MORRISON | FOERSTER

Legal Updates & News

Bulletins

Washington Update

June 2007

Privacy Bulletin -- June 11, 2007

By L. Richard Fischer and Ivan J. Flores

In an effort to keep our clients and friends apprised of federal legislative and regulatory initiatives regarding data privacy and security, we are providing this update of recent activity in Congress and the agencies. In this alert, we discuss several bills introduced in the House and Senate addressing data safeguards, security breach notification, privacy notices, and credit file freezes. We also discuss federal agency initiatives intended to strengthen pretexting prohibitions, the recently announced Strategic Plan of the President's Identity Theft Task Force, a new bank agency supervisory policy on identity theft, and various enforcement actions, reports and workshops.

Congressional Focus

Legislation Introduced To Protect Against Identity Theft

On March 26, 2007, Representative Tom Price (R-GA) introduced the "Data Security Act of 2007" (H.R. 1685), which is intended to enhance existing protections against data security breaches by applying a uniform standard for protection against, and disclosure of, potential security breaches. More specifically, H.R. 1685 would:

- Require companies and financial institutions to protect the security of sensitive information relating to consumers and to provide notice to consumers in the event there is a security breach involving this sensitive information.
- Provide a risk-based trigger, based on the Gramm-Leach-Bliley Act ("GLBA"), under which a security breach notification would be based on the likelihood that consumer information that is acquired without authorization will be misused for identity theft or account fraud.
- Require the GLBA regulators to harmonize their regulations with the details of H.R. 1685.
- Establish national uniformity with respect to data security or security breach notification.
- Apply to federal agencies that maintain sensitive personal information or sensitive account information.

Legislation Introduced To Protect Small Businesses

On April 19, 2007, Representative Peter J. Roskam (R-IL) introduced legislation that would provide regulatory relief for community and independent banks. The "Financial Privacy Notice Relief Act of 2007" (H.R. 1967) would assist in reducing unnecessary costs for banks and consumers and allow the banks to continue to compete in the larger financial services arena.

According to Representative Roskam, H.R. 1967 would remove an unnecessary and costly stipulation under Title V of the GLBA, which requires annual privacy notices to be provided to all consumers. Under Title V of the GLBA, notices are required regardless of whether an institution's privacy practices have changed and regardless of whether the company shares customer financial information.

"While this is a well intentioned protection of consumer privacy for financial institutions that share consumer information, this creates the unintended mandate to force smaller banks to spend money every year drafting,

printing and mailing privacy statements to consumers when their information has not been shared, nor has their private policy changed," Representative Roskam stated. Representative Roskam further stated that "consumers don't want these notices, most find the notices annoying and burdensome, rather than beneficial."

Legislation Introduced To Combat Identity Theft

On April 20, 2007, Senator Ted Stevens (R-AK) introduced the "Identity Theft Prevention Act" (S. 1178), which would strengthen information safeguards and ensure consumers are notified if their sensitive personal information is acquired without authorization.

S. 1178 also would direct the Federal Trade Commission ("FTC") to enforce rules that would require all covered entities that handle sensitive personal information to develop, implement and maintain appropriate safeguards to protect such information, and provide effective notice to consumers in the event of a breach involving that information. In addition, S. 1178 would allow consumers to freeze their credit files for a reasonable fee to protect themselves from identity theft.

Specifically, S. 1178 would:

- Require businesses that handle sensitive personal information to comply with existing requirements of the FTC's rules that currently apply to financial institutions. These rules require covered entities to develop, implement and maintain a written program for the security of sensitive personal information, and to protect against any anticipated threats and protect against unauthorized access to such sensitive information.
- Direct the FTC to develop rules that would require procedures for authenticating the credentials of third parties to whom or to which sensitive personal information is to be transferred or sold.
- Require all entities that handle sensitive personal information to provide notice to affected consumers in the event that a security breach creates a reasonable risk of identity theft.
- Allow consumers to place, lift, or temporarily remove a security freeze on their credit files, which would reduce identity theft by preventing credit from being extended to third parties without authorization from the consumer.
- Allow state attorneys general ("AGs") to bring actions under S. 1178, and in the place of the FTC, in either a state or district court on behalf of their residents. The AGs would be required to notify the FTC or the appropriate federal functional regulator prior to bringing the action, and the FTC or appropriate federal functional regulator would have the authority to intervene in the action.
- Preempt any state or local law that requires a covered entity to safeguard sensitive personal information or requires the notification of consumers of security breaches involving their sensitive personal information.
- Establish an Information Security and Consumer Privacy Advisory Committee comprised of industry participants, consumer groups, and AGs to develop best practices to protect sensitive personal information.
- Require the FTC and the Department of Justice to conduct a study of the correlation between methamphetamine use and identity theft crimes.

