November 20, 2001

Secretary
Federal Trade Commission
Room 159
600 Pennsylvania Ave., NW
Washington, DC 20580

Re: GLB Act Notice Workshop – Comment, P014814

Please include the attached preliminary survey results, entitled 2002 Best Privacy Practices Survey Preliminary Report, as a comment on the questions addressed at the above mentioned Public Workshop on Privacy Notices to be held December 4, 2001 in Washington DC.

Sincerely yours,

Walter F. Kitchenman
(by email)
wkitchen@tampabay.rr.com
(813) 248 – 0769

attachment:
2002 Best Privacy Practices Preliminary Report

2002 Best Privacy Practices Survey: Preliminary Report

The following preliminary results are based on surveys received through the first half of November 2001. The survey was jointly sponsored by Bankers Systems, Inc. (BSI), BankersOnline (BOL), and Information Security Programs (ISP).

Surveys were received online through the Web sites of BSI's Compliance Headquarters and BankersOnline's financial services portal. The 2002 Best Privacy Practices Survey will be conducted throughout the entire month of November and the first week of December in order to capture the responses of those attending the Eight Agency Workshop on Privacy Disclosures held December 4, 2001.

This preliminary report provides a snap shot of 146 different institutions' responses. Report results are broken up into five sections that cover and describe:

1. Survey Participants
2. Basic Privacy Policies
3. Disclosures
4. Customer Contact Management
5. Regulatory Examinations: Status & Perceptions

The final survey results will include many more institutions, be described in greater detail, and responses will be broken out and analyzed by institution type and asset size. In addition to the sections included in this preliminary report, the final report will also include a description and analysis of:

- Technology platforms used to gather non-public customer information today and in the future.
- Reported IT spending on the major components involved in managing privacy and privacy notices
- The major privacy related projects being undertaken by institutions.
- The average number of privacy notices sent out by each different type and size of institution.

For information about the final 2002 Best Privacy Practices Survey, please contact:

walterkitchenman@informationsecurityprograms.com
(813) 248 - 0769

Survey Participants

There are 146 individual institutions the responses for whom are included in this preliminary report. Nearly 80% of these survey participants identified the type and size of institution they represented. In terms of institution type and size, the preliminary respondents are reasonably representative of financial institutions subject to Gramm-Leach-Bliley (GLB) regulations governing the sharing of non-public information and the disclosure of institutional practices. In terms of internal organization, 36% of respondents (the most typical approach) delegate privacy issues under GLB to a Compliance Officer or Compliance Department.

Types Of Institutions Participating

Survey respondents identifying their type of institution have the following characteristics:

- Nearly half are state-chartered banks
- About 27% are national banks
- About 7% are savings & loans or thrifts
- Just over 4% are credit unions
- Almost 3.5% are insurance companies
- About 2.6% are securities firms or brokerages
- About 6% are finance companies and other financial services institutions

Exhibit 1

Preliminary Survey Respondents by Institution Type

Institution Type	#	% Answering Survey	% Answering Question
(Not Answered)	29	19.86	N/a
National Bank	32	21.92	27.35
State-chartered Bank	57	39.04	48.72
Credit Union	5	3.42	4.27
Savings & Loan or Thrift	8	5.48	6.84
Finance Company	1	0.68	0.85
Insurance Company	4	2.74	3.42
Securities Firm, Broker or Investment Bank	3	2.05	2.56
Other	7	4.79	5.98
Total Responses	146	100	80.12

Asset Size of Institutions Participating

More than 80% of the preliminary respondents have total assets of less than $1 Billion. This reflects the large number of state-chartered, community banks answering the survey.

About 40% have assets less than $250,000,000. About 8% of the preliminary respondents have assets greater than $3 Billion, and only one institution the preliminary results for which have been calculated to-date, had assets greater than $25 Billion.

In the final survey report, results for Top Ten institutions in terms of asset size will be broken out if possible. The preliminary respondents, however, are not significantly different in size than the institutions typically covered by GLB.

