



NATIONAL COUNCIL OF INVESTIGATION & SECURITY SERVICES, Inc.
THE NATIONAL VOICE OF PRIVATE INVESTIGATION & SECURITY

PO Box 755, Des Moines, IA 50303
Phone: 800-445-8408 • Fax: 515-224-1014
E-Mail Address: NCISS@ix.netcom.com

Jack H. Reed

First Vice President / Legislative Committee Member

Tel: (800)670-4772; Fax: (714)526-5836; E-Mail: jreed@irsc.com

Chairman of the Board
Michael L. Duffy
Per Mar Security Services
PO Box 4227
Davenport, Iowa 52808
(319) 326-6291
Fax: (319) 326-0225

January 31, 1997

President
Gary H. Kutty
Per Mar Security Services
PO Box 755
Des Moines, Iowa 50303
(515) 244-5660
Fax: (515) 244-3833

Mr. William W. Wiles, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Ave., NW
Washington, DC 20551

First Vice President
Jack H. Reed
I.R.S.C.
3777 N. Harbor Blvd.
Fullerton, California 92635
(714) 526-8485
Fax: (714) 526-5836

RE: Docket No. R-0953

Dear Mr. Wiles:

Second Vice President
John E. Slagowski
S & H Enterprises, Inc.
PO Box 12245
Wilmington, DE 19850
(302) 999-9911
Fax: (302) 992-9899

On behalf of the National Council of Investigation & Security Services, Inc. (NCISS), I appreciate the opportunity to respond to the above-referenced Request for Comments (RFC).

Third Vice President
John G. Talaganis
J.H.R.I., Inc.
1021 West Bastanchury Road
Suite 110
Fullerton, California 92633
(714) 526-7300
Fax: (714) 526-7458

This RFC is the result of a legislative directive from Congress to the Board to investigate whether the availability of "sensitive consumer identification information" to the public is creating "undue potential for fraud and risk of loss to insured depository institutions." NCISS member companies enjoy considerable expertise in assessing this vulnerability. Many of our companies provide investigative services to insured depository institutions and other financial institutions subject to federal regulation. We help these institutions to prevent the frauds and losses with which Congress was concerned in enacting this directive; to detect such frauds when they do occur; and to identify, bring to justice, and seek restitution from the perpetrators of such frauds.

Treasurer
W. Richard Moling
Moling & Associates
2101 S. Hamilton Rd. #201
Columbus, Ohio 43232
(614) 759-7435
Fax: (614) 759-7420

The anti-fraud work of NCISS member companies is not limited to services performed directly for financial institutions. On a much wider scale, NCISS members play a key role in preventing and investigating financial frauds carried out against American insurance companies, retail and wholesale commercial establishments, and other businesses. Our investigative work underlies the "due diligence" that American businesses

Secretary
Barbara Canario
International Research Services
PO Box 17098
Honolulu, Hawaii 96817
(808) 536-4058
Fax: (808) 533-2465

Board Members

Region I
Dan Westbrook
Tom Bucklin

Region II
Lynette Revill
Sydney Huckvale

Region III
Lloyd Davis
Martin Herman

Member-at-Large
Roy Bucklin

Region IV
Tom Davidson
Minor Dodson

Region V
Robert A. Heales
Dale Wunderlich

Region VI
John Eppick
Larry A. Webb

perform in order to minimize the risk of fraud and loss in literally millions of transactions each year, ranging from individual employment decisions to the purchase and sale of entire businesses.

Year in and year out, the American marketplace is the field of a seemingly never-ending battle against a wide range of financial frauds, ranging from simple theft to complex white-collar scams, that, taken together, constitute a multi-billion dollar drag on the economy. It is neither realistic nor appropriate to expect law enforcement authorities to shoulder the full burden of this warfare. Without the efforts of private investigative firms, as well as the security departments of thousands of individual businesses, this rising tide of fraud would seriously damage many firms, large and small, and consequently threaten a risk of loss to the institutions which finance, insure, and extend credit to these businesses.

