

Comments by the
National Insurance Crime Bureau
Concerning the
Gramm-Leach-Bliley Act Privacy Rule
16 CFR Part 313
Proposed Rule

Submitted

March 31, 2000

SUMMARY

Insurance companies and other financial institutions provide the National Insurance Crime Bureau (“NICB”) various types of data deemed “financial” under the Gramm-Leach-Bliley Act of 1999 (“the GLBA”)¹ and the Commission’s proposed rule (“the Privacy Rule”)². All such data, including information that would also be protected “health information” under privacy standards recently proposed by the Department of Health and Human Services (“HHS”)(“HHS Standards”)³, is used solely for the purpose of reporting, investigating and preventing insurance fraud.

To combat sophisticated, interstate insurance fraud rings, which inflict much of the almost \$30 billion in fraudulent claims paid by property and casualty insurers each year, it is essential that the NICB have access to several types of individually-identifiable information. NICB guards such data tightly to assure it is never used for any other purpose.

Congress has repeatedly and consistently recognized the compelling need for NICB to look for fraud indicator “links” across a broad pool of neutral insurance claims information. Most recently, in the GLBA, Congress declared that “investigating or preventing fraud” is “necessary to . . . administer” a “consumer’s insurance” policy and emphatically stated its intention *not* to restrict disclosure and use of information “to protect against or prevent actual or potential fraud.”⁴

¹ 15 U.S.C. Sec. 6801 et seq.

² “Privacy of Consumer Financial Information; Proposed Rule,” 65 Fed. Reg. 11174 (March 1, 2000)

³ “Standards for Privacy of Individually Identifiable Health Information,” 64 Fed. Reg. 59918 (Nov. 3, 1999) and 65 Fed. Reg. 427 (Jan. 5, 2000)

The Commission's proposed rule, accordingly, specifically exempts communications by, between or among insurance carriers, the NICB and law enforcement from the notice and opt-out requirements.⁵ Under the proposed Rule, insurers will need to inform customers only that they "make disclosures to other non-affiliated third parties as permitted by law."⁶ The Commission invited comment "whether such a notice would be adequate."⁷ In these responsive comments, NICB explains why the proposed customer notice is consistent with the GLBA and provides adequate notice without creating unnecessary burdens or confusion.

I. TO COMBAT SOPHISTICATED INSURANCE FRAUD RINGS, NICB MUST HAVE ACCESS TO INDIVIDUALLY-IDENTIFIABLE INFORMATION.

The National Insurance Crime Bureau ("NICB") is a not-for-profit organization, formed in 1992, dedicated to providing unique solutions to the problems of detecting, preventing and deterring insurance-related crime. NICB is supported by nearly 1,000 member property-casualty insurers and self-insured companies and works with insurers and law enforcement in identifying and prosecuting organized criminal conspiracies dealing in insurance fraud and vehicle theft.

The NICB is not a "financial institution" or an "affiliate" under the GLBA and the Privacy Rule.⁸ It is not significantly engaged in financial activities; it does not provide insurance; nor does it transact any business with "consumers" or "customers."⁹ It does, however,

⁴ GLBA, Secs. 509(7)(C) and 502(e)(3)(B)

⁵ Privacy Rule, Secs. 313.10 & 313.11(a)(2)(ii)

⁶ *Id.* Sec. 313.6(b)

⁷ 65 Fed. Reg. 11174, 11181.

⁸ *See* GLBA Sec. 509(3) & (6) and Privacy Rule Sec. 313.3(a) & (j)(1)

receive and use various types of “nonpublic personal information” from insurance carriers and other “financial institutions” with which NICB is not affiliated.¹⁰

Insurance fraud is the second most prevalent and costly form of white-collar crime. Recent studies have estimated that insurance fraud costs Americans between \$35 and \$80 billion per year. This amounts to a \$100 per year premium surcharge for the average ratepayer. More than \$30 billion is lost annually to property/casualty insurance fraud.

Organized insurance fraud rings have existed in major cities across the country for years. The most sophisticated of these gangs have formed interstate fraud rings and ingeniously avoid suspicion by filing false injury claims under different types of insurance policies with different carriers in different states.