Senator Calls For Crackdown On Security Breaches

On April 24, 2007, Senate Finance Committee Chairman Max Baucus (D-MT) called for a crackdown on accidental releases of Social Security numbers ("SSNs") to the public. In a letter to the Director of the Office of Management and Budget ("OMB"), Senator Baucus condemned two recent security breaches involving thousands of SSNs on a U.S. Department of Agriculture Web site and printed on outgoing FEMA mail. Senator Baucus, whose Committee oversees Social Security policy, requested a report from the OMB on the investigation into the recent breaches and on steps being taken to secure the personal information of U.S. citizens at federal agencies.

According to Senator Baucus, "[i]t seems some Federal agencies still don't get how sensitive Social Security numbers are. But identity theft is already rampant in our country, and I'd rather the government didn't offer crooks any extra help." Senator Baucus also stated that "Congress has passed significant legislation to protect Americans' private information, but these episodes show that more needs to be done. I want to know what's being done to investigate these breaches, and what's being done to keep this from happening again."

Legislation Introduced To Protect Consumers From ID Theft

On May 1, 2007, Senator Tom Carper (D-DE) joined fellow Senate Banking Committee member Bob Bennett (R-UT) in introducing legislation intended to help protect consumers and businesses from identity theft and

account fraud. The "Data Security Act of 2007" (S. 1260) would require entities to safeguard sensitive information and notify consumers of a security breach that is likely to lead to identity theft and cause serious harm.

S. 1260 would require "financial establishments," retailers and federal agencies to safeguard sensitive information, investigate security breaches, and notify consumers when there is a substantial risk of identity theft or account fraud. According to the Senators, that means retailers who take credit card information would be covered; data brokers who compile private information would be covered; and government agencies that possess nonpublic personal information also would be covered. The Senators note that S. 1260 is modeled after the data security breach-response regime established under the GLBA and subsequent banking agency regulations.

Regulatory Efforts

FCC Strengthens Privacy Rules On Pretexting

On April 2, 2007, the Federal Communications Commission ("FCC") announced that it has strengthened its privacy rules by requiring telephone and wireless carriers to adopt additional safeguards to protect the personal telephone records of consumers from unauthorized disclosure. According to the FCC, the new safeguards will help prevent unauthorized access to customer proprietary network information ("CPNI").

The new safeguards include:

- **Carrier Authentication Requirements.** Carriers are prohibited from releasing telephone call records of customers when a customer calls the carrier except when the customer provides a password. If a customer does not provide a password, carriers may not release the telephone call records of a customer except by sending it to an address of record or by the carrier calling the customer at the telephone number of record. Carriers are required to provide mandatory password protection for online account access and are permitted to provide all CPNI, including customer telephone call records, to customers based on in-store contact with a valid photo ID.
- **Notice to Customer of Account Changes.** Carriers are to immediately notify the customer when the following are created or changed: (1) a password; (2) a back-up for forgotten passwords; (3) an online account; or (4) the address of record.
- **Notice of Unauthorized Disclosure of CPNI.** A notification process is established for both law enforcement and customers in the event of a CPNI breach.
- **Joint Venture and Independent Contractor Use of CPNI.** Consent rules are modified to require carriers to obtain explicit consent from a customer before disclosing a customer's CPNI to a carrier's joint venture partners or independent contractors for the purposes of marketing communications-related services to that customer.
- **Annual CPNI Certification.** Certification rules are amended to require carriers to file with the FCC an annual certification, including an explanation of any actions taken against data brokers and a summary of all consumer complaints received in the previous year regarding the unauthorized release of CPNI.
- **CPNI Regulations Applicable to Providers of Interconnected VoIP Service.** All CPNI rules are extended to cover providers of interconnected Voice over Internet Protocol ("VoIP") service.
- **Business Customers.** In limited circumstances, carriers may bind themselves contractually to authentication regimes other than those adopted in the order for services they provide to their business customers that have dedicated account representatives and contacts that specifically address the carrier's protection of CPNI.

