

What happened?

ONLY A SHORT TIME AGO, CREDIT CARD lending was not of extraordinary concern to regulators, legislators, or community activists. Fair lending and predatory lending scrutiny, for example, was reserved for mortgage lending. While the fair lending focus still largely remains on mortgage lending due to the availability of Home Mortgage Disclosure Act (HMDA) data, credit card lenders have experienced increased oversight by all parties of their fair lending activities. Due to recent Reg. B amendments, credit card lenders may now choose to obtain race/sex data from credit card applicants for fair lending testing purposes. Most (if not all) card issuers have elected not to collect such data and to maintain the status quo. However, the increased focus on fair lending in the card industry in one example of reorganization in the regulatory landscape.

It would take volumes (and several days' reading time) to detail the myriad regulatory requirements applicable to credit card lenders. Accordingly, this article will focus on regulatory and environmental changes that affect the card industry and card compliance.

As credit card compliance professionals, what challenges and opportunities face us today?

Since 2002, credit card issuers have faced mounting federal and state legislation, especially in privacy, data protection, and telemarketing. To compound matters, new requirements were layered upon existing federal laws, which include Truth in Lending (Reg. Z); Equal Credit Opportunity Act (Reg. B); Fair Credit Reporting Act (FCRA); and state consumer, debt collection, tax, and other laws. State regulatory mandates continue to be particularly difficult to manage because of the lack of uniformity and the difficulties of keeping abreast of new or changed requirements.

In December 2002 we began our journey through the changing regulatory landscape by welcoming the new (and improved?) Telemarketing Sales Rule (TSR). The new TSR spawned "expressed informed consent" and broadened the regulatory requirements to include inbound call "cross-sell-

ing" or "up-selling." The rule also brought us the notorious National Do Not Call Registry, which has continued to receive substantial media and political coverage. Unfortunately for credit card issuers who have been in the business of telemarketing or cross-selling, the news media and politicians trumpeted the National Do Not Call Registry as the long-awaited respite from all telemarketing calls. Few of these "trumpeters" chose to become familiar with the TSR's exemptions for established business relationships, charitable organizations, and political contribution solicitations. Because of the resulting confusion and misinformation, call center volume and complaints from customers, as well as placements on companies' own do-not-call lists, increased. To further complicate matters, the FTC and FCC did not provide reasonable implementation time for the new TSR disclosure requirements, as the revised disclosures became effective April 1, 2003.

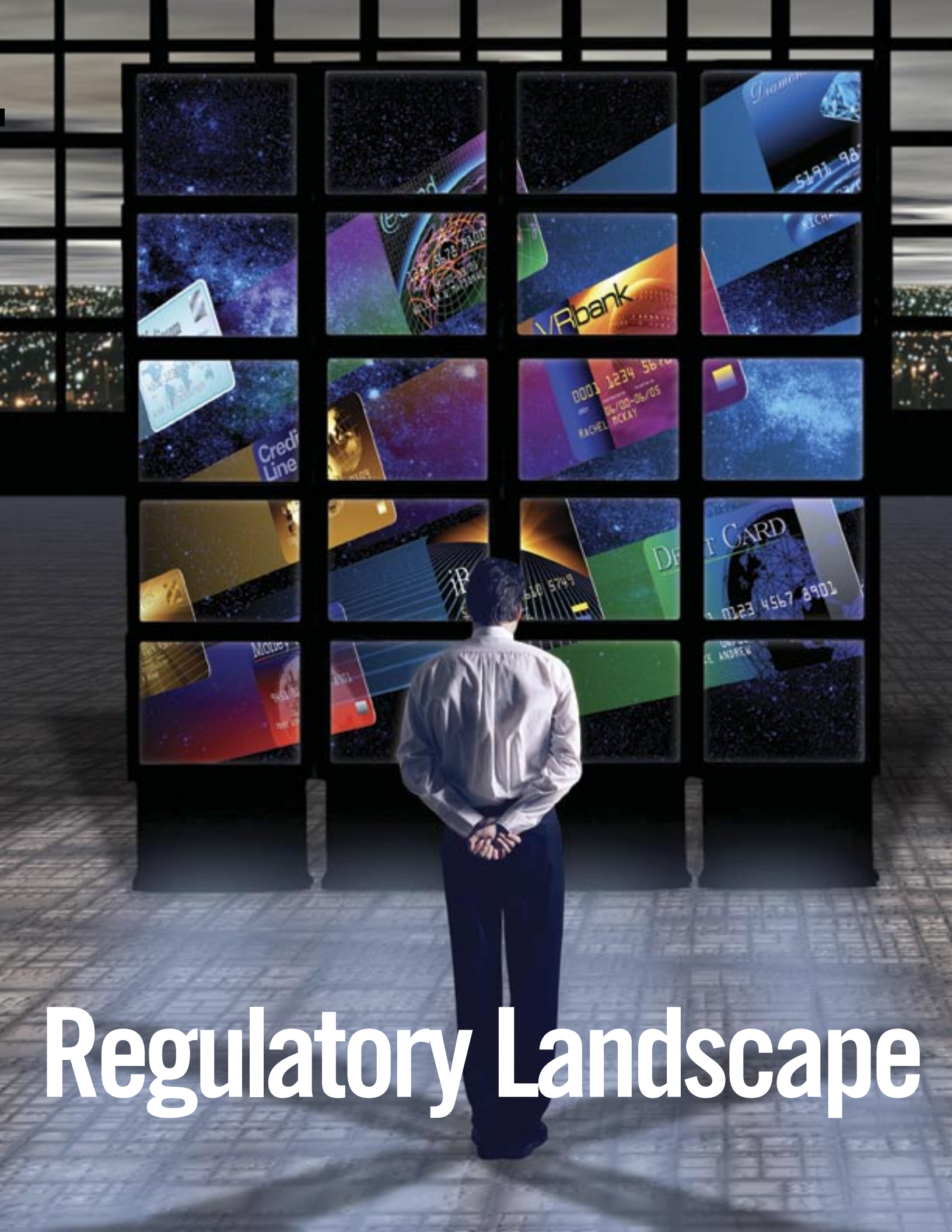
Less visible, but equally important, are provisions of the new Telemarketing Sales Rule that included new restrictions on the use of automatic dialers and abandoned calls as well as caller identification requirements.

