Center for American Progress

Center For Democracy & Technology

Online Consumers at Risk and the Role of State Attorneys General

Reece Rushing, Ari Schwartz, and Alissa Cooper

August 2008

ONLINE CONSUMERS AT RISK AND THE ROLE OF STATE ATTORNEYS GENERAL

Reece Rushing, Ari Schwartz, and Alissa Cooper

The Center for American Progress and
The Center for Democracy and Technology

August 2008

Contents

Executive Summary

Internet commerce has provided consumers with more convenience, more choices, and lower prices. These benefits, however, are being threatened by high levels of fraud and abuse unique to the online environment. If problems such as malware, phishing, and spam are left unchecked, many consumers may lose trust and abandon e-commerce. Action is urgently needed to ensure this does not happen.

State attorneys general are an important part of the solution. The federal government, in particular the Federal Trade Commission, is beginning to step up, but resources are still limited. State attorneys general can augment the federal capability to protect consumers. Over the past three years, for example, state attorneys general have brought 11 cases against spyware distributors, the same number as the FTC.

State consumer protection laws are sometimes stronger than federal laws. Leading attorneys general, in particular those in New York and Washington, have used such authority against spyware purveyors to levy penalties that are tougher than those the FTC can impose. In part because of this increased enforcement, consumer losses from spyware have declined 35 percent.

This is certainly positive, but the problem of Internet crime is still far from solved. To better assess online fraud and abuse, the Center for American Progress and the Center for Democracy and Technology asked states to provide data on consumer complaints they received in 2007 and 2006, organized by category. Of the 36 states that provided at least some data, most supplied a top 10 list ranking complaint categories (Internet-related and other), with a few going beyond the top 10. In 2007, 24 out of 30 states that provided rankings reported an Internet-related category within their top 10. Eight states ranked Internet-related complaints among their top three most common consumer complaints, including four states that ranked Internet-related complaints No. 1.

For 2007 and 2006, 20 states provided the number of consumer complaints associated with each category—the others merely provided rankings without giving the number of complaints. In both years, these states reported roughly 20,000 Internet-related complaints, with slightly more in 2006. This number generally does not include Internet-related complaints that are not associated with a top 10 category.

The Federal Trade Commission also provides data for all 50 states on consumer complaints related to Internet fraud. These data include not only complaints submitted to the FTC, but also complaints directed to a variety of other actors, including the

U.S. Department of Justice, Better Business Bureaus, the National Consumers League, and 13 state attorneys general. The number of contributors to the FTC data is one reason the FTC reports a greater volume of complaints than attorneys general.

In 2007, the FTC reported 221,226 Internet-related fraud complaints, up almost 16,000 from 2006 and more than 24,000 from 2005.[1] These numbers may even understate the problem. Consumers are often unaware, and thus may not report, when they are victimized by online threats such as malware, which cyber-security experts say is rising dramatically.

Weaknesses in state data, unfortunately, impede more detailed analysis of various types of Internet-related consumer complaints. State reporting typically groups all Internet-related crime into one or two broad categories. Complaint information is also inconsistently categorized across states, or not categorized at all, preventing reliable comparisons between states. Nonetheless, the large volume of Internet-related complaints demonstrates the seriousness of the problem and the need for action.

To assess how state attorneys general are responding, we reviewed their annual or biennial reports (roughly half of attorneys general create such reports), their websites, news articles, and the bimonthly Cybercrime Newsletter released by the National Association of Attorneys General.

Attorneys general have brought some notable cases on behalf of consumers, but generally online fraud does not seem to be a top priority. Rather, most investigations and prosecutions involving the Internet appear to be focused on sexual enticement of minors and child pornography. Such cases accounted for more than 60 percent of the cases highlighted in 2007 and 2006 by the Cybercrime Newsletter, which lists Internet-related cases brought by state attorneys general.

Among other cases highlighted, 8.9 percent involved data security, confidential records, or identity theft, and 15.5 percent involved online sales and services, such as failure to deliver on a purchase or failure to provide a product or service that meets advertised quality. This type of crime has clear parallels to fraud conducted in the physical world—the Internet is merely the medium for the transaction.

This is not the case, however, for spyware, adware, spam, and phishing, which represent completely new categories of fraud and abuse. Over the course of 2007 and 2006, the Cybercrime Newsletter highlighted just 14 cases (8.3 percent of the total) brought by state attorneys general in these areas, 10 of which were brought by Washington or New York. We describe a number of these cases on page 22.

These cases and others listed in the Appendix have achieved significant benefits. But given the still-high levels of online fraud and abuse, they should be viewed as just a start. All attorneys general—not just a few standouts—must give priority to this problem to provide consumers the protection they need and deserve. In particular, we recommend that attorneys general:

- Review relevant laws to provide clarity for enforcement and to make recommendations for needed legislative action
- Train investigators and prosecutors on how to identify online fraud and abuse

- Develop computer forensic capabilities to trace and catch Internet fraudsters
- Devote greater resources to Internet enforcement efforts
- Partner with commercial and public-interest coalitions that are fighting online fraud and abuse
- Establish coordinated efforts with other attorneys general
- Aggressively investigate consumer complaints
- Develop better data systems to track complaints regarding Internet fraud and abuse, including the response of the attorney general's office

Currently, there is insufficient incentive against committing online fraud and abuse. Internet crime requires almost no expense to execute, carries potentially high financial rewards, and involves relatively little risk of being caught and punished. It is thus unsurprising that online fraud and abuse are at such high levels. What's needed now is a stronger deterrent. Through committed action and vigorous enforcement, state attorneys general can help provide one.

The Rise of Online Fraud and Abuse

The explosion of Internet commerce has delivered enormous benefits for consumers. Prices have dropped due to the ease of Internet comparison shopping. The marketplace has expanded as barriers to entry have diminished and buyers and sellers easily link up through websites such as eBay. And transactions are now quickly and conveniently conducted from a home computer, without the hassle of waiting in a line, holding on the telephone, or mailing a check.

These benefits, however, are being threatened by the rise in Internet fraud and abuse. According to a 2006 survey conducted by the Cyber Security Industry Alliance, half of all Internet users now avoid making online purchases because they are afraid personal financial information will be stolen; barely a third of Americans believe online banking is as secure as banking in person; and 95 percent view identity theft as a serious problem.[2] As a result of these concerns, Internet commerce may lose out on several billion dollars a month.[3]

Most Internet transactions, to be sure, are conducted without harm to the consumer. Unfortunately, not all sellers offering products on the Internet are scrupulous. Consumers, faced with a vast array of unfamiliar choices, may have difficulty judging where to take their business and whom to avoid.

Indeed, as the numbers presented in this report show, consumers frequently complain of being victimized in online auctions and Internet sales. These complaints are most typically made against sellers for not delivering a product on time, not delivering at all, or delivering a product that does not meet the advertised quality.[4] Consumers may also be lured to use phony escrow services—escrow services are commonly used to hold money for large online purchases—or to buy from fraudulent sellers who "siphon" bidders off of legitimate auction sites or employ "shill bidding" to drive up a product's price.

In addition to such transactional fraud—which has clear parallels to fraud conducted in the physical world—consumers face a host of new threats that are completely unique to the Internet. Moreover, these threats affect not just a percentage of online consumers, as with transactional fraud, but to varying degrees, virtually everyone with a computer.

In particular, personal information is often surreptitiously gathered on Internet users through invasive means such as spyware or adware. Companies large and small do this to aid unwanted marketing or to monitor consumer use of products and services. Fraudsters, many operating from foreign countries with weak or uncooperative govern-

ments, also employ spyware to maliciously gain control of personal computers and steal private data[5]—such as credit card information or Social Security numbers—that might be transmitted during online transactions.

The prevalence of spyware and adware cannot be reliably measured by the number of consumer complaints, as many consumers are unaware that they have been victimized. Indeed, F-Secure Corporation, an Internet security company, detected an explosion of such malware in 2007 even though Internet-related consumer complaints have been relatively steady over the last several years.[6]

Consumers are further subjected to a constant barrage of annoying and frequently offensive spam e-mail. Some of this spam is sent by fraudsters posing as legitimate businesses, such as a bank where the consumer may have an account. These "phishing" e-mails typically employ fake but often very real-looking websites—and sometimes even fake images of bank account information—to con consumers into providing personal information, which can be used for identity theft.

U.S. consumers pay a staggering price for this Internet fraud and abuse. In 2007, an estimated $7.1 billion was lost due to viruses, spyware, and phishing alone[7]—up almost $2 billion from the 2006 estimate—and the cost of dealing with spam was an estimated $100 billion worldwide (including $35 billion in the United States), double the amount in 2005.[8] These trends undoubtedly are linked to skyrocketing identity theft, with as many as 9 million Americans victimized every year.[9]

The rise in Internet crime is not likely to reverse course given current incentives. Perpetrators face little to no start-up or overhead costs,[10] can reap substantial financial rewards—the average phishing outfit, for example, earns an estimated $250,000 per month[11]—and can operate anonymously from anywhere in the United States or the world, with relatively little prospect of detection or punishment. Efforts by law enforcement remain inadequate to alter these incentives.

The Role of State Attorneys General

Federal agencies, particularly the Federal Trade Commission,[12] are beginning to take action to protect consumers online. But because of the FTC's limited resources and weaknesses in federal law,[13] state attorneys general are essential to buttress these efforts. Over the past three years, for example, state attorneys general brought 11 cases against spyware purveyors, the same number as the FTC.[14] During this time, consumers saw spyware losses drop from $2.6 billion to $1.7 billion.[15] There are multiple reasons for this drop, but federal and state law enforcement is undoubtedly an important contributor.[16]

Despite this success, state attorneys general can still do much more to police Internet fraud and abuse. The National Association of Attorneys General has undertaken educational efforts for state attorneys general on a wide range of cybercrime issues, including online fraud.[17] But Internet-related cases brought by attorneys general appear to be heavily focused on stopping child predators and child pornography. Such cases accounted for more than 60 percent of the cases highlighted in 2007 and 2006 by the Cybercrime Newsletter, which lists Internet-related cases brought by state attorneys general. While cases involving child pornography and other forms of predation against children deserve high priority, new tools and greater commitment are needed to tackle other online threats such as spyware.

The attorneys general in Washington and New York are showing how this can be done. Respectively, they have opened a consumer protection "High Tech Unit" and an "Internet Bureau," which have allowed attorneys and computer forensic specialists to gain the added skills necessary to fight online fraud and abuse. As discussed on page 22, Washington Attorney General Rob McKenna and former New York Attorney General Eliot Spitzer both launched successful suits against spyware purveyors. Spitzer's successor, Andrew Cuomo, has continued to aggressively pursue cases of Internet fraud and abuse.

In response to such cases, as well as a number of new state laws against Internet fraud and abuse, some business interests have lobbied Congress to preempt states with a single federal regime for online consumer protection, enforced by federal regulators only. Broadly preempting states in this way would be a severe setback.

