

# The Impact of The USA PATRIOT Act On Business

**Dan Davidson**

Professor of Business Law  
Radford University  
Radford, Virginia

(540) 831-5071

ddavidson@radford.edu

*The USA PATRIOT Act is an extremely controversial statute. Much has been written about its impact on individual rights and civil liberties. Literally dozens of articles have addressed the seeming conflict between this act and the Constitutional protections afforded to U.S. citizens by the Bill of Rights. However, little attention has been paid to the impact of the Act on business. The USA PATRIOT Act is a broad, wide-ranging statute that could affect virtually every business — and businessperson — in the United States. Several of the areas that have the most significant impact on business will be addressed in this paper.*

On October 26, 2001— a mere 45 days after the devastating terrorist attacks of 9-11 — Congress responded by enacting “The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act,” better known as the USA PATRIOT Act.<sup>1</sup> This Act, 342 pages long, reformed and extended the powers of our international intelligence agencies and of our law enforcement agencies in order to facilitate the fight against terrorism, no matter where the terrorists are located or under what name they operate. The expressed purpose was, and still is, a noble objective, and few people in this country would quibble with these objectives of the Act.

However, the Act has other aspects, some of which are relatively well known and others of which many Americans seem to be unaware. A few of these “other aspects” have created a great deal of concern across society. For example, there are some provisions of the Act that effectively deny some of our basic civil liberties and civil rights to persons suspected of committing acts of terrorism, and to those who are suspected of aiding and abetting terrorists or terrorism. That topic has been covered in a plethora of articles and op-ed pieces, often negatively. “Among its detractors are 152 communities, including several major cities and three states, that have

now passed resolutions denouncing the Patriot [sic] Act as an assault on civil liberties.<sup>2</sup>

But other aspects of the Act have not generated such discussion or such passion in society. Nonetheless, a number of these other aspects directly affect business, which, in turn, affects most of our society. It is these aspects, the ones affecting business, which are the focus of this paper. What does the USA PATRIOT Act do to business? What does the USA PATRIOT Act require of business? What must businesses and businesspersons do in order to comply with the relevant provisions of the Act? Those are the questions that are addressed below.

## **Title III: Anti-money Laundering Provisions and the Financial Services Industry**

Probably the area of business affected most directly by the USA PATRIOT Act is the financial services industry. Title III of the USA PATRIOT Act is the “International Money Laundering Abatement and Anti-Terrorism Financing Act of 2001.” This portion of the Act expands the definition of money laundering and also expands the role of the financial services industry in combating money laundering. Among the increased responsibilities imposed on the financial services industry is a redefining of due diligence, more

emphasis on “knowing one’s customers,” and heightening the duties of banks in their dealings with correspondent banks and private banks.<sup>3</sup> Initially the anti-money laundering provisions of the Act only applied to “traditional” financial services businesses (banks, savings and loan associations, credit unions, registered brokers and dealers in securities, futures commission merchants, money services businesses, operators of credit card systems, and mutual funds), with other financial services institutions (dealers in precious metals, stones, or jewels; pawnbrokers; loan or finance companies; private bankers; insurance companies; travel agencies; telegraph companies; businesses engaged in vehicle sales; and others) deferred until October 4, 2002.<sup>4</sup> (The deadline for compliance was subsequently extended to October 1, 2003.<sup>5</sup>)

Money laundering is big business. Many people think that money laundering is the exclusive province of drug dealers and organized crime.<sup>6</sup> While drug dealers and organized crime are involved in money laundering, they are not alone. In fact, money laundering is reputed to be the world’s largest business, involving more than \$1 trillion annually, with at least half of the funds passing through U.S. financial institutions.<sup>7</sup> (At least one estimate puts the volume of “business” in money laundering as high as \$1.5 trillion annually.<sup>8</sup>) At least a portion of those funds are believed to be used by terrorist groups, and the government decided that in order to prevent future terrorist attacks it had to be able to discover the money trails terrorists used.<sup>9</sup> Thus, “[t]he events of September 11 put financial institutions in the front lines of the war on terrorism, asking them to detect patterns of financial activity that might indicate an objective to engage in terrorist acts.”<sup>10</sup> “The idea is that terrorist threats to the U.S. will be thwarted if the government is able to ‘follow the money.’”<sup>11</sup>