In its directive to the Board Congress focused on the availability of "sensitive consumer identification information, including social security numbers, mothers' maiden names, prior addresses, and dates of birth." There is no question whatsoever that the availability of this information has led to abuses that have facilitated fraud and caused losses to insured depository institutions. In the RFC itself, the Board has cited an anecdotal example of "identity theft." NCISS members can provide many more anecdotal instances in which unscrupulous individuals have obtained personally identifiable information and abused it as part of a scheme to commit fraud, steal, evade taxes, or even carry out crimes of violence. For example, many identity thefts are accomplished by theft of wallets, purses, autos, and burglaries of homes and businesses. From these activities, the criminals obtain driver's licenses, checkbooks, Social Security numbers, tax returns, and credit cards. They move quickly to steal the individual's identity. Another source of identity theft occurs by postal employees stealing credit cards in bulk and reselling them on the black market, along with theft from mailbox and postal delivery personnel. Fraudulent use of Social Security numbers is another serious problem; in one case, forty-seven different individuals were discovered to be using a single Social Security number.

This is one aspect of the issue that Congress directed the Board to investigate. However, to stop there would be to give Congress an incomplete and misleading answer to the question it has posed: whether the availability of this information "create[s] undue potential for fraud and risk of loss to insured depository institutions." A complete answer to this question requires the Board to consider how the availability of this information – to law enforcement, to private

investigative services, to businesses and consumers, and to financial institutions themselves – contributes to preventing, detecting, and combating fraud and risk of loss. This is the side of the coin to which NCISS's comments will be primarily directed.

The experience of NCISS members in literally hundreds of thousands of background checks, fraud investigations, and financial due diligence projects is unequivocal. If the availability of personally identifiable information about individuals were drastically restricted, committing fraud would become more difficult. But preventing, detecting, and combating fraud would become virtually impossible. The net effect of such restrictions would be extremely harmful to the insured depository institutions, as well as to the millions of American consumers and businesses who are their depositors and customers.

Those in the front lines of the battle against financial fraud – including, but by no means limited to, NCISS members – need timely and reliable access to accurate factual information about individuals to do our job. We use this information to verify the identities and check the backgrounds of job applicants, prospective business partners, and other participants in financial transactions; to conduct due diligence investigations of financial representations and claims made; to develop leads and identify and locate witnesses in insurance fraud investigations; and for a host of other purposes that help to prevent the commission of acts of fraud, to detect them when they do occur, and to positively identify those responsible.

NCISS members' investigative activities also advance many other important social goals. We help find missing and stolen children, stop spousal abuse, and locate deadbeat parents. All these investigations require considerable use of "sensitive data" on the parties involved or those who have information as to the whereabouts of individuals and witnesses. Governments will not, and many times cannot, get involved in these cases. There must be a way to help these people and take the pressure and demands off the public sector.

Our job has been made easier and more efficient in recent years by ready access to current and updated electronic databases of personally identifiable information, including the "sensitive consumer identifying information" listed in the Congressional directive. This access lets us conduct the necessary investigations much faster and more economically than in the past. Our clients – including financial institutions and their customers and depositors – are the beneficiaries of these improvements. Conversely, if changes in law or regulation made the

compilation, maintenance, and support of these databases illegal, or made access to them for legitimate investigative purposes more difficult, time-consuming, or expensive, the defenses of financial institutions and other businesses against fraud would be weakened or compromised.

The information contained in these databases is obtained from a number of different sources. Understanding this diversity of sources underscores some of the difficulties that any highly restrictive regulations would have to surmount.

Some of the categories of information identified by congress as "sensitive consumer identification information," such as date of birth, are readily found in records systems maintained by government agencies, such as vital statistics bureaus, voter registration boards, and motor vehicle administrations. These have traditionally been viewed as public records that are available to any citizen for any lawful purpose.¹ Investigators and other legitimate users may obtain access to this data either directly from the government agency involved, or, more often, from a private sector source which compiles and makes available a number of public record data sets. Access to much of this data cannot be significantly restricted without impinging on long-standing American traditions embodied in the concept of the public record.