Exhibit 2

Preliminary Survey Results by Institution Size

Asset Size	#	% Answering Survey	% Answering Question
(Not Answered)	31	21.23	N/a
Less than $250,000,000	46	31.51	40.00
$250,000,000 to $500,000,000	25	17.12	21.74
$500,000,000 to $1 Billion	23	15.75	20.00
$1 Billion to $3 Billion	11	7.53	9.57
$3 Billion to $10 Billion	3	2.05	2.61
$10 Billion to $25 Billion	6	4.11	5.22
More than $25 Billion	1	0.68	0.87
Total Responses	146	100	78.77

Organization of Privacy Functions of Participating Institutions

More than 84% of the 146 respondents to-date explained how customer privacy related issues (including GLB-related responsibilities) are handled organizationally within their institutions. Over 50% of the respondents reported that more than one department handles privacy matters. No standard approach emerged. The major findings summarized in Exhibit 3 show that:

- Privacy related issues to date are largely viewed as compliance issues and handled by the compliance department at 36% of institutions.

- IT Departments are not very involved to-date, especially as privacy under GLB is largely concerned with the initial disclosures (only 4% of responding institutions involve their IT Departments).

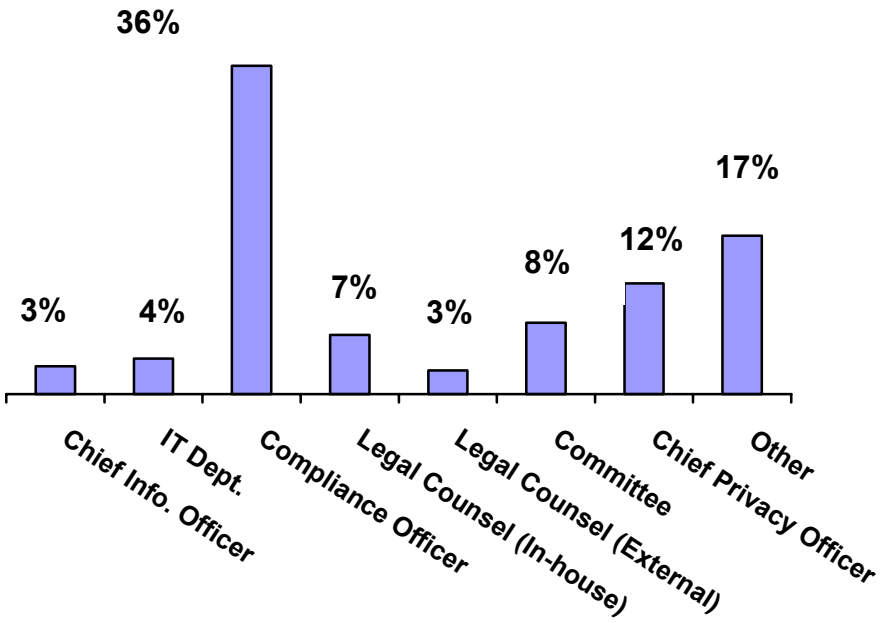
- The Chief Information Officer is involved at only about 3% of institutions.

These finding may also indicate that over 40% of the respondents – and the typical institution subject to GLB, may not have all of the possible functional areas described in the graph below, e.g., a Chief Information Officer, or separate IT Department Head. The initial generation of the initial privacy disclosure may not be as technology oriented as subsequent privacy steps that are likely to gain in importance over-time, such as the

ongoing creation and management of a privacy database.

Exhibit 3

Internal Organization of Privacy Functions (Multiple Responses Possible)



Over 80% of the preliminary respondents described the ability of bank employees to protect customer information and carry out institutions' privacy policies. It is interesting to note that:

- 60.2% of responding institutions said that the caliber of employee was either no obstacle or a small obstacle.
- 31.4% described employee abilities in the area as a medium sized obstacle.
- 8.5% described the caliber of employee and staff as a major obstacle.