One major provision of the law can be found in § 326, which amends the Bank Secrecy Act,<sup>12</sup> “Identification and Verification of Account Holders.” This amendment allows the Secretary of the Treasury to prescribe regulations that set forth the minimum standards for

financial institutions and their customers for establishing the identity of a customer opening a new account at a financial institution. These regulations establish that, at a minimum, a financial institution must collect a name, address, birth date, and taxpayer identification number from each person who opens an account, including partnerships, trusts, and corporations.<sup>13</sup> The information obtained at the time an account is opened must be maintained for at least five years. The financial institution must also cross-reference the information obtained from any new customer against lists of known or suspected terrorists or terrorist organizations provided by various government agencies, and must notify the agency if a name appearing on the list matches the name of the applicant for the new account. The new rules are not that much of a change for banks from their earlier requirements, but it may become a major issue for various financial services firms that did not previously face such identification and verification procedures. For example, security dealers, car dealers, mutual fund operators, and comparable firms will need to establish such a system and implement these systems “on the fly.”

The expense of establishing a system can be significant. “U.S. brokerages will spend nearly \$700 million through 2005 on technology to comply with the Patriot Act [sic] — nearly three quarters of which will be directed towards software and integration.”<sup>14</sup> Reports estimate that the financial services industry will spend a total of \$10.9 billion in order to comply with the anti-money laundering requirements of the USA PATRIOT Act by the end of 2005.<sup>15</sup>

Some of these expenses will go to purchase software designed to help the industry comply with the new standards. Some will be spent on training of employees and on establishing an independent audit process that verifies internal controls and procedures. However, regardless of how the money is allocated, it is obviously expensive. Under the USA PATRIOT Act, financial services industry institutions are required to:

- Examine data of all customers from sources, both internal and external to the organization

- Determine the customer’s behavioral patterns that might affect business and national security
- Appoint a compliance officer to lead the Anti-Money Laundering program of the institution
- Create internal anti-money laundering procedures, and develop and institute training programs
- Create an independent auditing process to test internal procedures and safeguards
- Establish minimum procedures to verify identifications of customers when new customers open accounts
- Cross-check account holder names against all government lists of known or suspected terrorists or terrorist organizations
- Record the owner of any account, the originator of any transaction, the person who approved the transaction, and other individuals involved in the transaction.

From the financial institution’s perspective, the cost for compliance is huge. Some of the smaller firms and agencies will be driven out of business because they will not be able to afford the cost of meeting these requirements.<sup>16</sup> In order to comply with the new, tighter security, banking will become more expensive and less friendly. Banks will no longer be as willing to accept new customers, so changing banks or opening new accounts will be more expensive and more time-consuming.

There are substantial penalties for failure to comply with the new standards. For example, violations of International Counter Money Laundering provisions, found in § 363 of the Act, carry civil penalties of “not less than 2 times the amount of the transaction, but not more than \$1,000,000 on any financial institution or agency that violates any provision...or any special measures imposed under § 5318A.”<sup>17</sup>

There are also potential criminal penalties, including fines of no less than two times the amount of the transaction, but not more than \$1 million. Further, any financial institution that fails to implement a compliance program can be fined up to \$25,000 per day. If the failure is deemed criminal, the fines increase to an amount from \$250,000 to \$500,000 per day. Violating the due diligence

provisions, or failing to “know your customers” can lead to a penalty equal to double the value of the transaction(s) involved. And violations of the Office of Foreign Asset Control (OFAC) regulations can result in fines ranging from \$10,000 to \$1 million and imprisonment for a term of 10 to 12 years.<sup>18</sup> In addition, officers can be charged with criminal conduct, and the negative publicity for failing to follow the requirements of the USA PATRIOT Act might cause irreparable harm to the firm.

## **Title II: Enhanced Surveillance Procedures**

Title II of the USA PATRIOT Act involves the enhanced rights provided to law enforcement, especially the FBI, in an effort to thwart terrorists and terrorism. While this portion of the Act is generally viewed from the perspective of civil liberties and the possible invasion of the constitutional rights of the individual, it also impacts on business. Businesses and businesspersons may be compelled to aid in investigations of suspects, to provide relevant records requested under a search warrant, or to otherwise cooperate with the government. These activities carry potential costs to the affected businesses, both in terms of money and in terms of time spent in these activities that might otherwise be spent on the normal operations of the business.