In other cases, businesses obtain information directly from the individual concerned. Typically, the individual voluntarily discloses the information on an application or other form completed when the individual becomes a customer, client, insured, or depositor, or at some other point in a business relationship. Often, the individual is specifically advise that the information is subject to disclosure and use for the purposes of verifying statements made in the application or for similar anti-fraud objectives. To the extent that access to this information for legitimate investigative purposes is restricted, regulatory action aimed at protecting personal privacy may end up frustrating the intentions and expectations of the individual involved. If economically beneficial transactions such as the extension of credit, issuance of insurance, or establishment of banking

¹ Congress broke with this tradition in 1994, when it enacted the Driver's Privacy Protection Act, Pub. L.103-322, Title XXX, codified at Title 18, Chapter 123, U.S. Code. While this legislation requires states to modify the traditional public record status of motor vehicle records, it includes a number of exceptions necessary to preserve access to these records for legitimate investigative purposes, specifically recognizing licensed private investigators and the security industry. See, e.g., 18 U.S.C. 2721(b)(3) (business verification to prevent fraud), (b)(4) (use in connection with judicial or administrative proceedings), (b)(6) (insurance anti-fraud activities).

relationships become more expensive or harder to conclude because the flow of personally identifiable information is restricted, the individual suffers.

The free flow of information, including personally identifiable information provided by individuals or gleaned from public records, provides enormous benefits to the banking system, to business in general, and to society as a whole. These benefits are too often taken for granted. In carrying out the study mandated by Congress, the Fed and its fellow agencies must be sure to present the whole picture, and not focus solely on the possibilities for abuse.

As noted above, NCISS is well aware of those possibilities; we see them realized every day. Too often – because even once is too often – personally identifiable information is accessed and disseminated, not for the legitimate investigative purposes outlined above, but for frivolous or malicious purposes. The availability of this data through online services and the Internet highlights this problem, but it certainly did not create it. Many of the anecdotal “horror stories” about abuse of personally identifiable information involve individuals who obtained the information over the counter at a government agency holding public records, or through fraudulent means unrelated to online access. No regulatory or statutory changes can ever entirely eliminate this vulnerability to abuse. Proposals to restrict access in ways that make such abuse less likely must be balanced against the social and economic costs of the restrictions, notably the reduced ability of financial institutions and other businesses to prevent, detect, and combat fraud.

In the view of NCISS, new laws or regulations to constrict the flow of information that is so essential to the efficient functioning of the economy are not justified at this time. Instead, NCISS urges the Fed to focus on three alternative means of discouraging abuses while retaining the benefits of the status quo: encouragement of sound business practices, vigorous enforcement of existing laws, and better education of all participants in the financial system.

There are many steps the private sector can take, on its own and in cooperation with the Fed and other agencies, to lessen the likelihood of the abuses that motivated Congress to call for this study. For example, responsible database vendors conduct their own due diligence on parties seeking to obtain online access to personally identifiable databases that contain the kind of sensitive consumer identification information specified by Congress. Vendors typically require strict verification of the claimed status (for example, as a licensed private investigator)

of would-be customers. They demand specific evidence of the legitimate purpose for which access is sought (such as pre-employment screening, fraud investigation, or collections, for instance). References may be demanded and checked; onsite inspections of the customer's premises are sometimes required. Actual use of the service can be carefully monitored to ensure that it conforms with the stated purpose for which access was sought. Failure to satisfy these criteria will result in a denial of service, or, if service has already been commenced, its immediate termination.

Furthermore, some investigative needs can be adequately satisfied through less than full access to the entire database. For example, obtaining part of an individual's Social Security number is rarely useful to someone seeking to commit a financial fraud. It may, however, be sufficient to allow a financial institution or other business to establish the approximate age or geographical origin of an individual, and thus assist in verifying whether other identifying information presented by an individual is real or bogus.

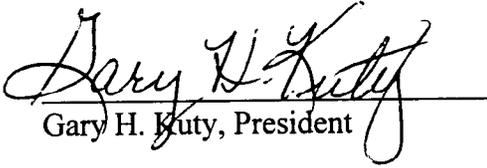
Providers of personally identifiable information who adhere to these practices significantly lessen the risk that this data will be used, not to protect the financial system against fraudulent or illegal behavior, but to commit frauds or even criminal acts. Of course none of these practices can reduce that risk to zero. NCISS believes that, beyond the encouragement of responsible business practices in this field, the federal government can most constructively attack this problem by vigorously enforcing the laws already on the books. Those laws, including the Fair Credit Reporting Act, general criminal laws such as wire and mail fraud, and the new prohibitions contained in the Driver's Privacy Protection Act, already forbid identity fraud and virtually all the other serious abuses that can be committed with the help of access to personally identifiable information. If any loopholes are identified, they should be closed. In any event, a focus on the specific fraud or other abuse that is actually carried out with the assistance of personally identifiable information is clearly preferable to a restrictive, regulatory approach that may prevent a few abuses, but also makes legitimate uses more difficult, more expensive, or even impossible.