State laws are sometimes needed to fill the gaps in federal law.[18] For example, in early 2004, it was revealed that sham businesses, some intent on identity theft, had purchased the personal records of 145,000 consumers from the information-services company ChoicePoint. The public learned about this security breach because of a California law

that requires disclosure of data thefts. No similar federal law existed at the time, nor has one been passed since. Most states, on the other hand, responded to the California example by enacting their own data breach security laws.

Similarly, state attorneys general can fill federal enforcement gaps by bringing additional resources to bear and supporting the efforts of federal agencies such as the FTC, which often face budgetary and staffing constraints that impede robust Internet enforcement. As NAAG explains, "In many areas traditionally considered the exclusive responsibility of the federal government, the Attorneys General now share enforcement authority. Indeed, a major trend of the last several years has been the increasingly cooperative working relationships the Attorneys General have forged with their federal counterparts, particularly in the areas of trade regulation, environmental enforcement, and criminal justice."[19] Enforcement of online consumer protections should be no different.

Major Findings

All states allow residents to register consumer complaints. Such complaints are handled by the attorney general's office in most cases or by separate consumer protection departments in a handful of states.

The Center for American Progress and the Center for Democracy and Technology requested state data on these complaints to assess the prominence of Internet-related concerns. The data gathered make clear that states receive a high volume of Internet-related complaints. The overwhelming majority of states that responded to our request ranked Internet-related complaints among the top 10 of all consumer complaints.

Nonetheless, a fuller assessment proved more difficult than expected due to shortcomings in state data. Fourteen states did not provide any data at all, while just a few states provided detailed complaint data. Instead, most states supplied only a list ranking their top 10 consumer complaints (Internet-related and other), in some cases without providing the number of complaints received for each category. Moreover, the Internet-related categories used by states are broad and unspecific—frequently simply "Internet."

In addition, we sought to assess the response of attorneys general to complaints over fraud and abuse unique to the Internet such as spyware and adware. We did this by reviewing news articles, attorney-general websites and annual or biennial reports, and the bimonthly Cybercrime Newsletter jointly put out by the National Association of Attorneys General and the National Center for Justice and the Rule of Law at the University of Mississippi School of Law.

The attorneys general cited in the case examples on page 22 have taken aggressive action on spyware, adware, spam, and phishing. Attorneys general have also brought a number of other important cases involving Internet sales and services, as well as data security, confidential records, and identity theft. A list of such cases can be found in the Appendix. Nonetheless, it seems clear that most attorneys general are not giving high priority to Internet fraud and abuse.

Our major findings include the following:

State attorneys general receive a high volume of Internet-related consumer complaints. Thirty states provided a ranked list of consumer complaints for 2007. Of these, 24 reported an Internet-related category within their top 10, and two others reported an Internet-related category within their top 15. Eight states ranked Internet-

INTERNET CONSUMER COMPLAINT DATA PROVIDED BY STATES

STATE*	DEPARTMENT HANDLING COMPLAINTS	INTERNET-RELATED CATEGORY	RANK IN 2007**	NUMBER OF 2007 COMPLAINTS	RANK IN 2006 (OR PREVIOUS)**	NUMBER OF 2006 COMPLAINTS
Alabama	Attorney General	Internet	2	417	1	390
Alaska	Attorney General	Internet (auctions, goods and services, service providers, spamming)	No Top 10 List Provided for 2007		5	Not Provided
Arizona	Attorney General	Internet Auctions	4 (July 1, 2006–June 30, 2007)	550 (approximate)	8	800 (approximate)
		Telemarketing, Spam			2	1,100 (approximate)
Arkansas	Attorney General	InternetAuction/ Internet Service	7	206	9	190
Connecticut	Dept. of Consumer Protection	Internet	8	201		
		Online Scams		69		
		Service Providers		22		
		Auctions		22		
		Spam		17		
		Internet Sales			7	Not Provided
Delaware	Attorney General	Internet	15	104	No Internet Category in 2006 Top 10	
Florida	Attorney General	Internet, including ISPs & Internet commerce	1 (January–June 2007)	Not Provided		
Georgia	Office of Consumer Affairs	Miscellaneous Matters (Internet auctions, sweepstakes, and lotteries)	4	Not Provided		
		Internet Goods and Services			4	Not Provided
Hawaii	Office of Consumer Protection (within Dept. of Commerce & Consumer Affairs)	Computer /Internet Services and Fraud	1	Not Provided		
		Internet Fraud Complaint Center	Category Not Used for 2007 Ranking	369	1	319
		Internet Transactions	Category Not Used for 2007 Ranking	394	2	315
		Computer Information Services		*10*		
		Spamming		*1*		*2*
Idaho	Attorney General	Internet	4	104	3	142
Illinois	Attorney General	Not Applicable	No Internet Category in 2007 Top 10		No Internet Category in 2006 Top 10	
Indiana	Attorney General	Internet Goods & Services	7	Not Provided		
		Internet Auctions /Internet Sales			2	637
Iowa	Attorney General	Services (including some Internet)	No Top 10 List Provided for 2007		7	Not Provided
Kansas	Attorney General	Internet Sales	7 (January–June 2007)	214		
Kentucky	Attorney General	Internet Sales and Auctions, Internet-based Companies, and Internet Scams	7 (Jan. 1, 2007–March 4, 2008)	109		
		Internet Sales and Auctions			3	141

INTERNET CONSUMER COMPLAINT DATA PROVIDED BY STATES (CONTNUED)

STATE*	DEPARTMENT HANDLING COMPLAINTS	INTERNET-RELATED CATEGORY	RANK IN 2007**	NUMBER OF 2007 COMPLAINTS	RANK IN 2006 (OR PREVIOUS)**	NUMBER OF 2006 COMPLAINTS
Louisiana	Attorney General	Internet Goods and Services	No Top 10 List Provided for 2007		8	90
Massachusetts	Attorney General	Not Applicable	No Internet Category in 2007 Top 10		No Internet Category in 2006 Top 10	
Michigan	Attorney General	Internet	3	Not Provided	2	Not Provided
Mississippi	Attorney General	Nigerian Scams	9	Not Provided		
		Internet Sales of Goods and Services			7 (2005)**	Not Provided
Missouri	Attorney General	Computer Software, Online Services and Internet Auctions	9	1,018	4	1,791
Montana	Attorney General	Internet Purchases	3	Not Provided		
		Internet Fraud			8	Not Provided
Nebraska	Attorney General	Internet Transaction	5	261	1	452
New Hampshire	Attorney General	Internet Goods and Services	No Top 10 List Provided for 2007		3	Not Provided
New Jersey	Attorney General	Internet	No Top 10 List Provided for 2007		7 (2005)**	1,470 (2005)**
New York	Attorney General	Internet	1	7,469	1	7,723
North Carolina	Attorney General	Internet Service and Sales	7	710	10	779
North Dakota	Attorney General	Internet Scams (Classified Ad, Lottery, Phishing, and Nigerian Letter)	10	36	8 (2005)**	54 (2005)**
Ohio	Attorney General	Computers and Internet Sales and Services	3	962	5	1,270
		Internet/On-Line Service Provider		*277*		*349*
		Computers & Internet		*118*		*195*
		On-Line Shopping		*202*		*104*
		Computer Software		*101*		*100*
		Phishing		*25*		*25*
		On-Line Auctions		*44*		*23*
		Spam		*26*		*12*
Oklahoma	Attorney General	Internet (auctions, service providers)	1	1,002	1	904
Oregon	Attorney General	Internet Service Providers	Subcategory of No. 1 "Telecommunications"	194		
		Internet Auctions	9	237	9	288
		Internet Retailers			5	469
South Carolina	Dept. of Consumer Affairs	*Internet Service Provider*	No Internet Category in 2007 Top 10	*No Category Data Provided for 2007*	*No Ranked List Obtained for 2006*	83
		Internet Fraud Complaint Center				3
Tennessee	Division of Consumer Affairs (within Dept. of Commerce & Insurance)	Internet Sales	No Internet Category in 2007 Top 9***		2	764

INTERNET CONSUMER COMPLAINT DATA PROVIDED BY STATES (CONTINUED)

STATE*	DEPARTMENT HANDLING COMPLAINTS	INTERNET-RELATED CATEGORY	RANK IN 2007**	NUMBER OF 2007 COMPLAINTS	RANK IN 2006 (OR PREVIOUS)**	NUMBER OF 2006 COMPLAINTS
Texas	Attorney General	Internet Sales	6	444	5	609
		Internet Access Provider		*159*		*235*
		Internet Auction		*31*		*100*
		Unsolicited Email		*49*		*73*
Washington	Attorney General	Electronic Shopping	4	1,210	5	819
		Internet Service Providers	16	398	12	443
		Online Auctions	19	316	19	319
		Phishing		*70*		*51*
		Unsolicited Email		*43*		*69*
		Spyware		*8*		*28*
Wisconsin****	Dept. of Ag., Trade, & Consumer Protection	*Spam*	*14*	*416*	*12*	*534*
		Internet Service Provider	*22*	*288*	*13*	*335*
		Fictitious Email	*24*	*222*	*22*	*221*
		Internet Auction Sales	*19*	*196*	*17*	*204*
		Phishing/Spoofing	*31*	*173*	*28*	*163*
		Internet Auction Service	*44*	*108*	*39*	*109*
Wyoming	Attorney General	Internet Auctions	No Top 10 List Provided for 2007		8	Not Provided

* States that do not appear on this list did not provide consumer complaint data.

** Most states listed here provided a list ranking their Top 10 consumer complaints, Internet-related and other. Several states provided rankings beyond the Top 10. In three cases, we provide 2005 data instead of 2006 data. North Dakota did not have an Internet-related category in its Top 10 in 2006. Mississippi and New Jersey did not provide 2006 data.

*** A "glitch" in Tennessee's database turned out only 9 top categories, instead of the typical 10.

**** Wisconsin provided detailed consumer complaint data. Complaints are organized and ranked by "product" categories, "business practice" categories, and "problem" categories. Of the categories presented here, "Internet Service Provider" and "Internet Auction Service" are product categories. "Internet Auction Sales" is a business practice category. And Spam, Fictitious Email, and Phishing/Spoofing are problem categories. The rankings presented here are within these separate groupings. Thus, for example, "Internet Auction Sales" ranks 19th among business practice categories for 2007, while Fictitious Email ranks 24th among problem categories.

Italics indicate categories that did not appear on a ranked list, but rather were obtained from more detailed consumer complaint data provided by the state. These categories may comprise the more general categories, not italicized, that are used for rankings. Most states did not provided detailed consumer complaint data. In the case of Hawaii, "Internet Fraud Complaint Center" and "Internet Transactions" appeared on the state's Top 10 list in 2006 but were subcategories in 2007, and thus are italicized.

related complaints among their top three most common consumer complaints, including four states that ranked Internet-related complaints No. 1.

The story was similar for 2006. Thirty-one states provided a ranked list for 2006.[20] Of these, 25 reported an Internet-related category within their top 10, and another one reported Internet-related categories within its top 15. Twelve states ranked Internet-related complaints among their top three most common consumer complaints, including five states that ranked Internet-related complaints No. 1.