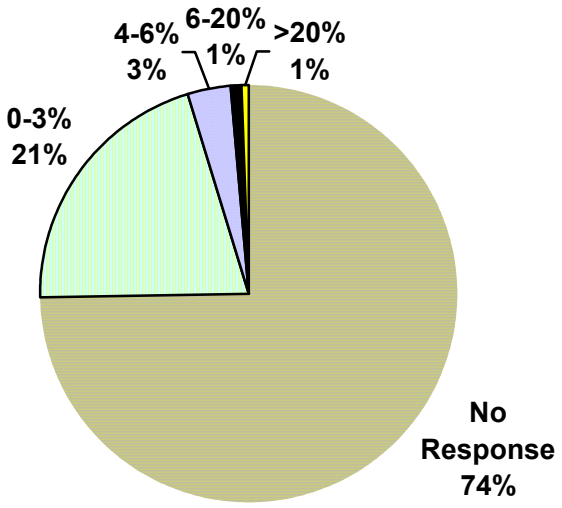
In the preliminary survey there was no significant difference between opt outs within and outside GLB exceptions. Respondents' opt out experience, at least in terms of their ability to report it at this time, is summarized in Exhibit 4.

Even with such a large number of institutions failing to respond, it is clear that not many customers have opt out of information sharing to date:

- 25% of institutions have an opt out rate of less than 6%
- 21% of institutions have an opt our rate of less than 3%
- Of institutions able or willing to provide opt out data, however, 81% reported that fewer than 3% of customers have opted out of information sharing to-date.

Exhibit 4

Customers Opting Out of Information Sharing with Affiliated Third Parties (within GLB Exceptions)



Basic Privacy Policies

Are Institutions Spending Enough on Privacy?

Preliminary results indicate that institutions may need to budget more resources for the privacy area.

Survey participants were asked whether budgetary concerns and/or the lack of a profit motive (privacy generally being considered a "cost" center in terms of P & L) had an impact on their overall ability to generate an adequate initial privacy policy and disclosure. More than 80% of the institutions in this preliminary survey responded to these questions. Over 50% of respondents to a question about the adequacy of budgets reported that a lack of budgeted resources hindered the development of adequate privacy policies, and about 47% reported that the lack of a profit motive was either a medium or major obstacle.

The following was revealed:

- 47.5% said that a lack of budget was either no obstacle or a small obstacle.
- 28% said that budget is a medium obstacle.
- About 25% reported that a lack of budget is a large or major obstacle to implementing an adequate policy.
- 53% reported that the lack of a profit motive is no obstacle or a small obstacle.
- About 18% said that a lack of a profit motive is a medium obstacle.
- About 29% stated that the lack of profit motive is a major obstacle.

How Are Privacy Policies Created?

Third party solutions available to determine privacy policies and generate compliant disclosures may be underutilized.

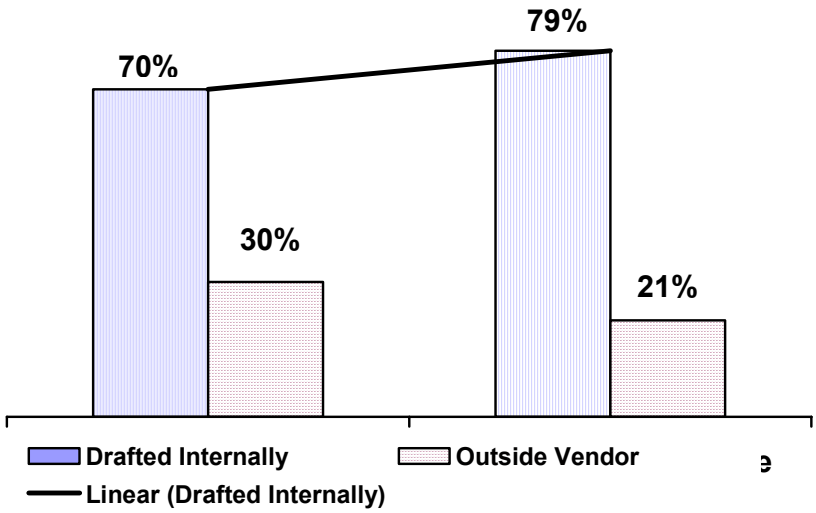
The institutions surveyed have generally developed proprietary solutions for privacy notices as opposed to taking advantage of many third party solutions that have emerged in the marketplace. Eighty-six percent of respondents say that their overall privacy policies were developed internally in 2001.