The infrastructure of a fraud ring is a network of dishonest lawyers and doctors who stage accidents and file dishonest claims with insurance companies. In some cases, the accident is real but the injuries are bogus. Middlemen, known as cappers or runners, monitor police radios closely and swarm to the scene of a genuine accident before the police arrive. They show up with business cards of personal injury lawyers, chiropractors, and clinics and promise cash payments for anyone willing to file a false insurance claim.

In other cases, a cast of participants in a fraud ring will stage an accident in front of honest witnesses or purposefully hit a driver of a new luxury car they assume is fully insured. For example, an uninsured participant will intentionally hit a car carrying four insured participants. The insured participants will then present themselves to a participating physician who will prepare an extensive medical history. Following the “accident”, the doctor or clinic

⁹ See Privacy Rule Sec. 313.3(e)(1) & (h)

will prepare detailed medical records consisting of visits that were never made and treatments that were never performed. To obtain payment and defraud the insurer, the claimants' attorney will then submit a demand package to the insurance carrier that includes, among other things, the name of the claimant, a description of the accident, statements of honest witnesses showing clear liability, the details of medical treatment and the basis for compensating the claimant for pain and suffering. Even where the medical records are nearly an exact duplicate of ones submitted previously for a different patient, nothing in an individual demand packet will make it obvious that the claim is fraudulent. In fact, in one recently prosecuted case, the fraud ring submitted the exact same medical records for thirteen different claims with the name of the original patient "whited out" and new names written in.

The increasing sophistication of fraud rings make it difficult for insurance carriers to decide whether claims should be paid quickly or investigated more thoroughly. By looking for links across a broad pool of neutral claims information, NICB offers predictive fraud solutions. Red flags arise if the claimant has been involved "coincidentally" in too many similar incidents, has filed claims for the same accident with multiple insurance carriers or if the attorney, doctor or other professional has a history of involvement in insurance fraud. Insurance carriers can thereby detect fraudulent activity, block payment of bogus claims and, even after payments have been made, prosecute participants and obtain restitution.

Access to insurance databases is restricted to authorized users and law enforcement officials who are investigating or prosecuting an insurance fraud crime. Authorized users can only retrieve the information in the databases with controlled passwords and do not receive a

¹⁰ See *id.* Sec. 313.1

password unless they register with the database managers and sign a confidentiality and compliance agreement. All the information contained in the database is encrypted to ensure that it cannot be seen or used by unauthorized parties. In addition, database managers maintain logs of authorized users and illegal or unauthorized attempts to access the databases. They do not permit the sale or use of information contained in the database for marketing or other unauthorized purposes. To ensure compliance with confidentiality standards, the database managers regularly audit the use of their databases.

II. CONGRESS AND FEDERAL AGENCIES HAVE REPEATEDLY AND CONSISTENTLY RECOGNIZED THE COMPELLING NEED FOR NICB'S FRAUD DETECTION AND DETERRENCE EFFORTS.

Congress acted in 1994 to protect the privacy of individuals' motor vehicle-related records, but it made clear its intention that States nevertheless permit driver license and similar personal information to be used to fight fraud. The law specifically allows disclosure to "[f]or use by any insurer or insurance support organization . . . in connection with . . . anti-fraud activities."¹¹

When Congress tightened those restrictions in 1999 by barring most disclosures of driver information absent express consent by the subjects of those records, it once again specifically exempted use by an insurance support organization in connection with anti-fraud activities.¹²

Federal agencies also recently have avoided restricting NICB's access to insurance claim information. For example, in its ongoing efforts to implement privacy provisions in Title II of

¹¹ Driver Privacy Protection Act, 18 U.S.C. Sec. 2721(b)(6)

the Kassebaum-Kennedy Act,¹³ HHS implicitly recognized that NICB is not covered by the statute. The agency proposed Standards that impose no restrictions on NICB's use of otherwise protected health information.¹⁴