For both 2007 and 2006, 20 states provided the number of consumer complaints associated with each category—the others merely provided rankings without giving the number of complaints. In both years, these states reported roughly 20,000 Internet-related complaints, with slightly more in 2006. This number generally does not include Internet-related complaints that are not associated with a top 10 category.

There are a number of possible explanations for states that do not list any Internet-related category in their top 10 complaint types: Internet complaints

may not be common enough; the state may not have a separate category for Internet complaints; or Internet complaints may be broken into a number of smaller categories.

The largest number of complaints appear to involve Internet sales and auctions. States typically use one or two broad categories for tabulating Internet-related complaints for their top 10 lists. For 2007, nine states use the category "Internet" to lump together all such complaints. More detailed analysis is obviously not possible without more specific categories. Nonetheless, most Internet-related categories that appear in state top 10 lists refer specifically to Internet sales and/or auctions, Internet transactions, Internet retailers, or Internet goods and services.

Very few states provided data on spam, spyware, and phishing. Only five states provided complaint data on spam—Wisconsin, Texas, Washington, Ohio, and Hawaii. (Arizona's top 10 list includes the category "Telemarketing, Spam," but there is no way to tell how many of the approximately 1,100 reported complaints involved spam.) Among these five states, Wisconsin had by far the most complaints at 416 in 2007 and 534 in 2006. Texas, with 18 million more residents than Wisconsin, reported 49 "Unsolicited Email" complaints in 2007 and 73 in 2006. Washington reported 43 "Unsolicited Email" complaints in 2007 and 69 in 2006. Connecticut reported 17 spam complaints in 2007, and Ohio and Hawaii reported just 38 and three spam complaints, respectively, in 2007 and 2006 combined. The reason for the wide difference in numbers is unclear, but it suggests potential differences in data collection and reporting.

Just three states provided complaint data on phishing. Wisconsin again had the most at 173 in 2007 and 163 in 2006. Washington reported 70 phishing complaints in 2007 and 51 in 2006, while Ohio reported 25 complaints in both 2007 and 2006. Only Washington provided spyware data, reporting eight complaints in 2007 and 28 complaints in 2006.

STATES THAT DID NOT PROVIDE CONSUMER COMPLAINT DATA

STATE	DEPARTMENT HANDLING COMPLAINTS
California	Dept. of Consumer Affairs
Colorado	Dept. of Public Health & Env. & Attorney General
Maine	Attorney General
Maryland	Attorney General
Minnesota	Attorney General
Nevada	Attorney General
New Mexico	Attorney General
Pennsylvania	Attorney General
Rhode Island	Attorney General
South Dakota	Attorney General
Utah	Division of Consumer Protection (within Dept. of Commerce) & Attorney General
Vermont	Attorney General
Virginia	Office of Consumer Affairs & Attorney General
West Virginia	Attorney General

More robust complaint data would be helpful, but alone would likely not capture the severity of these problems. Spam obviously is a continuing nuisance familiar to virtually everyone with an e-mail account. There may be a degree of resignation when it comes to spam that explains the relatively few complaints to attorneys general. In the case of spyware and phishing, consumers may be unaware that they have been victimized. Spyware installs itself on computers without the knowledge of the user, while phishing is intended to deceive consumers into thinking they are interacting with a legitimate business.

Most attorneys general are giving relatively low priority to online fraud and abuse. Attorneys general have brought some important cases on behalf of consumers against online fraud and abuse. Such cases are noted in the examples starting on page 22 and in the Appendix. Generally, however, online fraud does not seem to be a high priority.

The National Association of Attorneys General's bimonthly Cybercrime Newsletter lists Internet-related cases brought by state attorneys general. The list of cases that appears in each newsletter is not comprehensive. Rather, according to its editor, the newsletter seeks to highlight the most interesting cases. Nonetheless, it is revealing that relatively few of the cases highlighted involve Internet fraud.

Of the 168 total cases highlighted over 2007 and 2006, 26 of these (or 15.5 percent of the total) involved online sales and services; 15 (8.9 percent) involved data security, confidential records, or identity theft; and 14 (8.3 percent) involved spyware, adware, spam, and phishing. These numbers are presented in the table on page 9.

In addition, we reviewed annual or biennial reports from attorneys general. Such reports, which are produced by roughly half of the attorneys general, typically highlight major cases and initiatives that deal with priority issues, which can vary a great deal from state to state. In their most recent reports, less than a handful of attorneys general highlighted any cases or initiatives involving Internet fraud and abuse.

In dealing with cyber crime, attorneys general, as a whole, are giving greatest priority to Internet child predators and child pornography. The cases highlighted in the Cybercrime Newsletter suggest a far greater focus on child predators than on fraud. Of the 168 total cases highlighted over 2007 and 2006, 104 of these (or 61.9 percent of the total) involved sexual enticement of minors or child pornography.

In addition, the newsletter highlights other activities of the attorneys general, such as speeches given, educational materials produced, and investigative initiatives. Overwhelmingly, such activities also have been focused on child predators. Many states have established special investigative units or task forces on child predators. Few states have devoted similar investigative resources toward cracking down on Internet fraud.

Consumer complaint information was difficult to obtain. Less than a quarter of state websites provided a ranked list of consumer complaints, with the number of complaints for each category. Most states were contacted directly for this information. In most cases, we had to contact states three-to-four times through phone calls, e-mails, letters, and faxes.

AG CASES HIGHLIGHTED BY THE CYBERCRIME NEWSLETTER

CATEGORY	NO. IN 2007	NO. IN 2006	TOTAL FOR 2007 & 2006	% OF TOTAL FOR 2007 & 2006
Spyware, Adware, Spam, & Phishing	4	10	14	8.30%
Internet Sales, Services, & Auctions	12	14	26	15.50%
Data Security, Confidential Records, & Identity Theft	7	8	15	8.90%
Sexual Enticement of Minors & Child Pornography	50	54	104	61.90%
Other	4	5	9	5.40%
TOTAL	***77***	***91***	***168***	***100%***

The Cybercrime Newsletter is a bimonthly publication of the National Association of Attorneys General. Each issue lists Internet-related actions taken by attorneys general. Actions listed are not comprehensive—there may be actions that are not highlighted—but they do help understand what attorneys general are focused on. See the Appendix for details on these cases and an explanation of the data.

Calls to the offices were typically transferred to many different departments and staff members. One memorable call was transferred to six different people before finally being sent to voicemail. Frequently, the release of any information had to be approved by a supervisor or required internal consultation.

Many attorneys general were unable to produce basic data on consumer complaints. Ultimately, 14 of the 50 states did not respond to our repeated requests for consumer complaint data broken down by category. In some cases, the state attorney general's office conceded that its data system was poor. In one phone conversation, an office representative said "our reporting system stinks" and "I could give you some numbers, but they wouldn't be accurate." Another office said that categorizing the complaints by type would take far too much time. Some offices claimed that only information on complaints against a specific company was public and that aggregate data was confidential.

Consumer complaint data are inconsistently compiled. Each state has its own way of categorizing consumer complaints, making comparisons among states difficult to draw. Internet-related complaints appear in the top 10 lists under the following categories: Internet Transaction, Internet Fraud, Internet, Internet Retailers, Internet Auctions, Internet Goods and Services, and more.

Moreover, it's possible that states collect and group complaints differently even when using the same category name. For the category of Internet auctions, for example, Texas reported 100 complaints in 2006, while Oregon, with more than 20 million fewer residents, reported 288 complaints, and Arizona, with more than 17 million fewer residents than Texas, reported approximately 800 complaints. Whatever the explanation for this variation, it is clear that differences in data reporting prevent meaningful comparisons and permit only rough conclusions.

Almost all state attorneys general do a poor job of communicating actions taken in response to consumer complaints. Texas provided data on actions taken in response to consumer complaints, including the num-

ber of cases that were opened, referred, recorded, settled, and went to litigation. Most other states, unfortunately, do not systematically gather and publicly report data on actions taken.

If actions are reported at all, it is through press releases and annual or biennial reports, many of which are not accessible through the Internet (Virginia even charges $25 for a copy of the attorney general's annual report). Press releases provide notification of specific actions and cases. Annual reports or biennial reports—which, again, are done by only about half of state attorneys general—may highlight key actions, but they do not provide a full accounting of the attorney general's activities.

The attorney general of Utah has one of the more informative annual reports. Unlike others, this report provides the total number of cases opened, closed, lawsuits filed, criminal charges filed, fines paid, and more. These numbers, however, are aggregated and not broken down by category, so it is still unclear what types of problems the attorney general is focused on.

Most state attorneys general do not contribute data for national monitoring of Internet-related fraud. The Consumer Sentinel, a project of the Federal Trade Commission, provides a state-by-state breakdown of consumer complaints related to fraud (see table on page 16). For each state, the commission ranks and enumerates fraud categories—including the categories of "Internet Services," "Computer Equipment and Software" and "Internet Auctions"—and provides the aggregate and average amount paid to those who filed complaints. Rankings are also available to compare the number of fraud complaints among states and metropolitan areas.

Data for the Consumer Sentinel are compiled from a variety of sources, including the FTC, the U.S. Department of Justice, Better Business Bureaus, and the National Consumers League, just to name a few. Only 13 state attorneys general, however, are listed as contributors to the Consumer Sentinel.[21] (This includes attorneys general from Alabama, California, Colorado, Kentucky, Louisiana, New Jersey, North Carolina, Ohio, Oklahoma, Rhode Island, South Dakota, Virginia, and Washington.) This lack of participation impedes our ability to observe national trends and reliably compare states.

The percentage of fraud complaints related to the Internet appears to be higher at the federal level. For 2007, the FTC's Consumer Sentinel reported that 40 percent of fraud complaints were Internet-related. States report a much lower percentage of Internet-related consumer complaints. The Consumer Sentinel data, however, cover only fraud, not consumer protection in general. Also, consumers may be more likely to report Internet-related complaints to a federal agency, whereas consumers with more traditional complaints, such as auto sales or home improvement, may be more likely to talk to a state office.

INTERNET-RELATED FRAUD COMPLAINTS COMPILED BY THE FTC

These complaint numbers are compiled from a variety of sources, including the FTC, the U.S. Department of Justice, Better Business Bureaus, and the National Consumers League, just to name a few. The FTC lists only 13 state attorneys general, however, as contributors of consumer complaint data.