Seventy percent of respondents report developing the initial privacy disclosure in-house. And nearly 80% report that they will develop the annual privacy notice internally beginning in 2002. The lack of past, and planned, reliance on third party solutions is surprising since the typical institution participating in this preliminary survey is a smaller community based bank. Many such institutions often rely on outsourced and other third party vendors.

When asked specifically whether they were more or less likely to develop the initial and annual notices in-house over the next five years, 95% of the institutions answering the question reported they would either keep the same practices or be more likely to develop a solution in-house. With regards to the annual notice, institutions seemed a bit more flexible, since only 79% planned to develop the annual notice internally in 2002.

Exhibit 5

Respondents Using Use Internal vs. External IT Spending In Creating Privacy Notices



With Whom Is Customer Information Shared?

Responding institutions in the preliminary survey may not understand completely rules governing information sharing outside of the exceptions to the FCRA privacy rules. Nearly 80% of survey respondents were not able, or were unwilling, to describe their information sharing policies outside the exceptions.

As for information sharing within the exceptions of the FCRA, more than 86% of survey respondents could describe their practices. Data sharing is common, distributed fairly evenly among affiliated and non-affiliated parties. The following findings emerge, and are summarized in Exhibit 6:

- Only 25% of financial institutions answering this question share customer data with third party marketing firms.

- Less than one third report sharing data with a parent company or holding company (this may reflect the fact that most survey participants are community-banks)

- There is almost universal reporting of credit and other account histories to the major credit bureaus, as indicated by the fact the 86% of institutions answering this question report such sharing.

- Reflecting the important role of outsourcers (and the need for financial institutions to document service bureau compliance with privacy standards and rules), more than 70% of respondents share information with outsourcers and service bureaus.

- Nearly half the respondents share customer data with affiliates and institutions and firms with which they have joint marketing agreements (e.g., credit card issuers).

Exhibit 6

Information Sharing Within the Privacy Rule of the FCRA

NPI Is Shared (within exceptions)	#	% Answering Survey	% Answering Question
(Not Answered)	25	17.12	N/a
Non-affiliated marketing firms	30	20.55	24.79
Affiliates	59	40.41	48.76
Joint marketers	56	38.36	46.28
Parent/Holding company	39	26.71	32.23
Outsourcers/Service bureaus	85	58.22	70.25
Credit bureaus	104	71.23	85.95
Other	6	4.11	4.96
Total Responses	404	N/a	N/a

NPI Is Shared (outside exceptions)	#	% Answering Survey	% Answering Question
(Not Answered)	115	78.77	N/a
Non-affiliated marketing firms	5	3.42	16.13
Affiliates	22	15.07	70.97
Joint marketers	6	4.11	19.35
Parent/Holding company	10	6.85	32.26
Outsourcers/Service bureaus	3	2.05	9.68
Credit bureaus	7	4.79	22.58
Other	5	3.42	16.13
Total Responses	173	N/a	N/a

Information Sharing & Institutional Responses to July 1, 2001 Deadline

Mandates under the FCRA and GLB did not lead institutions to alter information sharing practices.

- Ninety-four percent of respondents to this preliminary survey did not share non-public customer information about consumers (as opposed to customers) in a manner than required them to provide an initial disclosure.

- Only 31% of the institutions that changed policies said it affected sharing with affiliates or both affiliates and non-affiliated third parties.

- Just over 60% of the institutions that changed information sharing policies prior to the July 1, 2001 deadline, believe that their changes were detrimental to their customers.