In the GLBA, Congress was equally careful not to restrict NICB's anti-fraud activities. Congress affirmatively declared that "investigating or preventing fraud" is "necessary to effect, administer or enforce" a "consumer's insurance" policy and emphatically stated its intention not to restrict disclosure or use of information needed "to protect against or prevent actual or potential fraud."¹⁵ In keeping with the intent and express terms of the statute, the Commission's proposed rule expressly exempts from the basic operative prohibitions and requirements of the statute, including the notice and opt-out requirements, information used for the purpose of "reporting, investigating or preventing fraud" or "to protect against or prevent actual or potential fraud"¹⁶

III. THE PROPOSED CUSTOMER NOTICE IS CONSISTENT WITH THE GLBA, PROVIDES CONSUMERS WITH ADEQUATE NOTICE AND AVOIDS UNNECESSARY BURDENS AND CONFUSION.

The Privacy Rule generally requires insurers to provide a detailed explanation to consumers and policyholders concerning the types of information they plan to disclose and the categories of affiliates and non-affiliated third parties with whom such information will be

¹² Department of Transportation and Related Agencies Appropriations Act for Fiscal Year 2000, Pub. L. No. 106-69, Sec. 350(b)

¹³ Health Information Portability and Accountability Act, 42 U.S.C. Sec. 1320d

¹⁴ 64 Fed.Reg. 59918 at 59923 & 59940-41

¹⁵ GLBA Secs. 509(7)(C) & 502(e)(1) & (3)(B)

shared.¹⁷ However, disclosures for fraud-fighting purposes are, as explained above, exempt from the operative provisions of the statute and the Commission therefore advises insurers that “[t]he requirements for initial notice . . . [and] the opt-out do not apply if you disclose . . . for . . . reporting, investigating or preventing fraud”¹⁸ The alternative, presumably, would be to require each insurance writer to list every federal state and local law enforcement agency, every insurance company, the NICB and every other insurance support organization with which it may share access to insurance claims information. That approach would make no sense. It would unduly burden insurance companies and confuse their customers.

The Commission’s proposal imposes reasonable requirements on insurers and provides adequate notice to consumers and customers. The Privacy Rule provides that privacy notices are required *only* if an insurer discloses “other than as authorized by Secs. 313.10 and 313.11.”¹⁹ Insurers who disclose information “as authorized under Secs. 313.10 and 313.11 . . . are not required to list those exceptions in the initial or annual privacy notices [Y]ou are only required to state that you make disclosures to other non-affiliated third parties as permitted by law.”²⁰

As noted above, access to insurance fraud-fighting data is tightly controlled and use is strictly limited to anti-fraud activities. NICB is already in full compliance with the Commission’s requirement that it may use “information . . . in accordance with . . . an exception

¹⁶ Privacy Rule Sec. 313.11(a)(2)(ii)

¹⁷ *Id.* Sec. 313.6

¹⁸ *Id.* Sec. 313.10

¹⁹ *Id.* Sec. 313.4(a) & (b)

²⁰ *Id.* Sec. 313.6(b)

. . . only for purposes of that exception.”²¹ The Commission also has effectively prohibited improper re-disclosure of protected information by holding the NICB to the same restrictions it has imposed on the financial institutions from which the information was initially received.²²

In addition to the privacy policies that have been implemented by carriers and the NICB, many states have adopted model privacy legislation approved by the National Association of Insurance Commissioners.²³ Individuals who are the subjects of the records already can avail themselves of a variety of safeguards, including the right to obtain copies of their records and to seek correction of any erroneous information.

CONCLUSION

The Commission correctly adheres to the GLBA by exempting the disclosure of fraud-fighting information from the notice and opt-out provisions of the Privacy Rule. The proposed customer notice serves the public interest and should be adopted in the final regulations as written.

Respectfully submitted,

Judith M. Fitzgerald
Vice President, Government & Public Affairs
NATIONAL INSURANCE CRIME BUREAU
10330 S. Roberts Rd.
Palos Hills, IL 60465-1997
(708) 430-7483

²¹ *Id.* Sec. 313.12(a)(2)

²² *Id.* Sec. 313.12(a)(1)

²³ *See, e.g.*, the Health Insurance Privacy Model Act.