STATE	2007			
	INTERNET-RELATED CATEGORY	RANK IN TOP 5	NUMBER OF COMPLAINTS	PERCENT OF TOTAL FRAUD COMPLAINTS
Alabama*	Internet Services	3	452	7%
	Computer Equipment and Software	5	303	5%
Alaska	Internet Services	3	111	8%
	Computer Equipment and Software	5	70	5%
Arizona	Internet Services	2	961	7%
Arkansas	Internet Services	2	236	7%
	Internet Auctions	3	184	5%
California*	Internet Services	2	5,629	9%
	Computer Equipment and Software	5	2,993	5%
Colorado*	Internet Services	2	939	8%
	Computer Equipment and Software	4	574	5%
	Internet Auctions	5	520	5%
Connecticut	Internet Services	4	360	7%
	Internet Auctions	5	342	6%
Delaware	Internet Services	2	122	9%
	Internet Auctions	5	88	7%
Florida	Internet Services	2	2,691	8%
	Internet Auctions	5	1,763	5%
Georgia	Internet Services	2	1,182	7%
	Computer Equipment and Software	5	779	5%
Hawaii	Internet Services	3	198	8%
	Internet Auctions	4	168	7%
Idaho	Internet Services	2	229	9%
	Internet Auctions	5	129	5%
Illinois	Internet Services	2	1,588	7%
	Computer Equipment and Software	3	1,173	5%
Indiana	Internet Services	3	716	7%
	Computer Equipment and Software	5	419	4%
Iowa	Internet Services	2	299	7%
	Internet Auctions	3	223	6%
	Computer Equipment and Software	5	212	5%
Kansas	Internet Services	3	252	7%
	Internet Auctions	4	203	5%
	Computer Equipment and Software	5	203	5%
Kentucky*	Internet Services	2	403	7%
	Computer Equipment and Software	5	309	6%
Louisiana*	Internet Services	4	308	6%
	Internet Auctions	5	264	5%

2006			
INTERNET-RELATED CATEGORY	RANK IN TOP 5	NUMBER OF COMPLAINTS	PERCENT OF TOTAL FRAUD COMPLAINTS
Internet Services and Computer Complaints**	3	417	9%
Internet Auctions	4	359	8%
Internet Services and Computer Complaints	1	286	27%
Internet Auctions	4	92	9%
Internet Services and Computer Complaints	3	952	10%
Internet Auctions	4	654	7%
Internet Services and Computer Complaints	2	224	9%
Internet Auctions	3	219	9%
Internet Services and Computer Complaints	1	5,324	11%
Internet Auctions	4	3,439	7%
Internet Services and Computer Complaints	2	723	9%
Internet Auctions	3	682	9%
Internet Services and Computer Complaints	3	499	11%
Internet Auctions	4	409	9%
Internet Services and Computer Complaints	2	129	12%
Internet Auctions	4	78	7%
Internet Services and Computer Complaints	2	2,601	10%
Internet Auctions	4	2,343	9%
Internet Services and Computer Complaints	2	1,171	10%
Internet Auctions	4	810	7%
Internet Services and Computer Complaints	3	207	10%
Internet Auctions	2	224	11%
Internet Services and Computer Complaints	4	165	8%
Internet Auctions	3	179	9%
Internet Services and Computer Complaints	3	1,354	10%
Internet Auctions	4	974	7%
Internet Services and Computer Complaints	3	688	9%
Internet Auctions	4	477	6%
Internet Services and Computer Complaints	3	271	10%
Internet Auctions	2	321	12%
Internet Services and Computer Complaints	4	276	9%
Internet Auctions	2	326	11%
Internet Services and Computer Complaints	4	399	9%
Internet Auctions	3	419	9%
Internet Services and Computer Complaints	4	339	9%
Internet Auctions	2	455	11%

INTERNET-RELATED FRAUD COMPLAINTS COMPILED BY THE FTC (CONTINUED)

STATE	2007			
	INTERNET-RELATED CATEGORY	RANK IN TOP 5	NUMBER OF COMPLAINTS	PERCENT OF TOTAL FRAUD COMPLAINTS
Maine	Internet Services	2	145	7%
	Internet Auctions	5	97	5%
Maryland	Internet Services	3	905	8%
	Computer Equipment and Software	5	622	5%
Massachusetts	Internet Services	2	802	8%
	Computer Equipment and Software	4	673	7%
Michigan	Internet Services	3	974	7%
Minnesota	Internet Services	2	654	7%
	Computer Equipment and Software	5	474	5%
Mississippi	Internet Services	2	212	8%
Missouri	Internet Services	2	807	6%
Montana	Internet Services	3	108	7%
	Internet Auctions	5	71	5%
Nebraska	Internet Services	2	219	8%
	Computer Equipment and Software	5	136	5%
Nevada	Internet Services	2	393	8%
	Internet Auctions	5	286	6%
New Hampshire	Internet Services	2	205	8%
	Internet Auctions	5	130	5%
New Jersey*	Internet Services	2	1,202	8%
	Computer Equipment and Software	3	884	6%
New Mexico	Internet Services	2	221	8%
	Computer Equipment and Software	5	114	4%
New York	Internet Services	2	2,332	9%
	Computer Equipment and Software	4	1,676	6%
	Internet Auctions	5	1,659	6%
North Carolina*	Internet Services	2	1,104	7%
	Computer Equipment and Software	4	765	5%
North Dakota	Internet Auctions	2	56	8%
	Internet Services	4	36	5%
	Computer Equipment and Software	5 (tie)	31	4%
Ohio*	Internet Services	2	1,274	7%
	Computer Equipment and Software	4	1,028	5%
Oklahoma*	Internet Services	2	350	7%
	Computer Equipment and Software	5	237	5%

2006			
INTERNET-RELATED CATEGORY	RANK IN TOP 5	NUMBER OF COMPLAINTS	PERCENT OF TOTAL FRAUD COMPLAINTS
Internet Services and Computer Complaints	2	177	10%
Internet Auctions	4	152	8%
Internet Services and Computer Complaints	2	998	12%
Internet Auctions	4	715	8%
Internet Services and Computer Complaints	2	801	11%
Internet Auctions	4	504	7%
Internet Services and Computer Complaints	3	993	9%
Internet Auctions	4	762	7%
Internet Services and Computer Complaints	3	532	9%
Internet Auctions	4	510	9%
Internet Services and Computer Complaints	3	173	7%
Internet Auctions	4	154	7%
Internet Services and Computer Complaints	3	688	9%
Internet Auctions	4	596	8%
Internet Services and Computer Complaints	3	121	9%
Internet Auctions	4	104	8%
Internet Services and Computer Complaints	3	183	9%
Internet Auctions	4	176	9%
Internet Services and Computer Complaints	4	397	9%
Internet Auctions	3	404	10%
Internet Services and Computer Complaints	3	225	11%
Internet Auctions	4	174	9%
Internet Services and Computer Complaints	2	1,320	12%
Internet Auctions	4	1,058	9%
Internet Services and Computer Complaints	2	222	9%
Internet Auctions	4	125	5%
Internet Services and Computer Complaints	3	2,157	10%
Internet Auctions	2	2,335	11%
Internet Services and Computer Complaints	3	998	10%
Internet Auctions	4	593	6%
Internet Services and Computer Complaints	4	39	7%
Internet Auctions	3	55	10%
Internet Services and Computer Complaints	3	1,318	9%
Internet Auctions	4	1,192	8%
Internet Services and Computer Complaints	3	356	10%
Internet Auctions	4	262	7%

INTERNET-RELATED FRAUD COMPLAINTS COMPILED BY THE FTC (CONTINUED)

STATE	2007			
	INTERNET-RELATED CATEGORY	RANK IN TOP 5	NUMBER OF COMPLAINTS	PERCENT OF TOTAL FRAUD COMPLAINTS
Oregon	Internet Services	2	671	9%
	Computer Equipment and Software	4	374	5%
	Internet Auctions	5	330	4%
Pennsylvania	Internet Services	3	1,419	7%
	Computer Equipment and Software	4	1,153	6%
Rhode Island*	Computer Equipment and Software	2	102	7%
	Internet Services	3	101	7%
South Carolina	Internet Services	3	439	7%
	Computer Equipment and Software	5	374	6%
South Dakota*	Internet Services	3	62	7%
	Internet Auctions	4	51	6%
Tennessee	Internet Services	2	691	7%
	Internet Auctions	5	466	5%
Texas	Internet Services	2	2,785	8%
	Computer Equipment and Software	4	1,795	5%
Utah	Internet Services	2	409	8%
Vermont	Internet Services	2	78	9%
	Internet Auctions	4	51	6%
Virginia*	Internet Services	2	1,116	8%
	Computer Equipment and Software	5	775	5%
Washington*	Internet Services	2	1,226	8%
	Computer Equipment and Software	4	795	5%
West Virginia	Internet Services	1	420	16%
	Internet Auctions	4	128	5%
Wisconsin	Internet Services	2	728	7%
	Computer Equipment and Software	3	580	6%
Wyoming	Internet Services	2	62	7%
	Internet Auctions	5	44	5%

* Indicates state attorney general listed as a contributor of consumer complaint data to the Consumer Sentinel (see http://www.consumer.gov/sentinel/contribs.htm).

** The category "Internet Services and Computers" was split into two categories—"Internet Services" and "Computer Equipment and Software"—in 2007.

Source: The Federal Trade Commission's Consumer Sentinel at http://www.consumer.gov/sentinel/

2006			
INTERNET-RELATED CATEGORY	RANK IN TOP 5	NUMBER OF COMPLAINTS	PERCENT OF TOTAL FRAUD COMPLAINTS
Internet Services and Computer Complaints	1	564	10%
Internet Auctions	4	433	8%
Internet Services and Computer Complaints	3	1,437	9%
Internet Auctions	4	1,298	8%
Internet Services and Computer Complaints	4	97	8%
Internet Auctions	1	160	14%
Internet Services and Computer Complaints	2	457	9%
Internet Auctions	4	348	7%
Internet Services and Computer Complaints	4	39	6%
Internet Auctions	3	56	9%
Internet Services and Computer Complaints	3	636	9%
Internet Auctions	4	605	9%
Internet Services and Computer Complaints	3	2,328	9%
Internet Auctions	4	1,617	6%
Internet Services and Computer Complaints	3	348	8%
Internet Auctions	4	282	6%
Internet Services and Computer Complaints	3	65	9%
Internet Auctions	4	56	8%
Internet Services and Computer Complaints	2	1,390	12%
Internet Auctions	4	829	7%
Internet Services and Computer Complaints	2	1,067	10%
Internet Auctions	4	631	6%
Internet Services and Computer Complaints	4	176	9%
Internet Auctions	2	184	9%
Internet Services and Computer Complaints	2	714	11%
Internet Auctions	4	520	8%
Internet Services and Computer Complaints	3	58	9%
Internet Auctions	4	58	9%

Case Examples: Attorneys General Combating Online Fraud and Abuse

State attorneys general can make a powerful difference in protecting consumers from Internet threats. States are not solely responsible for pursuing malicious actors, of course, nor should they be. Federal agencies, such as the Department of Justice and the Federal Trade Commission, play crucial roles in policing the Internet. But state attorneys general can broaden and diversify the pool of law enforcement officials who are actively combating Internet crime.

While most attorneys general, to this point, have not brought major cases against abuses unique to the Internet such as spyware, adware, and spam, there have been a few notable exceptions. This section summarizes a number of high-profile cases that ultimately resulted in settlements to the benefit of consumers. The attorneys general featured below are among the most aggressive online enforcers, setting an example for others to follow.

State of New York vs. Intermix Media

Long before the word "spyware" entered the popular lexicon, former New York Attorney General Eliot Spitzer was hot on the trail. In April 2005, Spitzer sued Intermix Media, a software distributor that was hijacking users' computers and serving loads of unwanted pop-up ads without providing any way for its software to be removed. The company ultimately entered into a $7.5 million settlement, and a separate $750,000 penalty was levied on the former CEO of Intermix. This remains the largest penalty to date for any state or federal spyware prosecution.