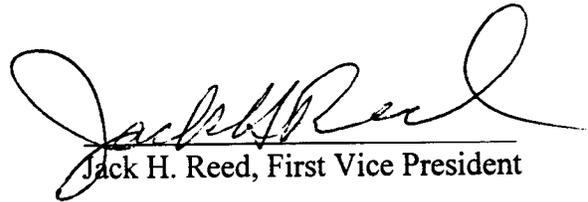
Finally, the Fed and other federal agencies have a critical role to play in educating financial institutions, their customers, and the general public about prudent use of personally identifiable information. Most members of the public, and even many who are deeply engaged in the banking, credit, retail, and other industries with the most at stake, have little understanding about how personally identifiable

information is collected, processed, and used to deliver economic benefits. The private sector can and should shoulder a significant role in dispelling this ignorance. For this reason, industry guidelines such as those promulgated by the Information Industry Association stress above all the importance of informing customers and the public about company information policies, and providing a mechanism for questions, concerns, and complaints. NCISS hopes that the Fed will work closely with the private sector in this educational effort.

NCISS appreciates this opportunity to offer its perspectives on the important issues addressed by the Request for Comments. We look forward to the opportunity to discuss these issues informally with the Fed staff as it prepares its report to Congress, and hope that you will not hesitate to contact the undersigned if we can provide further information.

Respectfully submitted,


Gary H. Kutty, President


Jack H. Reed, First Vice President

JHR:vr

Of Counsel:

Steven J. Metalitz
SMITH & METALITZ, L.L.P.
1747 Pennsylvania Ave., NW, 12th Floor
Washington, DC 20006
telephone: 202-833-4198
fax: 202-872-0546



NATIONAL COUNCIL OF INVESTIGATION & SECURITY SERVICES, Inc.
THE NATIONAL VOICE OF PRIVATE INVESTIGATION & SECURITY

PO Box 755, Des Moines, IA 50303
Phone: 800-445-8408 • Fax: 515-224-1014
E-Mail Address: NCISS@ix.netcom.com

April 15, 1997

Chairman of the Board
Michael L. Duffy
Per Mar Security Services
PO Box 4227
Davenport, Iowa 52808
(319) 326-6291
Fax: (319) 326-0225

President
Gary R. Kuty
Per Mar Security Services
PO Box 755
Des Moines, Iowa 50303
(515) 244-5660
Fax: (515) 244-3833

First Vice President
Jack H. Reed
I.R.S.C.
3777 N. Harbor Blvd.
Fullerton, California 92635
(714) 526-8485
Fax: (714) 526-5836

Second Vice President
John E. Slagowski
S & H Enterprises, Inc.
PO Box 12245
Wilmington, DE 19850
(302) 999-9911
Fax: (302) 992-9899

Third Vice President
John G. Tologenic
J.H.R.I., Inc.
1021 West Bastanchury Road
Suite 110
Fullerton, California 92633
(714) 526-7300
Fax: (714) 526-7458

Treasurer
W. Richard Molling
Molling & Associates
2101 S. Hamilton Rd. #201
Columbus, Ohio 43232
(614) 759-7435
Fax: (614) 759-7420

Secretary
Barbara Canerio
International Research Services
PO Box 17098
Honolulu, Hawaii 96817
(808) 536-4058
Fax: (808) 533-2465

Secretary, Federal Trade Commission
Room H-159
Sixth Street and Pennsylvania Ave., N.W.
Washington, DC 20580

RE: Data Base Study -- Comment, P974806

Dear Mr. Secretary:

In response to the Commission's Notice Requesting Public Comment and Announcing Public Workshop ("Notice"), issued March 4, 1997, the National Council of Investigation and Security Services, Inc. (NCISS) submits the following preliminary comments on issues relevant to the Commission's study on computerized databases containing sensitive consumer identifying information. By an accompanying separate letter, NCISS has requested the opportunity to participate in Session One of the Public Workshop on Consumer Information Privacy, scheduled for June 10, 1997.