Following closely behind the new Telemarketing Sales Rule requirements were new Reg. B mandates. In March 2003, the Federal Reserve revised Reg. B to establish new record retention requirements for prescreened credit solicitations. These requirements became effective April 15, 2003, with a mandatory compliance date of April 15, 2004. A 25-month retention period (12 months for business credit) was established for prescreened application text, lists of criteria the creditor used to select potential recipients of the solicitation, and any correspondence (e.g., letters, e-mail, or faxes) related to complaints about the solicitation. Lenders are now required to retain correspondence related to complaints on prescreened solicitations in a way that provides reasonable accessibility to examiners.

The final rule amending Reg. B also retained the prohibition against inquiring about or noting applicant characteristics for nonmortgage credit transactions while creating an excep-

MASTERFILE / BRANDX / BONOTOM STUDIO

The New Credit Card



Regulatory Landscape

Since 2000, credit card lenders have paid over \$600 million to settle lawsuits Federal Trade Commission (FTC) Act, the Truth in Lending Act, Fair Debt

tion that allowed collection of race/sex data when the purpose of collecting the data was for a self-test for fair lending. As mentioned earlier, few, if any, credit card issuers accepted the Federal Reserve's generous offer to obtain applicant personal data for fair lending test purposes.

In December 2003, the Federal Reserve announced advance notice of rulemaking for privacy notice revisions under the Gramm-Leach-Bliley Act. Card issuers were welcomed into 2004 with the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), the CAN-SPAM Act, and proposed rules by the Federal Reserve Board to establish more uniform standards for providing disclosures for five consumer protection regulations (B, E, M, Z, and DD). Card companies were also requested by the Federal Reserve to provide guidance on debt cancellation insurance and how it differs from credit insurance.

Credit card issuers have been bombarded with new regulations, changes to existing regulations, and requests for input to existing regulations. Meanwhile, the regulatory landscape experienced a landslide of class-action litigation that focused on unfair and deceptive practices as well as technical violations of the law.