State of New York vs. Direct Revenue

About a year after settlement of the Intermix case, Spitzer sued Direct Revenue for surreptitiously installing adware on consumers' computers. The case is still pending, but the facts that emerged as a result ultimately played a significant role in the company's demise.

As with the Intermix case, Spitzer's office filed extensive records that exposed how adware installations occurred and the financial arrangements among the various actors involved. The combined effect of these two lawsuits not only sent a signal to the online advertising industry, but also provided the public and policymakers with a rare window into the operations of this normally secretive industry.

People of the State of California vs. Optin Global et al.

Also in April 2005, former California Attorney General Bill Lockyer teamed up with the Federal Trade Commission to launch a suit against a pair of spammers running a massive operation under the names Optin Global, Inc. and Vision Media Limited Corp. The duo sent over 2 million unsolicited e-mails in a single year, advertising mortgage services, pharmaceuticals, auto warranties, and other products. Message recipients who responded to the offers were prompted to provide personal information, which the spammers secretly sold to marketers. The pair settled for $2.4 million in damages, penalties, and fees.

State of Texas vs. Sony BMG

In the fall of 2005, controversy erupted when it was discovered that Sony BMG had included invasive anti-piracy software on millions of its CDs. The software hid itself on users' computers using "rootkit" techniques common to spyware; opened security vulnerabilities on users' computers; did not ask for user consent prior to installation; and "rooted" itself so deeply into a computer's operating system that it could not readily be uninstalled.

The New York Attorney General's office quickly responded by demanding an immediate global recall, which Sony BMG agreed to within 12 hours. A number of other states, including Massachusetts, Florida, and Texas, then took notice and sought additional relief for consumers.

In December 2006, Texas Attorney General Greg Abbott settled with the company, securing replacement CDs for consumers and restitution for damaged computers. Ultimately, Sony also entered into a $4.25 million settlement with 40 other states and settled a separate California suit. These cases have spurred ongoing dialogue about the dangers of invasive technologies designed to restrict the use of copyrighted material.

State of Washington vs. Secure Computer et al.

In 2006, Washington Attorney General Rob McKenna launched six spyware lawsuits. This work began with a suit against Secure Computer, a company that used deceptive pop-up advertisements to convince consumers to purchase fake security software by alarming them about fictitious spyware infections on their computers. The company settled for $1 million in December 2006 and agreed to reimburse consumers who had purchased the fake products.

State of Washington vs. Consumer Digital Services et al.

McKenna followed up on the state's spyware work with a June 2007 lawsuit against the operators of several websites—including privasafe.com and surfsafe.com—that lured consumers into divulging personal information that the site operators then sold to third parties and used to bill consumers for unwanted services. The site operators hawked "free" gift cards, flat-screen monitors, and other products through Web pop-ups, banner ads, and e-mail. More than 13,000 Washington consumers submitted personal information in order to obtain the products, but only one consumer actually received a free item. All who submitted information were subsequently charged $14.95 on their monthly phone bills for Internet-related services they did not

want. The settlement requires the site operators to refund affected consumers and pay other penalties and fees that could ultimately total $1 million.

State of New York Settlements with Priceline, Travelocity, and Cingular

Growing out of New York's investigation of Direct Revenue, a company that surreptitiously installed adware on consumers' computers, Attorney General Andrew Cuomo announced groundbreaking settlements with three advertisers that had used Direct Revenue's software to display their ads. Priceline, Travelocity, and Cingular agreed to pay a combined $100,000 to the state for promoting their products through the deceptively installed adware. These settlements marked the first time that advertisers have been held responsible for doing business with adware distributors that engaged in nefarious practices.

Recommendations

Consumers are paying a steep price for online fraud and abuse. They need aggressive law enforcement to punish perpetrators and deter others from committing Internet crime. A number of leading attorneys general have shown they can make a powerful difference. But others must step up as well. To protect consumers and secure the future of the Internet, we recommend that state attorneys general take the following steps:

Evaluate state laws applicable to online consumer protection. It may be unclear how state consumer protection laws, many written before the explosion of the Internet, translate to the online world. State attorneys general should review their state laws and provide clarity to the relevant units in their offices on what constitutes Internet crime and how such crime should be enforced. Where state laws are not adequate to protect online consumers, attorneys general should make recommendations for legislative action. This evaluation should consider laws in those states that have been active in policing Internet crime.

Train investigators and prosecutors in identifying the legal attributes of online fraud and abuse. The newness and ever-evolving nature of online fraud and abuse presents significant challenges for investigators and prosecutors. State attorneys general should provide to their staffs continuing education on applicable laws, how they apply to the online world, and the attributes of Internet crime, so that fraud and abuse can be identified and prosecuted. State attorneys general might consider engaging private companies that sell anti-fraud products to assist with prosecutor training.

Develop computer forensic capabilities. Purveyors of online fraud and abuse—and the methods they use—are often extremely difficult to detect. Computer forensics are thus needed to trace and catch Internet fraudsters. Attorneys general in Washington and New York invested in computer forensics and, as a result, were able to prosecute successful cases against spyware. Most states, however, have little in the way of computer forensic capability.

Developing this capability may not require substantial new funds. Rather, most important are human and intellectual resources. Even New York's more intensive adware investigations, for instance, were done with free or low-cost software, which, among other things, captured screenshots, wiped hard drives, and tracked IP addresses and installation information through "packet sniffing" tools. Attorneys general must make investments in human capital so that such software can be harnessed and put to use.

Devote greater resources to Internet enforcement efforts. The state data presented in this report show that Internet crime is one of the most serious problems faced by consumers. Resources devoted to enforcement, however, are not yet commensurate with this problem. Attorneys general should assess what resources are necessary to investigate online fraud and abuse, to bring cases against perpetrators, and ultimately to provide a credible deterrent against Internet crime. Attorneys general should work with their governors and state legislatures to secure necessary funding.

Partner with commercial and public-interest coalitions that are fighting online fraud and abuse. The offices of state attorneys general frequently lack adequate expertise on Internet crime, but there are a number of coalitions that can help. They include the Coalition Against Unsolicited Commercial Email, the Anti-Spyware Coalition, StopBadware.org, and the Anti-Phishing Working Group. State attorneys general should draw on these coalitions for advice and support.

Establish coordinated efforts with other attorneys general. State attorneys general frequently engage in coordinated multi-state investigations in civil cases, but these usually focus on one company at a time, as with the Sony BMG case discussed earlier. There is no standing multi-state task force on Internet fraud and abuse that pools evidence and ideas, expands jurisdictional authority by having states issue subpoenas on each other's behalf, and takes collective action. In the criminal context, by contrast, there are a number of multi-state task forces, such as the Crimes Against Children Task Force. Without coordination, states may be deterred from pursuing cases that are cross-jurisdictional—as Internet cases typically are—or if they proceed alone, they may bring weak cases. By improving coordination, perhaps by establishing a standing Internet task force, attorneys general can build more cases with better evidence.

Aggressively investigate consumer complaints. Some states mediate consumer complaints against businesses. New York, for example, has several mediators who review complaints, gather evidence—which ultimately can be used to bring suit—and help consumers obtain any refunds they are owed. This mediation role forces the state to take a closer look at each complaint, carefully categorize complaints, and track how they are resolved. Moreover, the information gathered in this process assists broader analysis of harmful business practices, which can help guide priorities. A number of Internet-related cases have grown out of New York's mediation process (not including the spyware cases discussed earlier). Some states follow the FTC model, however, and do not mediate consumer complaints, or mediate only on a limited basis. Thus, complaints may not be investigated. States should consider adopting the mediation approach.

Categorize Internet-related complaint data by type using a consistent categorization system. It is difficult to assess consumer complaints because of weaknesses in state data. First, some states do not categorize complaints at all. This information is needed to help judge which types of consumer threats are most prevalent and most deserving of attention. Second, categories are inconsistently labeled across states. Nebraska, for example, uses the category "Internet Transaction" while Oregon uses two sepa-

rate categories, "Internet Retailers" and "Internet Auctions." Such inconsistencies make it difficult to draw comparisons across states and assess national trends. Finally, states typically do not break down categories into more detailed subcategories, such as spam and phishing. Lumping together all Internet-related complaint data is of limited use given the array of online threats. More precise assessment of our problems requires a more precise level of data. Accordingly, the state attorneys general should work together through the National Association of Attorneys General to develop more robust data and a common system of categorization.

Allow consumers to classify their own complaints through the Web. Many states already allow consumers to register complaints through online forms. It would not be difficult to let consumers categorize their own complaints through such forms. Providing this ability—and then aggressively publicizing it—would reduce the burden on states in categorizing data.

Compile data on actions taken against Internet fraud and abuse. State attorneys general must do a better job of communicating their work on behalf of consumers. Texas provided us with data on actions taken in response to consumer complaints. Such data should be routinely gathered and reported. Residents have a right to know whether their state attorney general is adequately protecting their interests on the Internet and in other areas.

Provide data through the Internet on consumer complaints and actions taken. It is not enough just to gather more robust data on consumer complaints and actions taken. State residents must also be able to easily obtain this information. As noted earlier, less than a quarter of state websites currently provide a ranked list of consumer complaints. It took repeated requests to obtain such data from other states. For 14 states, we were unsuccessful in obtaining any data at all. It is time for state attorneys general to move into the digital age. With access to relevant data through the Internet, state residents are alerted of potential threats, can participate in the policymaking process, and are able to hold the attorney general accountable for results.

Provide complaint data for the FTC's Consumer Sentinel. Only 13 state attorneys general are contributors to the Consumer Sentinel, which provides data by state on complaints related to fraud. All attorneys general should participate to ensure consistent data across states and to draw a clearer national picture of the problems facing consumers. To participate, states will need to break down data into the FTC's complaint categories. This should not preclude states, however, from developing their own separate categorization methods.

AG CASES HIGHLIGHTED BY THE CYBERCRIME NEWSLETTER

The Cybercrime Newsletter is a bimonthly publication of the National Association of Attorneys General. Each issue lists Internet-related actions taken by attorneys general. Actions listed in the newsletter are not comprehensive—that is, there may be other Internet-related actions not listed—but they do give a sense of what attorneys general are focused on. The numbers presented here include all inquiries, investigations, and enforcement actions related to specific cases. They exclude other actions highlighted in the newsletter such as speeches given, general initiatives, or educational materials produced. Issues of the Cybercrime Newsletter can be viewed at http://www.naag.org/publications_cybercrime.php.