NCISS is an association of about 1000 security and investigative companies, large and small, across the United States, serving individuals, businesses and government agencies. Our membership also includes the state associations representing all licensed private investigators and security services in 36 states. Founded in 1972, our mission focuses on training, education and advocacy on behalf of the private sector security and investigative industries. NCISS has participated actively in proceedings involving a number of state and federal privacy and information policy issues, including most recently the inquiry of the Board of Governors of the Federal Reserve System on the risks to insured depository institutions of the availability of sensitive consumer identification information.

These preliminary comments focus on the issue posed in question 1.11 of the Commission's Notice: "How do the risks of the collection, compilation, sale and use of ... information [in these databases] compare with the benefits?" Our answer, in short, is that these risks are dwarfed by the benefits.

Board Members

Region I

Region II

Region III
David Davis

Member-at-Large
Roy Bucklin

Region IV
Tom Davidson

Region V
Robert A. Heiles
Dale Wandertich

Region VI
John Eppick
Larry A. Wei

The experience of NCISS members in literally hundreds of thousands of background checks, fraud investigations, and financial "due diligence" projects is unequivocal. If the availability of personally identifiable information about individuals were drastically restricted, committing fraud would become more difficult. But preventing, detecting and combatting fraud would become virtually impossible. The net effect of such restrictions would be extremely harmful to American consumers, businesses, and the society as a whole.

NCISS member firms play a key role in preventing and investigating financial frauds carried out against American insurance companies, financial institutions, retail and wholesale commercial establishments, and other businesses. Our investigative work underlies the "due diligence" that American businesses perform in order to minimize the risk of fraud and loss in literally millions of transactions each year, ranging from individual employment decisions to the purchase and sale of entire businesses.

Year in and year out, the American marketplace is the field of a seemingly never-ending battle against a wide range of financial frauds, ranging from simple theft to complex white-collar scams, that taken together constitute a multi-billion dollar drag on the economy. It is neither realistic nor appropriate to expect law enforcement authorities to shoulder the full burden of this warfare. Without the efforts of private investigative firms, as well as the security departments of thousands of individual businesses, this rising tide of fraud would seriously damage many firms, large and small, and consequently threaten a risk of loss to the institutions which finance, insure, and extend credit to these businesses.

Those in the front lines of the battle against financial fraud -- including, but by no means limited to, NCISS members -- need timely and reliable access to accurate factual information about individuals to do our job. We use this information to verify the identities and check the backgrounds of job applicants, prospective business partners, and other participants in financial transactions; to conduct due diligence investigations of financial representations and claims made; to develop leads and identify and locate witnesses in insurance fraud investigations; and for a host of other purposes that help to prevent the commission of acts of fraud, to detect them when they do occur, and to positively identify those responsible.

NCISS member's investigative activities also advance many other important social goals. We help find missing and stolen children, stop spousal abuse, and locate deadbeat parents. All these investigations require considerable use of "sensitive data" on the parties involved or those who have information as to the whereabouts of individuals and witnesses. Governments will not, and many times cannot, get involved in these cases.

The vital services that NCISS members provide have been made easier and more efficient in recent years by ready access to current and updated electronic databases of personally identifiable

information, including the "look up services" with which the Commission's study is concerned. This access lets us conduct the necessary investigations much faster and more economically than in the past. Our clients -- businesses, government agencies, and individual consumers and citizens -- are the beneficiaries of these improvements. Conversely, if changes in law or regulation made the compilation, maintenance and support of these databases illegal, or made access to them for legitimate investigative purposes more difficult, time-consuming or expensive, the defenses of financial institutions and other businesses against fraud would be weakened or compromised.

The free flow of information, including personally identifiable information provided by individuals or gleaned from public records, provides enormous benefits to the banking system, to business in general, and to society as a whole. These benefits are too often taken for granted. In conducting its study, the Commission must be sure to present the whole picture, and not focus solely on the possibilities for abuse.