### **Section 215: Access to Business Records**

One of the most controversial portions of the USA PATRIOT Act is § 215, “Access to Records and Other Items Under the Foreign Intelligence Surveillance Act.” This section allows certain FBI agents to apply to the Foreign Intelligence Surveillance Act (FISA) court seeking a court order requiring the production of various records in the course of any terrorism investigation.<sup>19</sup> The records that can be requested include business records, library records, movie rental records, credit records, health records, and any other pertinent data. This data can be requested from a business if the FBI is investigating a customer, a supplier, or an employee of the targeted business. The access to

various records, and the related record-keeping requirements imposed on businesses, can be quite burdensome. The law does include a few restrictions. The section specifically states that the FBI cannot conduct an investigation of a U.S. person (either a U.S. citizen or a legal permanent alien) solely on the basis of that person’s protected First Amendment activities.<sup>20</sup> However, if there is any other basis for the investigation of a U.S. person and part of the investigation “strays” into protected First Amendment activities, this restriction will not apply, nor does the restriction apply to “non-U.S. persons” under investigation.

Many people have taken a “So what?” attitude toward this provision. A common assertion is that law enforcement personnel, including the FBI, could always ask for those types of records, so it is no big deal that this is allowed under the USA PATRIOT Act. This assertion is correct — to an extent. Law enforcement personnel could obtain either a court order or a grand jury subpoena authorizing them to obtain such records. However, under normal circumstances when a court order or a grand jury subpoena is sought, the law enforcement agency seeking the records has to show probable cause in order to obtain the records, and the person targeted is aware of the inquiry and is allowed to attempt to quash such a request by appearing in court to argue against issuance of the order.

Under the provisions of § 215 of the USA PATRIOT Act no such showing of probable cause is necessary, and the person being targeted is not made aware of the inquiry. If the FBI makes a request for such a court order to the FISA court, the court must issue the order. Section 215 “removes the normal requirement to meet the legal standard of ‘probable cause.’ The judge exercises no discretion and must issue the order upon receipt of the FBI application.”<sup>21</sup> The FISA judge must issue the order, and the investigation then begins without the person targeted by the investigation informed in any way. While the Department of Justice website claims that searches under § 215 are restricted to “business records,”<sup>22</sup> the Act itself allows access to “any tangible thing,” which would include books and records, papers and

documents, or any other “tangible thing” that is found in the course of the search.<sup>23</sup> Incidentally, the proceedings of the FISA court are secret and they are not open to the public. The hearings before the FISA court are conducted *ex parte* (without notice to or participation by the targeted person), its orders are accompanied by a “gag order” preventing the persons served with a search warrant from informing the target of the investigation that he or she is being investigated, and its proceedings are not covered by or reported in the press.<sup>24</sup>

Businesses or businesspersons who are served with a warrant obtained under § 215 are required to cooperate and to provide the requested information. They are also prohibited from notifying the targeted person that his or her records have been turned over to the FBI as part of an ongoing terrorism investigation. Such requirements will surely add to the expenses normally encountered by business. They will also serve to make the business somewhat leery of continuing to do business with the targeted person, at least in part because of the possibility of being included in the investigation themselves. It is nearly impossible to estimate the costs that § 215 may impose on businesses, but it is not difficult to foresee that there will be an increased cost and an added burden on businesses compelled to deal with § 215 warrants and investigations.

### **Section 216: Pen Registers and Trap and Trace Devices**

Section 216 of the Act is the section most likely to affect a broad range of businesses beyond the financial services industry. As one commentator put it: “Thanks to a new federal law, every employer that provides voice mail, e-mail, or Internet access to its employees may have to reexamine its internal policies. The new law may even require employers to assist authorities in investigations related to terrorism.”<sup>25</sup>

Pen registers and trap and trace devices are related electronic surveillance tools. A pen register captures the phone numbers dialed from a telephone (outgoing calls), while a trap and trace device captures the phone number of a caller to a telephone (incoming calls).<sup>26</sup> Law enforcement personnel do not need

a search warrant to install either device, although a court order is required. However, all that is needed to obtain the court order is an application from the law enforcement agency stating that any information likely to be obtained from use of the devices is relevant to an ongoing criminal investigation.<sup>27</sup> Upon receiving such an application, the FISA court must issue the court order. These standards have been part of the Foreign Intelligence Surveillance Act (FISA) since its inception,<sup>28</sup> as well as part of the coverage of the Electronic Communications Privacy Act of 1986.<sup>29</sup> However, the USA PATRIOT Act has broadened the scope of the use and availability of these devices, as well as specifically including the Internet and e-mails as being covered by both devices.