2008

CATEGORY	STATE	CASE DESCRIPTION	ISSUE*
Spyware, Adware, Spam, and Phishing	WA	AG Rob McKenna filed suit against the owner of Messenger Solutions, LLC., for violating the state's Computer Spyware Act by blasting out ads for pornography and Viagra in an effort to trick consumers into buying software that purported to protect against pop-ups but actually caused their computers to continuously send messages to other consumers.	March–April
Internet Sales, Services, and Auctions	Multi-state	AGs of 26 states reached a settlement with the Florida-based operators of USDirectory.com, an Internet Yellow Page service, in which the company agreed to stop deceptive marketing and pay $400,000 in restitution.	March–April
	AL	AG Terry Goddard filed suit against Internet-business Top Stone, Inc., for failing to deliver marble and granite products ordered online, even though customers provided large deposits.	March–April
	FL	AG Bill McCollum reached a $1 million settlement with World Avenue, LLC, which promotes Internet goods and services, over allegations that the company deceptively offered free merchandise.	January–February
	ID	AG Lawrence Wasden announced a $163,225 civil penalty against an Internet tobacco seller who sold more than two million cigarettes that were not on the state's Directory of Compliant Tobacco Product Manufacturers and Brand Families.	March–April
	KY	AG Jack Conway announced the indictment of a woman for failing to deliver a Lexus she sold on eBay for more than $30,000 to a Kentucky resident.	March–April
	NY	AG Cuomo issued a subpoena to Comcast Corp. in connection to complaints over the cable company's handling of Internet traffic.	January–February
	OR	AG Hardy Myers entered into a settlement with Texas-based Ad TelAmerica Inc. in connection to complaints of bogus invoices and solicitations.	January–February
Data Security, Confidential Records, and Identity Theft	MO	AG Jay Nixon filed a lawsuit against www.PublicData.com for allegedly selling private information, such as Social Security numbers.	January–February
	MO	AG Jay Nixon filed a lawsuit against the business operating a1peoplesearch.com for allegedly selling personal information such as Social Security numbers, addresses, dates of birth and criminal records.	March–April
Sexual Enticement of Minors and Child Pornography	Multi-state	In an agreement with fifty attorneys general, MySpace.com committed to take steps to protect minors using its Website.	January–February
	FL	AG Bill McCollum announced a three-year sentence for a man who pleaded guilty to sexually propositioning a minor over the Internet.	March–April
	GA	AG Thurbert Baker announced that a man was sentenced to 30 years in prison for online child pornography.	March–April
	HI	AG Mark Bennett announced that a man was sentenced to five years in prison for enticement of a child over the Internet.	March–April
	IL	AG Lisa Madigan's Internet Crimes Against Children Task Force arrested an alleged child pornographer.	January–February
	LA	AG James Caldwell's High Technology Crime Unit arrested an alleged online child predator.	January–February
	LA	AG Caldwell's High Technology Crime Unit arrested a man for Internet solicitation of a minor.	
	MS	AG Jim Hood announced a five-year sentence for a man who pleaded guilty to possession of child pornography.	January–February
	MS	AG Hood announced that a former school teacher was convicted on possession of child pornography received by e-mail from Russia.	March–April
	NM	AG Gary King's Internet Crimes Against Children Task Force arrested an alleged online predator and child pornographer.	January–February
	NC	AG Roy Cooper's office arrested a former youth soccer coach for allegedly possessing child pornography downloaded from the Internet.	March–April
	PA	AG Tom Corbett's Child Predator Unit arrested a man for sexually propositioning a minor over the Internet.	January–February
	PA	AG Tom Corbett's Child Predator Unit arrested a man for sexually propositioning a minor over the Internet.	March–April
	SC	AG Henry McMaster announced the arrest of an alleged online child predator.	January–February
	SC	AG Henry McMaster announced the arrest of a man for soliciting a minor over the Internet.	March–April
	TX	AG Greg Abbott's Cyber Crimes Unit arrested a police officer for online solicitation of a minor.	January–February
	TX	AG Greg Abbott announced the guilty plea of a man who used MySpace to e-mail child pornography to a minor.	March–April
	UT	AG Mark Shurtleff announced three arrests for online child pornography.	March–April
Other	CT	AG Richard Blumenthal requested documents from JuicyCampus.com, a college gossip site, on its enforcement of rules against libelous, defamatory, and abusing postings.	March–April
	NJ	AG Anne Milgram's prosecutors subpoenaed the records of JuicyCampus.com, a college gossip site, to determine whether the web site is violating the state's Consumer Fraud Act by claiming it does not allow offensive material.	March–April

*2008 cases cover only the January–February and March–April issues.

AG CASES HIGHLIGHTED BY THE CYBERCRIME NEWSLETTER (CONTINUED)

2007

CATEGORY	STATE	CASE DESCRIPTION	ISSUE
Spyware, Adware, Spam, and Phishing	NY	AG Andrew Cuomo reached settlements with three major online advertisers—Priceline.com, Travelocity.com LP, and Cingular Wireless LLC—that allegedly promoted services and products on the Internet through deceptively installed programs known as adware.	January–February
	WA	AG Rob McKenna reached a settlement with HoanVinh Nguyenphuoc, the owner of FixWinReg, which allegedly violated the state's consumer protection and spyware laws by simulating Windows security warnings that were actually ads for registry-cleaner software.	September–October
	WA	AG McKenna reached a settlement with three California-based businesses—Digital Enterprises d/b/a Movieland.com, AccessMedia Networks and Innovative Networks—that allegedly violated the state's spyware and consumer protection laws by installing software on consumers' computers that launched persistent pop-ups demanding payment for a movie download service.	March–April
	WA	AG McKenna reached a settlement that requires the operators of www.privasafe.com and www.surfsafeinternetservices.com to refund as much as $1 million for billing consumers for "free" gifts promised by pop-up and banner ads.	May–June
Internet Sales, Services, and Auctions *(12 cases)*	Multi-state	AGs of 48 states and the District of Columbia reached a $3 million settlement with AOL over consumer complaints of difficulty and confusion in trying to cancel their AOL paid services.	July–August
	CT	AG Richard Blumenthal demanded information from Sunrocket, a Virginia-based Internet telephone provider, about its Connecticut customers who abruptly lost phone service when the company shut down.	July–August
	ID	AG Lawrence Wasden reached a settlement in which Thompson Hill Publishing of Montreal, a publisher of "Internet Yellow Pages," agreed to cancel the outstanding accounts of 10 Idaho businesses that claimed Thompson Hill falsely represented itself as the consumers' local "yellow page directory."	July–August
	IN	AG Steve Carter reached a settlement with an Internet seller who allegedly did not deliver auto parts advertised online in a timely fashion and delivered incorrect or defective parts.	March–April
	MO	AG Jay Nixon obtained a preliminary injunction barring a couple that made false guarantees in selling Internet advertising to small businesses from operating to Missouri.	January–February
	NJ	AG Anne Milgram announced that a prisoner would serve an additional three years for defrauding investors out of $35,500 by falsely claiming over the Internet that he could obtain investors and investment capital from businesses.	July–August
	NY	AG Andrew Cuomo announced a $1 million settlement with Verizon Wireless in which the company agreed to stop deceptive advertising.	September–October
	NY	AG Cuomo reached a $400,000 settlement with ENH Group, LLC, one of the nation's largest jewelry auction houses, which allegedly used shill bidding to inflate prices of goods sold through online auctions.	May–June
	OH	AG Mark Dann filed suit against Courts Online, an Internet-based company offering unlimited searches of its data holdings for a one-time fee, for allegedly failing to deliver purchased services, misrepresenting services offered, and failing to properly advise consumers about refund policies.	March–April
	OK	AG Drew Edmondson filed charges against an eBay seller for allegedly defrauding consumers in five states out of more than $10,000.	November–December
	WA	AG Rob McKenna sued Internet Advancement (also know as 4GreatBuys.com), a search engine marketing services company, for allegedly misrepresenting its services, failing to honor its guarantees on refunds, and making unauthorized charges to customers' credit cards.	November–December
	WV	AG Darrell McGraw shut down Sataline.com for failing to deliver promised services involving the delivery of premium cable television via the Internet.	March–April
Data Security, Confidential Records, and Identity Theft	Multi-state	In a settlement with the AGs of 43 states and the District of Columbia, ChoicePoint agreed to adopt stronger security measures in response to a massive breach of its data holdings containing consumers' personal information.	May–June
	AL	AG Troy King announced the arrest of a former state conservation officer for unlawfully obtaining criminal records.	September–October
	CT	AG Richard Blumenthal sued Accenture, a New York-based technology services company, for failing to secure confidential information of 58 state taxpayers and hundreds of state bank accounts.	September–October
	CT	Connecticut Attorney General Richard Blumenthal asked Pfizer to take steps to protect its employees following a massive security breach at the company.	May–June
	NY	AG Andrew Cuomo reached a first-ever settlement under the state's Information Security Breach and Notification Act with CS STARS LLC, a Chicago-based claims management company, which allegedly did not provide timely notification that the personal information of about 540,000 state consumers was at risk.	March–April
	RI	AG Patrick Lynch filed a Civil Investigative Demand against The TJX Companies Inc. for its alleged failure to prevent computer security breaches and to properly notify consumers of compromised information.	January–February
	TX	Attorney General Greg Abbot filed suit against TheDollPalace.com and Gamesradar.com, two web sites that cater to children but allegedly fail to adequately protect their privacy and safety as required under the federal Children's Online Privacy Protection Act (COPPA).	November–December

AG CASES HIGHLIGHTED BY THE CYBERCRIME NEWSLETTER (CONTINUED)

2007 (CONTINUED)