FTC Submits Do-Not-Call Report To Congress

On April 5, 2007, the FTC approved the issuance of a report to Congress regarding the Do-Not-Call Registry ("DNC Registry") for the Fiscal Year 2006. The report was submitted to the House Committee on Energy and Commerce and Senate Committee on Commerce, Science, and Transportation, pursuant to section 4(b) of the Do-Not-Call Implementation Act.

According to the FTC, the report contains information on the following topics:

1. An analysis of the effectiveness of the DNC Registry;
2. The number of consumers who have placed their telephone numbers on the DNC Registry;
3. The number of entities paying fees to access the DNC Registry and the amount of the fees;
4. The progress of coordinating the operation and enforcement of the DNC Registry with similar registries maintained by the states;

5. The progress of coordinating the operation and enforcement of the DNC Registry with enforcement activities of the FCC under the Telephone Consumer Protection Act; and
6. FTC enforcement of the DNC Registry under the Telemarketing Sales Rule.

FTC Obtains Judgement Against Cross-Border Scammer

On April 9, 2007, the FTC announced that a federal district court in Seattle, Washington, has entered an order for permanent injunction and other relief against a Canadian con-man whom the FTC charged with targeting elderly U.S. consumers with bogus bond pitches and unfulfilled promises of money. The order bars the scammer from engaging in similar illegal conduct in the future, as well as from calling consumers whose telephone numbers are on the DNC Registry. The order also requires the scammer to pay $4.75 million for use in providing refunds to the consumers who bought his fake bonds.

The court order resolves the FTC's charges that the defendant falsely promised consumers that if they purchased bonds, they would be entered into a monthly drawing and that they were likely to receive substantial cash winnings or receive regular cash payments. Few consumers received such payments after buying the nonexistent bonds, leading the FTC to charge the defendant with violating the Federal Trade Commission Act ("FTC Act") and the Telemarketing Sales Rule ("TSR"). The defendant also was charged with illegally calling consumers on the National DNC Registry maintained by the FTC and the FCC.

According to the FTC's complaint, the defendant violated section 5 of the FTC Act and the TSR by telemarketing fake foreign bonds to U.S. consumers. Specifically, the defendant misrepresented that consumers who bought from, or paid fees to, the defendant would receive regular cash payments, would be entered into monthly drawings to win cash prizes, and were highly likely to receive cash winnings. Further, the FTC charged that the defendant failed to disclose to consumers that importing and trafficking in foreign lotteries is a crime in the U.S. and that the bond scheme he was pitching constituted such a lottery. Finally, the FTC's complaint charged the defendant with violating the DNC Registry provisions of the TSR by calling, or causing other people to call, telephone numbers on the DNC Registry, as well as failing to pay the required fees to access telephone numbers in the area codes he and his telemarketers called.

Among other things, the judgment and order permanently bars the defendant from violating the TSR, including making any calls to telephone numbers on the FTC DNC Registry or causing anyone else to do so. The order also contains monitoring provisions to ensure the defendant's compliance, bars the defendant from selling or transferring his customer lists to anyone else, and within 10 days of the order's entry by the court requires him to pay $4.75 million to the FTC for consumer redress.

FDIC Issues Supervisory Policy On Identity Theft

On April 11, 2007, the Federal Deposit Insurance Corporation ("FDIC") issued its "Supervisory Policy on Identity Theft," which describes the characteristics of identity theft. The policy also sets forth the FDIC's expectations that financial institutions under its supervision will take steps to detect and prevent identity theft and mitigate its effects in order to protect consumers and help ensure safe and sound operations of FDIC-regulated financial institutions.

In particular, the Guidance indicates that financial institutions under the supervision of the FDIC should:

- Properly safeguard and dispose of consumer information;
- Use stronger and more reliable methods to authenticate the identity of customers using electronic banking systems;
- Comply with emerging information technology guidance and the requirements of the Bank Secrecy Act;
- Ensure compliance with the Fair Credit Reporting Act's fraud and active duty alert provisions and requirements governing the accuracy of data provided to consumer reporting agencies; and
- Provide consumers with accurate, up-to-date information designed to educate them concerning steps to take to reduce their vulnerability to fraud.