The effect of this expanded definition and applicability of pen registers and trap and trace devices will obviously have an impact on individuals who are targeted for surveillance and investigation, but how will it affect business? Depending on the circumstances, the effect on any given business could be substantial.

If a business has an employee, regardless of the level of that employee, who is suspected of being engaged in any seditious or terrorist-related activities, that employee is likely to be investigated. And that investigation is quite likely to affect the business employing the suspect. The Act permits widespread wiretapping authority, allowing both “roving taps” and “pen/traps” (the use of both a pen register and a trap and trace) under a court order issued by the FISA court. Once again, the proceedings of the FISA court are conducted *ex parte*, without notice to the person being investigated or to other persons who may be affected, such as the business that employs the targeted individual. The court order is likely to allow the FBI to conduct its “pen/trap” surveillance on any telephone or computer that the person is likely to use: his or her home phone, his or her cell phone, and any phone that may be used at work; his or her personal computer and any other computer that he or she may use to access the Internet, including computers at work. The pen/trap devices collect “non-content” information about

all types of electronic communications, including Web surfing and Internet keyword searches, from any and all electronic communication devices (telephones and computers) subject to the device. Thus, any number of telephones or computers owned by the business and located within the business could well be subject to pen/trap surveillance, regardless of the user at any given time, if the person being investigated had access to the device.

The Act also provides for “emergency disclosures” of information under certain circumstances, even absent a search warrant or a court order.<sup>30</sup> Under the guidelines of § 212, “an owner or operator of a network system who reasonably believes that they have accessed information endangering life or limb [is allowed] to disclose that information to virtually anyone—whether it is a law enforcement official or the guy sitting next to you...without fear of subsequent liability under ECPA.”<sup>30</sup>

At least the employer who cooperates with law enforcement will not have to worry about any liability to his or her employees for any alleged invasions of privacy, or on any other basis. Section 225 of the Act provides that:

“No cause of action shall lie in any court against any provider of a wire or electronic communications service, landlord, custodian, or other person (including any officer, employee, agent or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act.”<sup>32</sup>

### **Section 217: Interception of Computer Trespasser Communications**

Not all aspects of the USA PATRIOT Act necessarily impose a burden on business. At least one aspect can be viewed as generally beneficial for business, the new coverage of computer crimes, including hacking. Computer crimes affect a great many businesses, and computer “attacks” by hackers can be anything from a nuisance to a major financial setback to businesses and

individuals. Partially in recognition of the susceptibility of computers to attack, and partially to try to head off terrorists who might try to disrupt a business or an industry through hacking, the USA PATRIOT Act has several sections addressing computers and computer attacks. Section 217 permits any person or business who is subjected to a “computer attack” to strike back by hiring his or her own experts. These people are deemed to be acting under color of law to monitor intruders onto the system, to intercept any communications from the intruder, and to collaborate with law enforcement officials in investigating the attacks and identifying and prosecuting the hacker.

In addition, § 814 greatly increases the damages that a business or an individual can recover from a hacker once he or she is caught and convicted, and greatly expands the definition of damages, to include lost revenues and the costs of assessing, responding to, and recovering from a computer attack. Finally, § 815 provides for the development and support of computer forensics laboratories and training so that businesses subjected to a computer attack can seek help in the investigation and prosecution of such attacks.

The Act also provides the owner or operator of a computer network a cause of action against computer trespassers for damages in excess of \$5000. Given the potential for serious financial losses when a computer system is “hacked,” this provision seems to be a valid and beneficial protection for owners and operators of computer networks.