CATEGORY	STATE	CASE DESCRIPTION	ISSUE
Sexual Enticement of Minors and Child Pornography *(50 cases)*	AL	AG Troy King announced the arrest of a man for child pornography.	July–August
	AZ	AG Terry Goddard announced the arraignment of two individuals on multiple charges related to identity theft and possession of child pornography.	May–June
	FL	AG Bill McCollum's Child Predator CyberCrime Unit arrested a man for approaching an undercover investigator on an online chat room and offering to pay for sex with children.	July–August
	FL	AG McCollum announced that 126 alleged child predators were arrested by a task force of local, state and federal law enforcement officials.	May–June
	FL	AG McCollum's Child Predator CyberCrime Unit arrested a man for sexually propositioning a minor over the Internet.	March–April
	FL	AG McCollum announced a 10-year sentence for a man who pled guilty to sexually soliciting a minor over the Internet.	January–February
	FL	AG McCollum announced that an offender was sentenced to 15 years in prison after pleading guilty to multiple charges of possession of child pornography.	November–December
	HI	AG Mark Bennett announced the conviction of a man for online enticement of a child.	September–October
	HI	AG Bennett announced the arrest of a man for online enticement of minors.	May–June
	HI	AG Bennett announced the arrest of a man for online enticement of a child.	July–August
	HI	AG Bennett announced a guilty plea for online enticement of a child.	November–December
	IL	AG Lisa Madigan announced the arrest of an individual for online enticement of a child.	September–October
	KY	AG Greg Stumbo announced the arrests of seven in a child sexual predator sting.	September–October
	KY	AG Stumbo announced the arrest of a man in a child predator sting.	March–April
	KY	AG Greg Stumbo announced that eight individuals caught in a child predator sting have been scheduled for court appearances.	January–February
	LA	AG Charles Foti, Jr. announced the arrest of a high school teacher for inappropriate contact with one of his students based on transcripts of chats on MySpace.com.	January–February
	MA	AG Martha Coakley announced the indictment of a man for possession of child pornography based on information provided by the state's Internet Crimes Against Children Task Force.	July–August
	MI	AG Mike Cox announced the arrest of a man for using the Internet to solicit a minor for sexual acts and sending a minor pornographic images.	November–December
	MI	AG Cox's investigators arrested a man for using the Internet to solicit child pornography and sex from a minor.	July–August
	MI	AG Cox announced the arrest of a Cornell educator for using the Internet to arrange a sexual encounter with a minor.	May–June
	MI	AG Cox announced the arrests of two individuals for using the Internet to sexually proposition a minor and to disseminate sexually explicit material to a minor.	March–April
	MI	AG Cox's investigators arrested a man for using the Internet to disseminate sexually explicit material to a minor.	January–February
	MS	AG Jim Hood announced the sentencing of a man for child pornography.	November–December
	MS	AG Hood announced the conviction of an offender for transmitting and possession of child pornography.	September–October
	MS	AG Hood announced the sentencing of a community college professor who pled guilty to 12 counts of possession of child pornography.	May–June
	NJ	AG Anne Milgram announced the results of her Operation Silent Shield investigation into child pornography that led to 41 arrests.	September–October
	NM	AG Gary King's Internet Crimes Against Children Unit arrested a father and son on multiple charges of possession and distribution of child pornography.	November–December
	NM	AG King prevailed in convincing the state Court of Appeals to overturn a lower court ruling that had excluded a suspect's computer drive from evidence gathered to prosecute him on child pornography charges.	July–August
	NM	AG King announced that an offender was sentenced to 18 months for soliciting a child over the Internet.	March–April
	NM	AG King announced that a former police officer was sentenced to six and a half years for child solicitation over the Internet.	January–February
	PA	AG Tom Corbett's Child Predator Unit agents arrested a man for sexually propositioning a minor over the Internet.	November–December
	PA	AG Corbett announced the arrests of two individuals caught in a child predator sting.	September–October
	PA	AG Corbett's Child Predator Unit agents arrested a man for propositioning two minors in an Internet chat room.	July–August
	PA	AG Corbett's Child Predator Unit agents arrested a man for using an Internet chat room to sexually proposition what he believed to be a 13-year-old girl.	May–June
	PA	AG Corbett's Child Predator Unit agents arrested a man for sexually propositioning a minor.	March–April

AG CASES HIGHLIGHTED BY THE CYBERCRIME NEWSLETTER (CONTINUED)

2007 (CONTINUED)

CATEGORY	STATE	CASE DESCRIPTION	ISSUE
Sexual Enticement of Minors and Child Pornography *(50 cases)* (continued)	PA	AG Corbett's Child Predator Unit arrested a man for using an Internet chat room to sexually proposition a minor.	January–February
	SC	AG Henry McMaster announced the arrest of a man who was caught in a child predator sting.	September–October
	SC	AG McMaster announced the arrest of a man who was caught in a child predator sting.	July–August
	SC	AG McMaster announced the arrest of a man who was caught in a child predator sting.	May–June
	SC	AG McMaster announced that a Michigan man was arrested in a child predator sting.	March–April
	SC	AG McMaster announced the arrest of a man in an undercover Internet sting for sexually soliciting a minor.	January–February
	SC	AG McMaster announced the arrest of a man for soliciting sex from a minor over the Internet.	November–December
	TX	AG Greg Abbott announced a seven-year sentence for a man who solicited sex over the Internet from someone he believed to be a 14 year-old girl.	September–October
	TX	AG Abbot announced the sentencing of an offender to 40 years in prison for possessing and transmitting child pornography.	July–August
	TX	AG Abbot announced the sentencing of an offender to 70 years in prison for using the Internet to solicit sex with a minor and possession of child pornography.	May–June
	TX	AG Abbott announced that a man arrested by Abbott's Cyber Crimes Unit was sentenced to 95 years.	March–April
	TX	AG Abbott's Cyber Crimes Unit obtained a guilty plea from a former police officer for possession of child pornography.	January–February
	UT	AG Mark Shurtleff announced the arrest of a man for allegedly sexually abusing a 6-year-old boy and manufacturing and distributing child pornography.	May–June
	UT	AG Shurtleff announced the arrest of a man for possessing child pornography and another man for enticement of a minor over the Internet.	March–April
	UT	AG Shurtleff announced the conviction of a man for enticement of a minor over the Internet.	January–February
Other *(4 cases)*	CT	AG Richard Blumenthal sued Maximus Inc., a Virginia company, for failure to provide a timely and complete upgrade of a major online law enforcement database in accordance with their contract with the state.	November–December
	IN	AG Steve Carter obtained a court order halting two businesses from selling imitation high school and university diplomas via the Internet.	July–August
	FL & KY	Florida AG Bill McCollum and Kentucky AG Greg Stumbo cooperated on an investigation resulting in a seizure of illegal shipments of Phentermine, a weight loss drug with potentially serious side effects that had been shipped to state residents from an unlicensed Internet pharmacy in Florida.	May–June
	OK	AG Drew Edmondson announced that two employees of the Kiamichi Technology Center were named in a multicounty grand jury indictment that accuses them of using their state-issued computers and printers to print campaign material for a Center Board of Education member.	July–August

AG CASES HIGHLIGHTED BY THE CYBERCRIME NEWSLETTER (CONTINUED)

2006

CATEGORY	STATE	CASE DESCRIPTION	ISSUE
Spyware, Adware, Spam, and Phishing *(10 cases)*	CA	A prolific spam operation (involving Optin Global and Vision Media) agreed to pay $475,000 and refrain from illegal activity as part of a settlement with then AG Bill Lockyer and the FTC.	March–April
	FL	AG Charlie Crist filed a lawsuit against Rik Rodriguez for allegedly sending more than 1,100 illegal emails to more than 2,500 recipients in an effort to sell a bogus device, Fuel Saver Pro.	January–February
	MS	Following a joint investigation by the AG's office and the FBI, Robert Swilley pled guilty to a phishing scheme that spoofed the America Online web site to collect names and passwords that he then sold to a spamming business.	March–April
	NY	AG Eliot Spitzer sued Direct Revenue LLC for secretly installing malicious programs on personal computers and delivering ads using spyware.	May–June
	NY	AG Spitzer sued Gratis Internet for selling e-mail addresses obtained from millions of consumers—lured to a company Website promising free iPods, DVDs and video games—despite a promise of confidentiality.	March–April
	TX	AG Greg Abbott charged Sony BMG with violating the state's spyware and deceptive trade practices law.	January–February
	WA	AG Rob McKenna reached a $1 million settlement with NY-based Secure Computer in the first case under the state's new computer spyware law.	November–December
	WA	AG McKenna filed a lawsuit under the state's new computer spyware law accusing four California-based companies (Digital Enterprises, d/b/a Movieland.com; Alchemy Communications; AccessMedia Networks; and Innovative Networks) of installing software on personal computers that launches persistent pop-ups demanding payment for a move download service.	July–August
	WA	AG McKenna launched a spyware lawsuit against NY-based Secure Computer that was subsequently settled for $1 million (see above).	January–February
	WA	AG McKenna announced a settlement with the owners of two California companies—AvTech Direct and MD&I—in the state's first anti-spam lawsuit filed under the 2004 federal Can-Spam law.	May–June
Internet Sales, Services, and Auctions *(14 cases)*	Multi-state	In a settlement with AGs of 33 states, Lorillard Tobacco Co. agreed to implement new measures to prevent the illegal sale of its cigarettes over the Internet and by mail.	July–August
	Multi-state	In a settlement with AGs of 37 states, Phil Morris USA agreed to voluntarily incorporate protocols aimed at combating the illegal sale of its cigarettes over the Internet and by mail.	January–February
	Multi-state	In a $2 million settlement with AGs of 34 states, YP Corporation agreed to resolve claims that the company deceived consumers by automatically signing them up for its online yellow pages.	November–December
	Multi-state	AGs of 28 states settled with PayPal following consumer complaints about the company's billing and dispute resolution practices.	September–October
	AZ	AG Terry Goddard filed suit against Guaranteed Prescriptions Pharmaceutical Wealth Network for allegedly selling bogus pharmaceutical Websites to consumers.	November–December
	CA	AG Bill Lockyer reached a settlement with MyPerfectCredit, which allegedly engaged in false Internet advertising and unfair business practices in promising consumers to correct credit errors.	January–February
	FL	AG Charlie Crist reached settlement with America Online providing restitution to state consumers who experienced billing and membership problems.	November–December
	MA	AG Tom Reilly reached an agreement with an Internet company, registered to a Massachusetts resident, that allegedly failed to refund overcharges and misled 128 British consumers into thinking the site was based in the UK.	January–February
	MO	AG Jay Nixon filed suit against the owner of Doxy Lingerie for failing to promptly deliver goods ordered and paid for online.	November–December
	OK	AG Drew Edmondson charged a woman with violating the state Consumer Protection Act for selling, but failing to deliver, five laptop computers on the Internet.	January–February
	OR	AG Hardy Myers filed an Assurance of Voluntary Compliance with westcoastwagers.net in connection with the site's unauthorized use of the Oregon Food Bank's name in text message solicitations.	May–June
	WA	AG Rob McKenna reached a $400,000 settlement with SoftwareOnline.com after a four-month investigation found that the company falsely claimed its products were necessary to prevent attacks from malicious Websites, bombarded potential customers with pop-up ads, and used deceptive billing practices.	March–April
	WV	AG Darrell McGraw sued to enforce investigative subpoenas against 14 Internet payday lenders accused of making usurious "payday" loans with interest rates well over the state legal limit.	November–December
	WV	AG McGraw worked with Canadian police and Internet service providers to shut down Global Capitol Solutions and New Balance Express, two online loan companies who tried to defraud out-of-state consumers. Both companies listed fake WV addresses on their web sites, but were actually based in Canada.	July–August

AG CASES HIGHLIGHTED BY THE CYBERCRIME NEWSLETTER (CONTINUED)

2006 (CONTINUED)