One of the most critical regulatory issues impacting credit card lenders has been ensuring fairness and clarity of information provided to consumers. Since 2000, credit card lenders have paid over \$600 million to settle lawsuits and regulatory actions tied to unfair or deceptive acts and practices under the Federal Trade Commission (FTC) Act, the Truth in Lending Act, Fair Debt Collection Practices Act, and other applicable federal and state laws. Unfair or deceptive practices targeted by federal and state regulators included improper disclosure of fees, unauthorized enrollment in products and services, unscrupulous debt collection practices, payment posting delays, and improper interest charges (e.g., predatory lending). In March 2002, the Office of the Comptroller of the Currency (OCC) issued an Advisory Letter (AL 2002-3) that provided guidance to lenders on the types of activities that pose the greatest risk of being viewed as unfair or deceptive. In March 2004, the Federal Reserve and FDIC issued guidance on unfair or deceptive acts or practices by state chartered banks. Both of these pronouncements should be required reading for anyone in a credit card organization who develops or implements marketing, telemarketing, or risk initiatives to enhance revenue.

Another critical area for card compliance has been the explosion of class-action litigation. Class-action litigation has targeted the accuracy of terms and conditions of products or services, and the authenticity of what is disclosed to consumers versus what is actually done by the credit card lender. The litigation tends to focus on the accuracy and clarity of initial disclosures, solicitations, and card member agreements, as well as any subsequent notifications to customers (e.g., annual privacy notices, change in terms notices, etc.), and these are areas that should be foremost in every card compliance professional's risk analysis. Class action suits attacking foreign exchange fee disclosures abound. In addition, numerous class-action suits have been filed against card issuers for alleged sale of customer and account information to third-party marketers.

The validity of mandatory arbitration clauses in card member agreements has also been the subject of litigation.

Truth in Lending Act (Reg. Z) compliance oversight has migrated from periodic examination by federal banking regulators, which typically resulted in relatively minor infractions and isolated reimbursements, to detailed investigation, analysis and scrutiny by plaintiffs' attorneys and attorneys general seeking class-action status. Fairness has replaced legality in the eyes of regulators, litigators, and customers. Accordingly, card issuers must maintain a maniacal focus on the true meaning and intent of what is fair and develop a "customer-centric" expertise in the requirements of Reg. Z:

- 1) that borrowers be provided information on credit terms, including costs of credit
- 2) that a credit card be issued only with an oral or written request or application for credit (or as a replacement or renewal card)
- 3) that we conform to the provisions for liability for unauthorized use of a credit card.

The prompt resolution of billing disputes, in particular, has received negative press as well as litigation for card issuers' failure to perform a "reasonable investigation" of these disputes. Prompt resolution of billing errors is not only a regulatory requirement, but it is also a necessity to differentiate quality of service. Many card issuers provide similar products and services to consumers, so service differentiation is key to holding consumer loyalty. Any practice that could be perceived by a consumer (or a judge or jury) to be unfair or deceptive should receive a compliance professional's highest attention.

Credit card compliance professionals have experienced much anguish and many sleepless nights over customer information protection and data privacy rules and regulations. The use and protection of customer data has driven many of the new regulatory requirements that impact card issuers. The Gramm-Leach-Bliley Act (GLBA), the FACT Act (and FCRA), the USA PATRIOT Act, California and Texas identity theft legislation, and the California Security Breach Notification Act established standards for how, when, why, and for what purposes card issuers (and others) obtain, use, and protect customer data.

In May 2002, Section 501(b) of the GLBA provided guidelines for implementing information security standards to ensure the security and confidentiality of customer information and to protect against threats or unauthorized access to customer information. In addition, Section 503 of the GLBA requires financial institutions to provide to each customer a notice that describes the institution's policies and procedures regarding the disclosure to third parties of nonpublic personal information. The privacy rule under Section 502 of the GLBA provided that the privacy notices explain the consumer's right to opt out of sharing nonpublic personal information. Now, about four years later, we are faced with potential changes to the privacy notice. It has become apparent that the intended purpose of providing clear, meaningful information on data privacy choices to consumers has not been achieved. Additional time and energy will be needed to resolve this issue.

Layered onto GLBA information protection requirements were the Fair and Accurate Credit Transactions Act (FACT) Act, the California

and regulatory actions tied to unfair or deceptive acts and practices under the Collection Practices Act, and other applicable federal and state laws.

Security Breach Notification Act (SB 1386), and the California and Texas identity theft acts.

While data protection has been paramount, the accuracy of credit report information and responsibilities for properly managing this data have been re-emphasized in the current regulatory environment. The FCRA and the new FACT Act assign responsibility to creditors and credit bureaus for providing and maintaining accurate credit information.