### **Conclusions and Recommendations**

The USA PATRIOT Act was passed with the best of intentions, but its application seemingly falls far short of its objectives. Much of the expense of the antiterrorism efforts covered under the Act is being borne by private industry. Airport security with the Transportation Security Administration costs nearly \$6 billion per year, paid for by the airports and airlines, and indirectly by the flying public.<sup>33</sup> By December 2002, 45 percent of the 797 businesses surveyed by *CSO* (Chief Security Officer) magazine had provided data on

their customers, employees, or business partners to various law enforcement officials following USA PATRIOT Act-based requests.<sup>34</sup> Internet service providers and phone companies are being particularly hard-hit. BellSouth reported that it received 32,370 subpoenas and 636 court orders for information on customers in 2002.<sup>35</sup> The cost to handle this workload is significant.

The USA PATRIOT Act may well reduce the risk of terrorism and terrorist attacks, but at what price? Compliance costs include nearly \$11 billion for the financial services industry and untold billions for airport and transportation security. There will also be costs related to the issuing of secret subpoenas and court orders, businesses will incur expenses in meeting requests for information about customers and employees, as well as in acting as informers for the FBI, whether the businesses want to inform or not. The St. Petersburg Times called the USA PATRIOT Act the largest unfunded federal mandate since the creation of the Social Security system.<sup>36</sup>

Businesses need to develop “best practices” in a number of areas to ensure that they comply with the Act, and to avoid the potential liability for failure to comply. Financial services industry firms must implement anti-money laundering practices, and they must “know their customers.” They also must report suspicious activities by their customers. Businesses need to develop policies for the retention of records that are in accord with the requirements of the Act, and must be prepared to turn over such records upon demand by law enforcement personnel, provided that the law enforcement personnel have an appropriate warrant. Businesses should also develop policies and procedures for dealing with pen/trap requests from the government, subject to an appropriate court order. A starting point should be the Sedona Conference, which has issued a report, “the Sedona Principles,” dealing with standards and best practices for the retention and production of electronic documents. This report has been favorably cited by the courts and seems to provide an excellent framework for dealing with electronic documents.<sup>37</sup> Businesses should also develop policies

and procedures that will help to identify “emergency disclosure” information and that will establish guidelines for dealing with such information if or when the situation arises.

The USA PATRIOT Act is an unwieldy statute. It runs 342 pages in length, and much of its content involves amendments to other federal statutes. The purpose of the law, combating terrorists and terrorism, is laudable. However, its implementation will be burdensome on society, and in particular on businesses. How much will it cost business? No one knows—yet. But the cost will be substantial. How much does it affect business? No one knows—yet. But the affect will be substantial. Is it worth the cost or the affect that it will have on business? Let us hope so.

### Endnotes

<sup>1</sup> Pub. L. No. 107-56, 115 Stat. 272 (2110).

<sup>2</sup> Dahlia Lithwick and Julia Turner, “A Guide to the Patriot Act, Part I,” *MSN Slate Magazine*, Jurisprudence (September 8, 2003).

<sup>3</sup> William Yela and Carol M. Beumier, “Money-laundering risks of electronic distribution channels,” *Bank Accounting & Finance*, Vol. 15, Issue 3 (Spring 2002), p. 45.

<sup>4</sup> Karen L. Grandstrand, “USA Patriot Act —The Regulations Just Keep Coming,” *Fredrickson & Byron, P.A.*, [http://www.fredlaw.com/articles/banking/bank\\_0206\\_klg.html](http://www.fredlaw.com/articles/banking/bank_0206_klg.html) (June 2002).

<sup>5</sup> Mary P. Gallagher, “New Patriot Act Rules Take Hold for Financial Institutions,” *Delaware Law Weekly*, Vol. 6, NO. 41 (October 15, 2003) p. D5.

<sup>6</sup> John J. Ensminger, “September 11 brings new anti-money laundering responsibilities to financial institutions,” *Review of Business*, Vol. 23, Issue 3 (St. Johns University, New York, N.Y., Fall 2002), p. 29.

<sup>7</sup> Mitali Kalita, “How Patriotic is the Patriot Act?” *U.S. Banker*, Vol. 114, NO. 3 (March 2004), p. 62.

<sup>8</sup> Yela and Beumier, “Money-laundering risks of electronic distribution channels,” p. 45.

<sup>9</sup> Gallagher, “New Patriot Act Rules Take Hold for Financial Institutions,” p. D5.