NCISS is well aware of those possibilities; we see them realized every day. Too often -- because even once is too often -- personally identifiable information is accessed and disseminated, not for the legitimate investigative purposes outlined above, but for frivolous or malicious purposes. The availability of this data through online services and the Internet highlights this problem, but it certainly did not create it. Many of the anecdotal "horror stories" about abuse of personally identifiable information involve individuals who obtained the information over the counter at a government agency holding public records, or through fraudulent means unrelated to online access. No regulatory or statutory changes can ever entirely eliminate this vulnerability to abuse. Proposals to restrict access in ways that make such abuse less likely must be balanced against the social and economic costs of the restrictions, notably the reduced ability of financial institutions and other businesses to prevent, detect and combat fraud.

In the view of NCISS, new laws or regulations to constrict the flow of information that is so essential to the efficient functioning of the economy are not justified at this time. Instead, NCISS calls the FTC's attention to three alternative means of discouraging abuses while retaining the benefits of the status quo: adoption of sound business practices; vigorous enforcement of existing laws; and better education of all participants.

There are many steps the private sector can take to lessen the likelihood of abuses. For example, responsible database vendors conduct their own due diligence on parties seeking to obtain online access to personally identifiable databases that contain sensitive consumer identification information, including verification of the customer's claimed status and of the legitimate purpose for which access is sought. References may be demanded and checked; onsite inspections of the customer's premises are sometimes required. Actual use of the service can be carefully monitored

to ensure that it conforms with the stated purpose for which access was sought. Failure to satisfy these criteria will result in a denial of service, or, if service has already been commenced, its immediate termination.

Furthermore, some investigative needs can be adequately satisfied through less than full access to the entire database. For example, obtaining part of an individual's social security number is rarely useful to someone seeking to commit a financial fraud. It may, however, be sufficient to allow a financial institution or other business to establish the approximate age or geographical origin of an individual, and thus assist in verifying whether other identifying information presented by an individual is real or bogus.

Providers of personally identifiable information who adhere to these practices significantly lessen the risk that this data will be used, not to protect consumers and businesses against fraudulent or illegal behavior, but to commit frauds or even criminal acts. NCISS is working actively with other industry participants to reach consensus on sound business practice guidelines. Although the industry is quite diverse, we are making real progress, on which we hope to report at the time of the FTC Public Workshop.

Of course, none of these practices can reduce that risk to zero. NCISS believes that, beyond the encouragement of responsible business practices in this field, the federal government can most constructively attack this problem by vigorously enforcing the laws already on the books. Those laws, including the Fair Credit Reporting Act, general criminal laws such as wire and mail fraud, and the new prohibitions contained in the Drivers' Privacy Protection Act, already forbid identity fraud and virtually all the other serious abuses that can be committed with the help of access to personally identifiable information. If any loopholes are identified, they should be closed. In any event, a focus on the specific fraud or other abuse that is actually carried out with the assistance of personally identifiable information is clearly preferable to a restrictive, regulatory approach that may prevent a few abuses, but also makes legitimate uses more difficult, more expensive, or even impossible.

Finally, the FTC and other federal agencies have a critical role to play in educating businesses, consumers, and the general public about prudent use of personally identifiable information. Most members of the public, and even many who are deeply engaged in the banking, credit, retail, and other industries with the most at stake, have little understanding about how personally identifiable information is collected, processed and used to deliver economic benefits. The private sector can and should shoulder a significant role in dispelling this ignorance.

Secretary, Federal Trade Commission
April 15, 1997
Page 5

NCISS appreciates this opportunity to comment on the issues raised in the Commission's Notice. We look forward to participating in Session One of the Commission's Public Workshop on June 10, and to supplementing these comments at a later point in these proceedings.

Respectfully submitted,

Gary H. Kutty / SSM

Gary H. Kutty, President
Per Mar Security Services
PO Box 755
Des Moines, IA 50303
(515) 244-5660
Fax: (515) 244-3833

Jack H. Reed / SSM

Jack H. Reed, First Vice President
I.R.S.C.
3777 N. Harbor Blvd.
Fullerton, CA 92635
(714) 526-8485
Fax: (714) 526-5836

Of Counsel:

Steven J. Metalitz
Smith & Metalitz, L.L.P.
1747 Pennsylvania Avenue, NW
12th Floor
Washington, DC 20006
(202) 833-4198
Fax: (202) 872-0546

SMITH & METALITZ, L.L.P.