The FACT Act provided permanent preemption for seven existing FCRA provisions that block states from enacting more stringent laws on the use, sharing, and reporting of consumer credit information. The act also provided permanent preemption of some state identity theft and information-sharing laws. Conversely, the FACT Act established new restrictions on the ability to market freely to customers of affiliates if the customer opts out. In addition, lenders must adhere to new guidelines to be issued by regulators for detecting identity theft and must provide new notices to customers who receive loan terms worse than those generally available based on credit bureau data.

The California Security Breach Notification Act required companies doing business in California that own or license computerized data to notify California customers or employees if their personal information has been compromised by a computer security breach. The requirements of the California and Texas identity theft acts are substantially similar. Under both laws, consumers may request that credit bureaus place security alerts or freezes on their credit lines. The California Identity Theft Act (SB 168) has no specific enforcement or penalty provisions, whereas the Texas act levies a civil penalty of up to \$2,000 per violation.

Despite the extensive regulatory guidance and requirements for data protection, information security, and data accuracy, the FTC received more than 500,000 consumer complaints of identity theft during 2003. The number of actual identity thefts may be much larger than reported, as some victims choose not to file formal complaints. The significant and ever-increasing focus on information protection by consumers (as well as banking regulators) should be a wake-up call for all card issuers.

How could one forget the USA PATRIOT Act and Customer Identification Program (CIP) requirements? On October 1, 2003, the CIP requirements in Section 326 of the USA PATRIOT Act became effective. The CIP requirements were implemented in response to terrorist activities and require financial institutions to obtain sufficient identification information from customers at account opening to reduce the likelihood of doing business with terrorists.

Along with existing Bank Secrecy Act (BSA) and Office of Financial Assets Control (OFAC) requirements, the USA PATRIOT Act creates ongoing monitoring and reporting requirements that subject card issuers to significant financial and reputation risks. The penalties for noncompliance are among the most significant in the regulatory scheme.

Other areas of focus for credit card compliance professionals should be the CAN-SPAM Act and the exponential growth in use of service providers by credit card lenders.

The CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act became effective January 1, 2004. The key provisions of CAN-SPAM include restrictions on sending deceptive or misleading e-mail messages; notification that an e-mail is an advertisement; inclusion of an opt-out notice and effective mechanisms to process the opt-out request within 10 days; inclusion of the sender's physical postal address in the e-mail; prohibition on transfer of e-mail addresses to other senders; and the establishment of a national "do-not-e-mail" directory by the FTC. Because e-mail has become an increasingly cost-effective communication and marketing channel for card issuers, CAN-SPAM should be a focus area for credit card lenders.

If your institution utilizes third-party service providers to process transactions or perform customer service (particularly off-shore), your risk of noncompliance with each of the regulatory requirements mentioned in this article is magnified. The use of third-party service providers has received substantial (and ever-increasing) regulatory and political attention. Banking regulatory agencies have provided guidance on the proper oversight of third party agencies to help ensure compliance (e.g., OCC Bulletin 2001-47, OCC Bulletin 2002-16, OCC Bulletin 2001-31, OTS TB-82, and the FFIEC's "Risk Management of Outsourced Technology"). Appropriate due diligence and a sound compliance risk management program (e.g., appropriate training, ongoing monitoring, capturing and resolving customer complaints, and reporting) for third-party service providers are must-haves. Customer data protection, particularly in an outsourcing relationship, is imperative and has become a primary focus of bank examiners and an increasing concern for consumers.

Wherever a credit card lender chooses to do business, it is clear that there are many opportunities-and regulatory, litigation, operational, and reputation risks-facing the industry. With the looming threat of litigation, there is little margin for error. As credit card compliance professionals, our mission (not an easy one by any means) must be to effectively and efficiently navigate the maze of federal and state regulatory requirements and somehow maintain our sanity. Credit card compliance is indeed a new world only for the brave. Good luck. **EC**

ABOUT THE AUTHOR

Mark W. McMillian, CBA, CIA, CRCM, serves as compliance director at American Express and brings more than 20 years in financial services compliance and internal auditing to his position. He is on the faculty at the ABA National Compliance School where he instructs the credit card curriculum that he developed for the school. Mr. McMillian has also served on the ABA's National Regulatory Compliance Conference Planning Committee and as a presenter at the National Conference. He has also served as Compliance Committee Chairperson for the Virginia Bankers Association and has provided his compliance insight to the OCC regarding fair lending programs in financial institutions. He can be reached by telephone at (336) 668-6430 or via e-mail at mark.w.mcmillian@aexp.com.