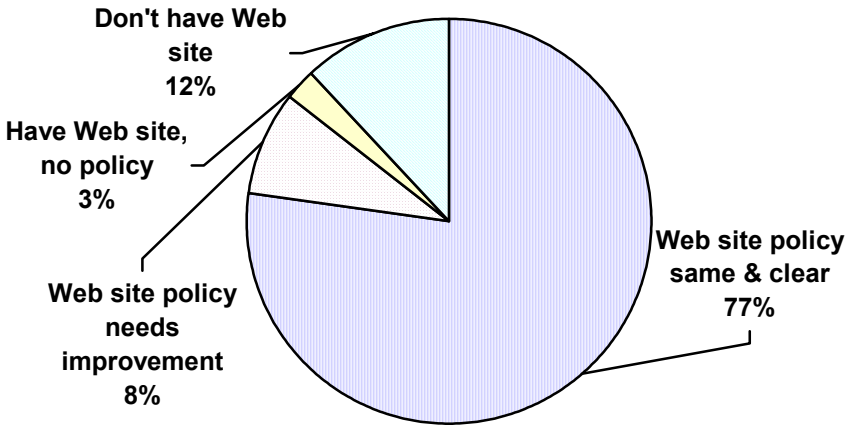
Information Sharing Policies & the Web

More than 10% of the respondents tabulated in the preliminary survey results report that they either have a Web site but do not have a privacy policy, or that their Web site policy needs improvement.

About 77% report that their Web site policy is consistent with that in force for other areas of the institution.

Exhibit 7

Privacy Policies & The Web



How Information Sharing Policies May Change

Survey participants overwhelmingly report that that they have no plans to increase the amount of information sharing before the mailing of the annual privacy notice.

This is particularly true in the case of non-affiliated third parties:

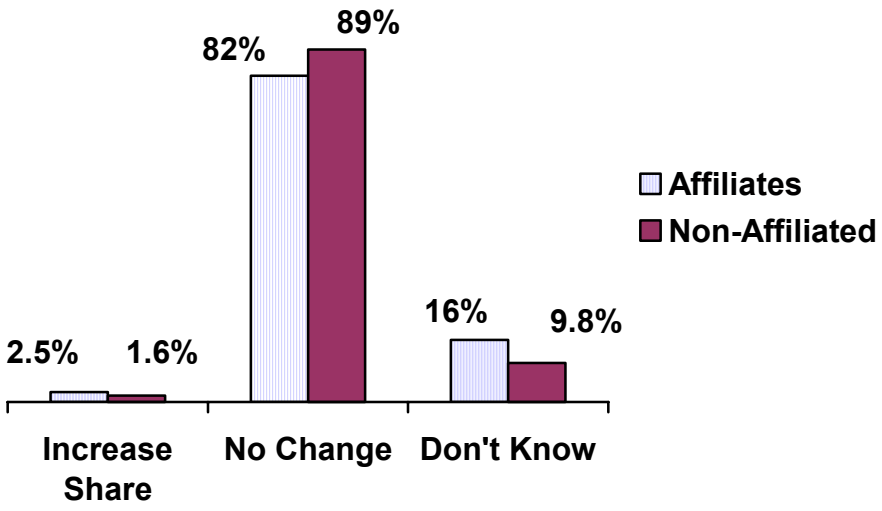
- About 89% report that there will be no change in the amount of information shared with non-affiliated parties.

- There seems to be some flexibility, however, in terms of potential sharing with affiliates only to the extent that 16% of the responding institutions state that they do no know at this time whether they will share more information or maintain existing policies.

- Just under 10% don't know whether they will increase information sharing with non-affiliated parties.

Exhibit 8

Change In Information Sharing Policies Between Initial & Annual Privacy Notice



Disclosures

About 84% of institutions participating in the survey answered the questions related to disclosures. About 70% used internal or proprietary solutions as opposed to vendors, outsourcers, or Application Service Provider (ASP) models to build the initial privacy notice. Although the number of responding institutions planning to use an ASP model to generate doubles in 2002 (for the annual disclosure), this still represents fewer than 2% of all institutions surveyed to-date. This is a surprisingly low use of external IT by the community banks which account for 40% of the survey respondents.