ERIC H. SMITH
STEVEN J. METALITZ
ERIC J. SCHWARTZ

MARIA STRONG
MICHAEL N. SCHLESINGER

1747 PENNSYLVANIA AVENUE, NW
12TH FLOOR
WASHINGTON, DC 20006-4601
TELEPHONE: (202) 833-4198
FAX: (202) 872-0836
E-MAIL: smimet@tipa.com

July 30, 1997

Lisa Rosenthal, Esq.
Bureau of Consumer Protection
Federal Trade Commission
6th Street and Pennsylvania Ave., N.W.
Washington, DC 20580

RE: Data Base Study, P974806

Dear Lisa:

This follows up on our brief telephone conversation of July 22 concerning a point raised in some of the hundreds of letters submitted by members of the National Council of Investigation and Security Services (NCISS) in connection with the Public Workshop held last month in the above-referenced matter.

You noted that several of the letters referred to a legal obligation of confidentiality with respect to information obtained by private investigators in the course of their investigations. This could, of course, include information obtained through use of the individual reference databases that were one of the subjects of the public workshop. You asked for information about the source of this obligation, including whether it derives from statute, regulation, professional standards, or simply contractual agreements between private investigators and their clients. This letter is a partial answer to your question.

As I am sure you know, the legal framework for licensing and regulating private investigators varies considerably from state to state. In many, but not all, states, statutory provisions impose a duty of confidentiality on private investigators. I have attached excerpts from the relevant laws of a few states (California, Florida, and Tennessee) which set forth this requirement. For example, the California statute (Business and Professions Code Section 7539(a)) forbids the disclosure of "any information acquired" by the investigator, except to law enforcement personnel concerning a criminal offense, or "at the direction of the employer or client."

Other states have a different method of arriving at the same result. For example, in Louisiana, the Board of Private Investigators Examiners, under the jurisdiction of the state's Department of Public Safety and Corrections, has issued regulations constituting professional and occupational standards for private investigators. Rule 709, entitled "Confidentiality of

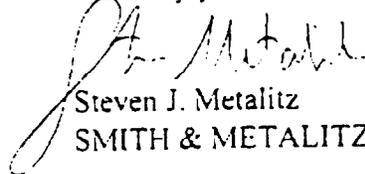
Information" (copy attached) forbids investigators from disclosing "information relating to representation of a client" without client consent or implied authorization, to prevent a crime, or to respond to a civil claim or criminal proceeding against the investigator.

Even in those states which do not impose a general confidentiality obligation on all investigators by statute or regulation, other legal doctrines frequently apply to achieve the same outcome. For instance, as I believe Bruce Hulme noted in his comments on behalf of NCISS at the public workshop, private investigators frequently act under the direction of an attorney in preparation for litigation when they consult individual reference service databases and undertake other investigative activities. Under most circumstances, such activities, and the information gained thereby, are shielded from unconsented disclosure under the attorney work product privilege.

While the foregoing is far from a comprehensive survey, it is enough to indicate that, in at least many states, private investigators are under a legal duty, derived from state statute or regulation, or from widely recognized evidentiary privilege, to avoid disclosure of the information they compile on behalf of a client, unless the client has specifically consented to the disclosure or unless some other exception (such as the prevention of a crime) applies. These duties clearly extend to information that investigators obtain through access to individual reference services, and would be seriously undermined by any generally applicable requirement that such services disclose to individual members of the public information about their customers or their customers' activities in accessing these databases. The same could be true of a generalized requirement that such services give individual members of the public unconstrained access to these databases in order to determine what information about them is contained therein.

I hope that you find this information responsive to your inquiry. If a more comprehensive survey of applicable state laws and regulations would be useful, we would be glad to undertake it. Please let me know if I can answer any questions.

Sincerely yours,



Steven J. Metalitz
SMITH & METALITZ, L.L.P.

Enclosures

cc: Jack Reed
Bruce Hulme