<sup>10</sup> *Ibid.*

<sup>11</sup> John Dizard, “Patriot act makes moles out of managers,” *The Financial Times*, Global Investing, USA Edition 1 (London, England, February 9, 2004), p. 25.

<sup>12</sup> 31 U.S.C. 5318.

<sup>13</sup> Gallagher, “New Patriot Act Rules Take Hold for Financial Institutions,” p. D5.

<sup>14</sup> Ensminger, “September 11 brings new anti-money laundering responsibilities to financial institutions,” p. 29.

<sup>15</sup> *Ibid.*

<sup>16</sup> *Ibid.*

<sup>17</sup> USA PATRIOT Act, § 363 (a)(7) for civil penalties and § 363 (d) for criminal penalties.

<sup>18</sup> Richard J. Ruszat II, “The USA Patriot Act, a Primer to Compliance Requirements,” *NACM*, <http://www.nacmint.com/articles/art324> (Reprinted by permission from *Trade Vendor Quarterly*, Spring 2003).

<sup>19</sup> “Rhetoric vs Reality: Section 215 of the USA PATRIOT ACT,” FCNL, Issues We Work On, USA PATRIOT Act of 2001, [http://www.fcnl.org/issues/item.php?item\\_id=344&issue\\_id=68](http://www.fcnl.org/issues/item.php?item_id=344&issue_id=68) (September 8, 2003).

<sup>20</sup> *Ibid.*

<sup>21</sup> “USA PATRIOT ACT Business Fact Sheet,” American Civil Liberties Union of Utah, <http://www.acluutah.org/Businessfacts.pdf>.

<sup>22</sup> <http://www.lifeandliberty.gov/>

<sup>23</sup> Lithwick and Turner, “A Guide to the Patriot Act, Part I.”

<sup>24</sup> “Rhetoric vs Reality: Section 215 of the USA PATRIOT ACT,” [http://www.fcml.org/issues/item.php?item\\_id=344&issue\\_id=68](http://www.fcml.org/issues/item.php?item_id=344&issue_id=68)

<sup>25</sup> Patrick J. Mulrone, “The Patriot Act: How to protect yourself and still comply,” *Connecticut Employment Law Letter*, Vol. 11, Issue 2 (December 2003).

<sup>26</sup> Anthony E. Orr, “Marking Carnivore’s Territory: Rethinking Pen Registers on the Internet,” *Mich. Telecomm. Tech. Law Review*, Vol. 8 (2002), p. 219.

<sup>27</sup> *Ibid.*

<sup>28</sup> 50 U.S.C. § 1842 (1978, amended 1999, amended 2110).

<sup>29</sup> 18 U.S.C. §§ 3121-3127 (1994).

<sup>30</sup> § 2702 of the Electronic Communications Privacy Act of 1986, as amended by USA PATRIOT Act, § 212.

<sup>31</sup> Tracy Mitrano, “Taking the Mystique Out of the USA-PATRIOT Act: Information, Process and Protocol,” Information Technologies Policy Office, Cornell University, <http://www.cit.cornell.edu/oit/PatriotAct/article.html>

<sup>32</sup> § 105 (h) of the Foreign Intelligence Surveillance Act of 1978, as amended by USA PATRIOT Act, § 225.

<sup>33</sup> Robyn E. Blumner, “With Patriot act, companies forced to play informant on customers,” *St. Petersburg Times Online*, (May 18, 2003). See also, the Report Before the Committee on Commerce, Science, and Transportation Subcommittee on Aviation of the United States Senate by Kenneth M. Mead, Inspector General of the U.S. Department of Transportation. “Aviation Security Costs, Transportation Security Administration,” (February 5, 2003).

<sup>34</sup> *Ibid.* See also *CSO Magazine* (December 2002).

<sup>35</sup> Tom Carver, “Does the Patriot Act infringe on civil liberties?” *News-Leader.com* (August 24, 2003).

<sup>36</sup> Blumner, “With Patriot act, companies forced to play informant on customers.”

<sup>37</sup> Albert Barsocchini, “Electronic Data Discovery Growth is Staggering: But keep things in perspective; it’s no different than paper discovery — there’s just more of it,” *New Jersey Law Journal* (September 8, 2003), and see [www.thesedonaconference.org](http://www.thesedonaconference.org)