Only 9% of responding banks state that they will be more likely to use a third party solution for either the initial privacy notice or the annual privacy notice.

The Delivery & Timing of Privacy Disclosures

The 146 institutions the results for which have been tabulated for this preliminary report, show a wide range in the number of disclosures mailed: From fewer than 1,000 to more than 10 million. The average number of disclosures mailed by institution type and size will be presented in the final report of the 2002 Best Privacy Practices Survey available after the week of December 3, 2001.

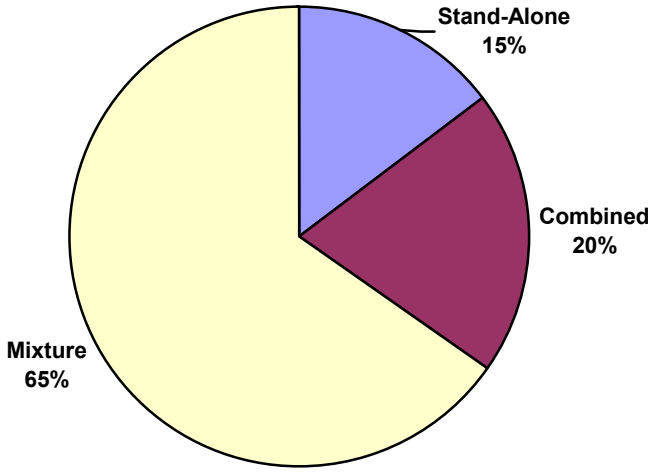
There is not much standardization in terms of either the method of delivering disclosures or the timing of the delivery of privacy notices:

- Only 20% of institutions participating in the preliminary survey results, sent the initial privacy notice out as a stand-alone mailing.
- The initial notice was sent combined with other material by 65% of respondents.
- 20% report that they sent out the privacy notice as a mixture of stand-alone and combined mailings.

These results are summarized graphically in Exhibit 9.

Exhibit 9

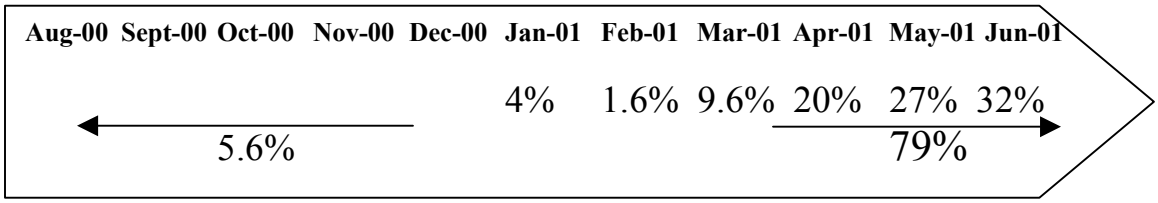
How Initial Privacy Notices Were Delivered



A standardized approach to the timing of the mailing of the initial disclosure is also lacking, as evidenced in Exhibit 10. Less than 6% of the initial disclosures were mailed in 2000, with 79% being mailed in April, May, and June of 2001, just before the July 2001 GLB deadline. About a third were mailed in June 2001.

Exhibit 10

Timing of Initial Mailing of Privacy Notices (% of Institutions Mailing)



Nearly half the respondents report that they will mail the annual privacy disclosure in 2nd Quarter 2002. But nearly 12% report that they "do not know" the timing yet, or plan "other" undisclosed timing. The remaining institutions plan their mailings of the annual privacy disclosure in a fairly even distribution throughout 2002.

