomes Senate Bill on Hidden Fees as Next Step in Credit Card Reform," June 9, 2009, available at http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=736.

[15] "Dead in '08, Back in '09: Congress Reintroduces an Interchange Bill," Digital Transactions News, June 8, 2009, available at http://www.digitaltransactions.net/newsstory.cfm?newsid=2232.

[16] Electronic Payments Coalition, "Electronic Payments Coalition Opposes Chairman Conyers Interchange Legislation," June 4, 2009, available at http://www.electronicpaymentscoalition.org/downloads/statement_epc090604.pdf.

[17] Government Accountability Office, *Credit and Debit Cards*, 10, 39-41 (May 2008), available at http://www.gao.gov/new.items/d08558.pdf.

[18] Letter from Timothy J. Muris, et al., to Congressman John Conyers, Jr., "H.R. 5546 Credit Card Fair Fee Act of 2008," July 14, 2008.

[19] Antitrust Modernization Commission Report, April 2007, at 335, available at http://govinfo.library.unt.edu/amc/report_recommendation/amc_final_report.pdf.

[20] "Answers to Questions for the Record, Confirmation Hearing of Christine A. Varney.

Before the Senate Judiciary Committee," March 10, 2009, at 3, available at http://judiciary.senate.gov/nominations/ChristineVarney/upload/QFRsSpecter.pdf.

[21] Letter from Keith Nelson, Principal Deputy Assistant Attorney General, June 23, 2008; Letter from William Kovacic, Chairman of the Federal Trade Commission (former), June 19, 2008.

stringent regulation of credit card issuers may be a sign of increased support for legislation that is intended arguably to benefit consumers and small merchants at the expense of the large EPS providers.

The Insurance and Financial Services Committee Newsletter is published 2-3 times a year by the American Bar Association Section of Antitrust Law Insurance and Financial Services Committee. The views expressed in the Insurance and Financial Services Committee Newsletter are the authors' only and not necessarily those of the American Bar Association, the Section of Antitrust Law or the Insurance and Financial Services Committee (or its subcommittees). If you wish to comment on the contents of the Insurance and Financial Services Committee Newsletter, please write to the American Bar Association, Section of Antitrust Law, 321 North Clark Street, Chicago, IL 60654-7598