CATEGORY	STATE	CASE DESCRIPTION	ISSUE
Data Security, Confidential Records, and Identity Theft *(8 cases)*	AZ	AG Terry Goddard announced an identity theft indictment.	January–February
	CA	AG Lockyer filed charges against former Hewlett-Packard Chairwoman Patricia Dunn and investigators hired by HP for fraudulently obtaining confidential records, identity theft, accessing computer data without authorization, and conspiracy.	September–October
	FL & MO	Attorneys general of FL and MO collaborated in the investigation of Henry Berry of Florida, who allegedly stole the identities of Missouri residents online in order to open credit accounts and purchase merchandise and gift cards.	January–February
	MO	AG Jay Nixon obtained a permanent injunction against Completeskipractice.com, a Utah-based Web site, prohibiting the company from obtaining or selling cell phone records of Missourians.	September–October
	MO	AG Nixon obtained court orders to stop Internet business Locatecell.com from offering to sell the cell phone records of customers in the state.	January–February
	MO	AG Nixon filed felony charges in an identity theft case.	March–April
	NV	AG George Chanos announced the arrest of an online identity thief.	May–June
	VA	AG Bob McDonnell announced a guilty plea in a case involving a perpetrator who used illegally obtained ID information to apply for credit cards over the Internet.	July–August
Sexual Enticement of Minors and Child Pornography *(54 cases)*	AZ	AG Terry Goddard announced the sentencing of a child predator.	September–October
	CO	AG John Suthers announced first arrest under new luring law.	September–October
	FL	AG Charlie Crist announced the arrest of an alleged child predator	September–October
	FL	AG Crist announced the sentencing of an individual for child pornography	July–August
	FL	AG Crist announced the sentencing of a child predator	May–June
	HI	AG Mark Bennett's agents arrested an alleged child predator.	November–December
	HI	AG Bennett announced charges against an alleged online predator.	January–February
	IL	AG Lisa Madigan's Internet Crimes Against Children task force arrested an alleged predator.	November–December
	IL	AG Madigan's task force arrested an alleged sex offender.	July–August
	IL	AG Madigan's task force apprehended an alleged child predator	May–June
	IL	AG Madigan's task force announced charges against an alleged online predator.	January–February
	LA	AG Charles Foti joined in an undercover Internet action that resulted in multiple arrests of alleged online predators.	September–October
	LA	AG Foti's agents arrested an alleged child pornographer.	July–August
	LA	AG Foti charged a man with 68 counts of child pornography.	January–February
	MA	AG Tom Reilly announced a guilty plea for possession and dissemination of child pornography.	September–October
	MA	AG Reilly's agents arrested alleged online child pornographers.	March–April
	MI	AG Mike Cox announced the arrest of an alleged Internet predator.	November–December
	MI	AG Cox charged a convicted child pornographer with committing identity theft to avoid having to register as a sex offender.	September–October
	MI	AG Cox announced the arrest of an alleged online child predator	July–August
	MI	AG Cox announced the arrest of an alleged online child predator	May–June
	MI	AG Cox announced the arrest of an alleged online child predator	March–April
	MI	AG Cox announced the conviction of an online child predator.	January–February
	MS	AG Jim Hood announced the arrest of an Internet child pornographer.	November–December
	MS	AG Hood announced the sentencing of an online child predator	May–June
	MS	AG Hood announced the sentencing of an online child predator	January–February
	NE	AG Jon Bruning announced the conviction of an online child predator	January–February
	NV	AG George Chanos announced indictments in connection to an Internet child pornography ring	March–April
	NM	AG Patricia Madrid announced the arrest of an alleged Internet sex offender	September–October
	NM	AG Madrid announced the indictment of an alleged child predator	July–August
	NM	AG Madrid's Internet Crimes Against Children unit arrested an alleged online child predator.	May–June
	NM	AG Madrid's Internet Crimes Against Children unit captured an alleged online child predator.	March–April

AG CASES HIGHLIGHTED BY THE CYBERCRIME NEWSLETTER (CONTINUED)

2006 (CONTINUED)

CATEGORY	STATE	CASE DESCRIPTION	ISSUE
Sexual Enticement of Minors and Child Pornography *(54 cases)* (continued)	NM	AG Madrid announced the indictment of an alleged child pornographer	January–February
	NC	AG Roy Cooper's agents participated in a sting that led to the arrest of a former chief of police for Landis, N.C., on charges of child solicitation and child pornography	July–August
	OH	AG Jim Petro announced the sentencing of a former Wapakoneta, Ohio, police chief for accessing child pornography on his work computer.	July–August
	PA	AG Tom Corbett announced the guilty plea of an online child predator	November–December
	PA	AG Corbett announced charges against an alleged online child predator	July–August
	PA	AG Corbett's Child Predator Unit arrested four in Internet sting.	May–June
	PA	AG Corbett announced charges against an alleged online child predator	March–April
	SC	AG Henry McMaster announced the arrest of an alleged online child predator.	November–December
	SC	AG McMaster announced the arrest of an alleged online child predator.	September–October
	SC	AG McMaster announced the arrest of an alleged online child predator.	July–August
	SC	AG McMaster announced the arrest of an alleged online child predator.	May–June
	SC	AG McMaster announced the arrest of an alleged online child predator.	March–April
	SC	AG McMaster announced the arrest of an alleged online child predator.	January–February
	SD	AG Larry Long announced the sentencing of a child pornographer.	March–April
	TX	AG Greg Abbott announced the indictment of three online child predators.	November–December
	TX	AG Abbott announced the indictment of an alleged online child predator.	September–October
	TX	AG Abbott announced the sentencing of a child pornographer.	July–August
	TX	AG Abbott announced the guilty plea of an online child predator.	May–June
	TX	AG Abbott announced the indictment of an alleged child pornographer.	March–April
	VA	AG Bob McDonnell announced the conviction of a child pornographer.	September–October
	VA	AG McDonnell announced a child pornography arrest.	May–June
	UT	AG Mark Shurtleff announced the arrest of two alleged online child predators.	November–December
	UT	AG Shurtleff filed charges against an alleged Internet predator.	January–February
Other *(5 cases)*	CT	AG Richard Blumenthal launched an investigation of Myspace.com for allegedly allowing minors easy access to pornography and other inappropriate material.	January–February
	FL	In a consent judgment reached with AG Charlie Crist, a man agreed to pay a $20,000 penalty for unlawfully soliciting Internet donations for victims of Hurricane Katrina.	March–April
	KY	AG's Greg Stumbo's agents seized shipments of illegal Internet drugs, including nearly $89,000 worth of Hydrocodone.	November–December
	KY	AG Stumbo's agents seized more than $580,000 in drugs sold over the Internet, including anabolic steroids and ingredients to make steroids.	September–October
	MA	AG Tom Reilly sued three Internet gun dealers for selling stun guns, which are outlawed in Massachusetts.	May–June

Endnotes

1 Federal Trade Commission, "Consumer Fraud and Identity Theft Complaint Data," January-December 2007, p. 4, available at http://www.consumer.gov/sentinel/pubs/top10fraud2007.pdf.

2 Cyber Security Industry Alliance, "Digital Confidence Survey," Spring 2006, available at http://www.csialliance.org/publications/publications/surveys_and_polls/dci_survey_May2006/.

3 Ibid.

4 Federal Trade Commission, "Internet Auctions: A Guide for Buyers and Sellers," March 2006, available at http://www.ftc.gov/bcp/conline/pubs/online/auctions.pdf.

5 For a discussion of the "elephants and mice" of the Internet, see Peter P. Swire, "The Internet and the Future of Consumer Protection" (Center for American Progress, 2006) available at http://www.americanprogress.org/kf/swire_consumer_protection_report.pdf.

6 F-Secure, "IT Security Threat Summary for H2 2007," available at http://www.f-secure.com/2007/2/.

7 Consumer Reports, "2007 State of the Net," September 2007, available at http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/state-of-the-net/0709_state_net.htm.

8 Ferris Research, The Cost of Spam, 2007.

9 See the Federal Trade Commission at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

10 See remarks of Federal Trade Commission Chairman Timothy Muris at the Aspen Summit, August 19, 2003, available at http://www.ftc.gov/speeches/muris/030819aspen.shtm.

11 See Lance James, "Phorensics: Counter-Intelligence Against the Quickest Adversary," January 2008, available at http://antispywarecoalition.org/events/jan2008/james.pdf.

12 The commission's Onguard Online website, available at http://onguardonline.gov/index.html, offers useful tips to consumers and details of the FTC's work against cyber fraud.

13 For example, the FTC only has the ability to receive civil penalties from malefactors in limited cases, such as spam. See the FTC's testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, April 8, 2008, available at http://www.ftc.gov/os/testimony/P034101reauth.pdf.

14 See Center for Democracy and Technology, "Spyware Enforcement," September 2007, available at http://www.cdt.org/privacy/spyware/20060626spyware-enforcement.php.

15 Consumer Reports, "2007 State of the Net," September 2007, available at http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/state-of-the-net/0709_state_net.htm.

16 Anti-spyware technology is often cited as another major reason. See Testimony of Ari Schwartz, Deputy Director of the Center for Democracy and Technology, before the Senate Committee on Commerce, Science, and Transportation, Subcommittee on Interstate Commerce, Trade and Tourism on "Reauthorization of the Federal Trade Commission," September 12, 2007, available at http://www.cdt.org/privacy/20070912schwartz-testimony.pdf.

17 NAAG and the National Center for Justice and the Rule of Law at the University of Mississippi Law School have a regular bimonthly "Cybercrime Newsletter" supported by the Bureau of Justice Assistance (Grant No 2006-DD-VX-0032). The index for the newsletter can be found at http://www.naag.org/publications_cybercrime.php.

18 For further discussion of preemption and other related issues, see Reece Rushing, Ari Schwartz, and Paula Bruening, "Protecting Consumers Online: Key Issues in Preventing Internet Privacy Intrusions, Fraud and Abuse," July 24, 2006, available at http://www.cdt.org/privacy/20060724consumer.pdf and http://www.americanprogress.org/kf/online_consumer_protection.pdf.

19 See NAAG's website at http://www.naag.org/about_naag.php.

20 The chart on page 9 lists 2005 data instead of 2006 data for three states: Mississippi, New Jersey, and North Dakota. Mississippi and New Jersey did not provide 2006 data and are thus not counted as part of the 31 states that submitted ranked lists for 2006. North Dakota's 2006 top 10 list did not include an Internet-related category, and thus our chart provides 2005 data. North Dakota is counted as part of the 31 states that submitted ranked lists for 2006.

21 See the Consumer Sentinel website at http://www.consumer.gov/sentinel/contribs.htm.

About the Authors

Reece Rushing is director of regulatory and information policy at the Center for American Progress.

Ari Schwartz is vice president and chief operating officer at the Center for Democracy and Technology.

Alissa Cooper is chief computer scientist at the Center for Democracy and Technology.

Acknowledgments

Karly Schledwitz and **Maeve Miccio** of the Center for American Progress and **Ethan Phelps-Goodman** of the Center for Democracy and Technology provided essential research for this report. This report would not be possible without their contributions. In addition, **Jim Dempsey**, vice president for public policy at the Center for Democracy and Technology, provided valuable editorial input in preparing the report.

ABOUT THE CENTER FOR AMERICAN PROGRESS

The Center for American Progress is a nonpartisan research and educational institute dedicated to promoting a strong, just, and free America that ensures opportunity for all. We believe that Americans are bound together by a common commitment to these values and we aspire to ensure that our national policies reflect these values. We work to find progressive and pragmatic solutions to significant domestic and international problems and develop policy proposals that foster a government that is "of the people, by the people, and for the people."

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

The Center for Democracy and Technology works to promote democratic values and constitutional liberties in the digital age. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

Center for Democracy and Technology
1634 Eye Street NW #1100
Washington, DC 20006
Tel: 202.637.9800 • Fax: 202.637.0968
www.cdt.org

Center for American Progress
1333 H Street, NW, 10th Floor
Washington, DC 20005
Tel: 202.682.1611 • Fax: 202.682.1867
www.americanprogress.org