Exhibit 11

Planned Timing of Annual Privacy Notices (% of Institutions Planning to Mail)

Q4-01	Q1-02	Q2-02	Q3-02	Q4-02	Don't Know	Other
4.9%	19.7%	46.7%	10.7%	6.6%	8.2%	3.3%

The Cost of Disclosures

The institutions responding to this survey spent from $10,000 to more than $25,000,000 for the creation and mailing of the initial privacy notice alone. More than half said that postage costs represented less than 25% of the total. About 19% reported that postage costs alone were 51% to 75%, while 9.6% responded that postage costs exceeded 75% of the cost of creating the privacy disclosures.

Customer Contact Management

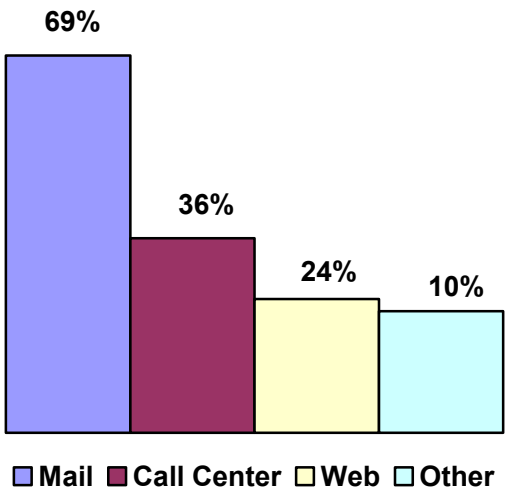
The mail is the most common channel by far through which customer opt out requests were received by the financial institutions surveyed. Mail is followed by call centers and the Web in terms of relative importance.

Managing Resources: How Are Opt Outs Received?

Sixty-nine percent of respondents to the preliminary survey did not report how they received their opt outs. As a result, only those responding to the relevant question's results are included. This suggests, however, that mail remains the overwhelming means by which customers must request opt outs. Call centers are likely the second most common means, followed by the Web (certainly for privacy policies related to the Web site).

We suspect that the dependence on mail is even greater than these results suggest. If we assume that the institutions not responding to the question use mail, than mail as a channel would be required by more than 90% of all institutions. The use of call centers, by comparison, would drop to about 11%. We also suspect that the use of call centers is more common among larger institutions with a number of affiliates with which information is shared.

Exhibit 12



Is IT Underemployed In The Management of Privacy?

As was the case with the generation of the initial privacy notice and disclosures, the management of contacts with customers for the purpose of recording customer opt out

preferences does not depend heavily on either outside vendors or ASP models and service bureaus. This is despite the fact that a lack of third party solutions for both is listed as an obstacle to implementing adequate privacy policies by half the institutions surveyed. This suggests that a lack of market awareness of third party solutions, or an inadequate number of vendor-supplied privacy solutions, may be the cause.

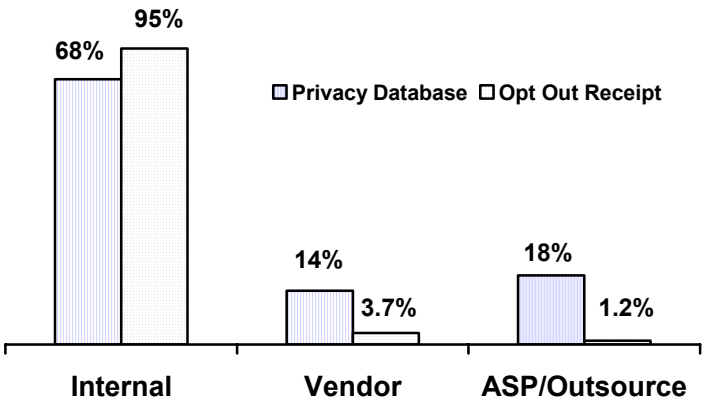
Findings show that in terms of managing opt out receipts, 95% of financial institutions responding to the survey managed customer contacts internally. In terms of developing a privacy database, or adapting existing customer information files (CIFs) to accommodate consumer opt out choices, however, vendors and outsourcers were far more active:

- 68% developed a privacy database of consumer choices internally.
- 14% report using a vendor to develop their solution in-house.
- 18% report using an ASP model or outsourcer.