FTC To Host Spam Summit

On April 18, 2007, the FTC announced that it will host a two-day public event, "Spam Summit: The Next Generation of Threats and Solutions," on July 11 and 12, 2007, in Washington, D.C. The summit will include experts from the business, government, and technology sectors, consumer advocates and academics to explore consumer protection issues surrounding spam, phishing and malware.

Topics include:

- Defining the Problem: Earlier findings indicated that most spam is fraudulent, deceptive and offensive. How has the nature of spam shifted? Is spam now being used for malicious and criminal purposes? Is spam reaching the inboxes of consumers or being filtered by filtering software of Internet service providers ("ISPs")?
- New Methods for Sending Spam: To what extent have e-mail address harvesting, dictionary attacks, and open proxies been replaced by botnets, zombies, and spam that uses images instead of text as the primary methods of spam distribution?
- The Covert Economy: What are the financial incentives for malicious spammers? To what extent does stolen information, such as government-issued identity numbers, credit cards, bank cards and personal identification numbers, user accounts, and e-mail addresses, play a role? What is the cost along the e-mail chain to consumers, businesses, ISPs, and networks?
- Deterring Malicious Spammers and Cybercriminals: What are the investigatory challenges faced by law enforcement as spammers mask their identities and use obfuscatory techniques? What are effective countermeasures?
- Emerging Threats: What emerging threats are occurring in media other than e-mail, including spam over instant messaging systems, spam over Internet telephony and spam to mobile devices?
- Technological Tools for Keeping it Out of the Inbox: During the FTC's 2004 E-mail Authentication Summit, co-hosted with the Department of Commerce's National Institute of Standards and Technology, the FTC initiated efforts to start the development and wide-scale adoption of domain level e-mail authentication. Where does the implementation of e-mail authentication stand? What are other key spam-reducing tools?
- Stakeholder Best Practices: What best practices should stakeholders adopt to reduce malicious spam and minimize its impact?

FTC Identity Authentication Workshop

On April 23 and 24, 2007, the FTC hosted a public workshop, "Proof Positive: New Directions in ID Authentication," to explore methods to reduce identity theft through enhanced authentication. The workshop included a discussion among public-sector, private-sector, and consumer representatives and focused on technological and policy requirements for developing better authentication processes, including the incorporation of privacy standards and consideration of consumer usability issues.

The FTC sought comment on ways to improve authentication processes to reduce identity theft, including:

- How can individuals prove their identities when establishing them in the first place?
- What are some current or emerging authentication technologies or methods and what are their strengths and weaknesses?
- To what extent do these technologies meet consumer needs, such as ease of use, and to what extent do they raise privacy concerns?

Identity Theft Task Force Releases Strategic Plan To Combat ID Theft

On April 23, 2007, the U.S. Attorney General and the FTC Chairman announced the completion of the President's Identity Theft Task Force Strategic Plan to combat identity theft. According to the FTC, although much has been done to combat identity theft, the specific recommendations outlined in the Strategic Plan are necessary to wage a more effective fight against identity theft and reduce its incidence and damage. Highlights of the recommendations include:

- Reduce the unnecessary use of SSNs by federal agencies;
- Establish national standards that would require private-sector entities to safeguard the personal data they compile and maintain and to provide notice to consumers when a breach occurs that poses a significant risk of identity theft;
- Implement a broad, sustained awareness campaign by federal agencies to educate consumers, the private sector, and the public sector on methods to deter, detect and defend against identity theft; and
- Create a National Identity Theft Law Enforcement Center to allow law enforcement agencies to coordinate their efforts and information more efficiently, and investigate and prosecute identity thieves more effectively.

The Task Force's recommendations also include several legislative proposals designed to fill the gaps in current laws criminalizing the acts of many identity thieves, and ensure that victims can recover the value of the time lost attempting to repair damage inflicted by identity theft. These proposals include the following actions:

- Amending the identity theft and aggravated identity theft laws to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted;

- Adding new crimes to the list of offenses that will subject those criminals to a two-year mandatory sentence available under the “aggravated identity theft” law;
- Amending existing laws to assure the ability of federal prosecutors to charge those who use malicious spyware and keyloggers; and
- Amending the cyber-extortion law to cover additional, alternate types of cyber-extortion.