We suspect that the outsourced and ASP models reported reflect the use of well known service bureaus as core processors by many smaller and community based institutions. Several outsourcers also provide target market list suppression services, and the use of list suppression technology may be reflected here as well.

Exhibit 13

How Institutions Will Process Receipts of Opt Outs & Creation of the Privacy Database



Regulatory Examinations: Status & Perceptions

About 85% of institutions responding to the survey answered questions about the regulatory practices to which they are subject.

- Over 80% report that they are currently not required to comply with state-specific privacy requirements in multiple states.
- About 34% are under the jurisdiction of multiple regulators
- About a quarter had already had their privacy related policies undergo official regulatory examinations.

Surprisingly, about half of the institutions that have undergone official regulatory examination of their privacy policies and disclosures anticipate results that are only satisfactory or need improvement. Most institutions do not consider compliance with privacy regulations to be overly burdensome.

- 50% percent of those undergoing examination anticipate excellent results.
- 42% of institutions responding to regulatory related questions state that compliance with regulations – even in terms of multiple jurisdictions (not common among our respondents) – is no obstacle whatsoever.
- 18% consider compliance to be a small obstacle.
- 40%, however, report that compliance with privacy regulations is a medium, large, or major obstacle.

Can You Prove What You Say?

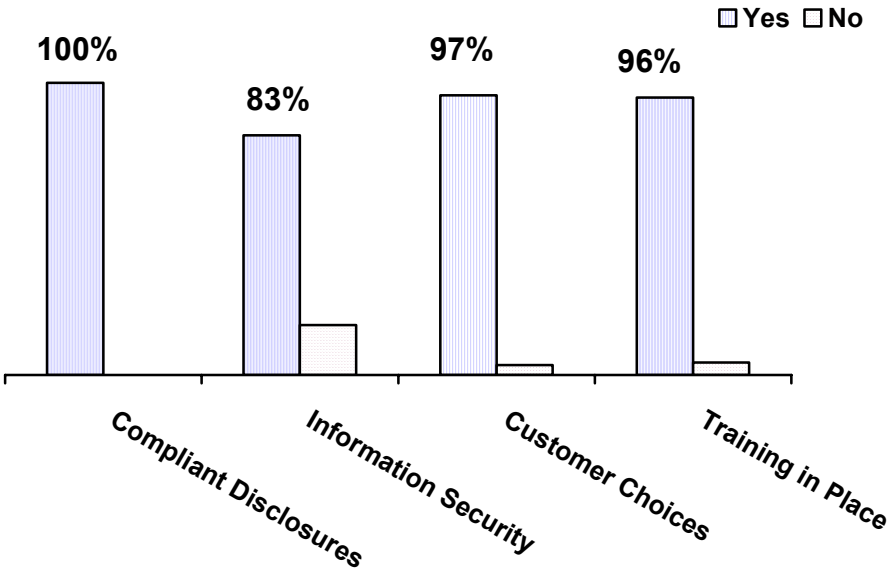
About 80% of survey respondents answered questions about whether they can actually test and document compliance in important privacy related areas such as disclosures (the clear and conspicuous privacy notice), information security programs, performing as advertised in the disclosure and honoring customer choices, and in terms of having employee-training programs in place.

With the exception of documenting the physical security of non-public customer information (only 83% say they can prove their compliance), 96% to 100% of institutions responding to these questions are overwhelmingly confident that they are compliant and can document it. One can assume that survey respondents are either overconfident or have done an excellent job.

This high confidence level contradicts to some degree the 50% of respondents that anticipate only satisfactory examination results – or worse. One suspects that the 20% of survey respondents not answering these questions, and whose responses do not appear as a result in Exhibit 14, may question their ability to document compliance.

Exhibit 14

Institutions That Can Document to Regulators Compliance In Key Areas



END of Preliminary Report of the 2002 Best Privacy Practices Survey Results

For information about a final and much more comprehensive report, please contact:

walterkitchenman@informationsecurityprograms.com
(813) 248 - 0769