

September 10, 2003

The Honorable Tommy G. Thompson  
Secretary  
U.S. Department of Health and Human Services  
Hubert H. Humphrey Building  
200 Independence Avenue, S.W.  
Washington, DC 20201

Dear Mr. Secretary:

We, the undersigned organizations, are writing to express our concern that financial institutions may have inappropriate access to protected health information (PHI). We are especially alarmed that financial institutions could use this sensitive information in data mining activities for their own purposes. We believe that this would be a violation of both the spirit and the letter of the HIPAA Privacy Rule. We are requesting that you and the Department provide strong, unequivocal affirmation of the December 2000 Preamble of the Final Rule that restricts such unauthorized disclosure of PHI.

On August 20, 2003, Katharina Kopp of the Health Privacy Project and Anna Slomovic of the Electronic Privacy Information Center met with staff of the Office for Civil Rights to discuss our concerns. We are now writing to outline these concerns in more detail.

Financial institutions have expressed strong interest in data mining information they obtain through transactions and in using this information for marketing to their existing customers, finding new customers, and evaluating credit risks. When banks process payments through the Automated Clearing House (ACH) network on behalf of health care clients, ACH transactions contain PHI when they include transmissions of the electronic remittance advice.

We urge HHS to reiterate that, under the Privacy Rule, use and disclosure of PHI must be safeguarded in the following ways:

First, PHI can be encrypted in a way that makes it accessible only to the intended recipient provider or health plan.

Alternatively, PHI can be separated from electronic funds transfers and sent to intended recipients outside the ACH network. Otherwise, if access to PHI by financial institutions is not restricted, financial institutions can use data mining techniques to obtain information about individuals. That information then can be used and disclosed without any restrictions.

We believe that the unrestricted disclosure of PHI to financial institutions is prohibited under the HIPAA Privacy Rule and that the potential for abuse of PHI by financial institutions through data mining is very high.

We understand that the American Banking Association (ABA) had several meetings with the Office for Civil Rights (OCR) asking OCR to retract or revise the clear guidance in the Preamble of the 2000 Final Rule. The Preamble states explicitly that PHI transmitted through the ACH network must be encrypted in a way that makes it inaccessible to anyone other than the receiving covered entity or the intended recipient's business associate. We request that the Department provide strong, unequivocal affirmation of this requirement, and resist efforts by financial institutions to eliminate this critical consumer privacy safeguard.

### **1. Evidence of interest in data mining of personal information by financial institutions.**

We would like to direct your attention to three recent articles (see attachments) that describe the expressed desire by financial institutions to data-mine transactional records and then to use the resulting information to assess financial risk posed by individual customers.

An article in the ABA Bankers News on March 4, 2003, "*Mining ACH Transactions*," enthusiastically declares that "most banks could hit the mother lode simply by mining their own customers' automated clearing house transactions..." This article discusses the ability of banks to obtain sufficient data from ACH transactions to create individual profiles and then to use those profiles for marketing and other activities.

An article in Bank Systems & Technology on July 28, 2003, titled "*Data Mining on Check Images OK, Says Legal Expert*," raises the issue of financial institutions data mining check image data, another type of transaction that might include sensitive information about the interaction between an individual and a health care provider.

The purpose of obtaining detailed personal information about individuals, including information about their health, is described in the August 6, 2003 article in the *Wall Street Journal*. This article discusses the use by financial institutions of medical data in credit reports and raises the issue of creditors potentially "evaluat[ing] a consumer's risk on the basis of health."

These articles show that financial institutions are very interested in obtaining access to their customers' personal information from transactions that flow through the banking system. The personal information obtained in this way may be used to deny important benefits and services, such as lines of credit or mortgages, to potential customers who pose a higher perceived risk. For example, the ABA article quotes Michael Uline of Insight Financial Marketing LLC: "...We can ... tell if they're involved in any kind of debt counseling, [and] you could use that in a protective position."

Even though data mining using ACH transactions might not be common practice today, the possibility that banks might use data mining techniques to obtain PHI and then use PHI to deny services is a major threat to patient privacy, and would clearly undermine the trust and confidence needed to ensure consumers access to health care, and full

participation in their own care. PHI must not be accessible to unintended recipients. To accomplish this, PHI must be encrypted before it flows through the ACH network and encryption must be such that only the receiving provider or health plan can have access to the PHI.

## **2. HIPAA Privacy Rule regulates ERA transactions.**

As you are aware, the HIPAA Transaction Rule adopted two payment transaction standards: The Health Care Payment and Remittance Advice (ASC X12N835) and the Health Plan Premium Payments (ASC X12N820). Both of these standards have two parts. As stated in the preamble to the December 2000 Final Rule:

*They [two parts of the transaction] are the electronic funds transfer (EFT) and the electronic remittance advice (ERA). The EFT part is optional and is the mechanism that payors use to electronically instruct one financial institution to move money from one account to another at the same or at another financial institution. The EFT includes information about the payor, the payee, the amount, the payment method, and a reassociation trace number [meeting the requirements for minimum necessary disclosure of protected health information in Sections 164.502 and 164.514]. Since the EFT is used to initiate the transfer of funds between the accounts of two organizations, typically a payor to a provider, it includes no individually identifiable health information not even the names of the patients whose claims are being paid....The ERA, on the other hand, contains specific information about the patients and the medical procedures for which the money is being paid and is used to update the accounts receivable system of the provider. This information is always needed to complete a standard Health Care Payment and Remittance Advice transaction, but is never needed for the funds transfer activity of the financial institution. The only information the two parts of this transaction have in common is the reassociation trace number. (The Standards for Privacy of Individually Identifiable Health Information; Final Rule; 45 CFR Parts 160 and 164; pages 82615 – 82616).*

***Processing ERAs is part of the health care provider's 'back-office' function, not a banking transaction, and is therefore subject to the Privacy Rule.***

The banking industry has asserted that receiving banks must have access to the ERA in order to perform banking functions such as reconciliation of amounts transferred. This assertion confuses reconciliation of banking transactions (making sure that amounts authorized by the payor are paid out by the originating bank and appropriately credited by the receiving bank) with reconciliation of the accounts receivable system that is part of a health care provider's back-office operations. Electronic remittance advice is intended to simplify health care operations and reduce health care costs by permitting claims payment to be automatically reconciled with a provider's accounts receivable.

Many payors send out ERAs directly to providers or to providers' billing companies. When a provider or its billing company receives the ERA, software captures the

information in the ERA and reconciles it with accounts receivable. This is a completely separate operation from reconciling amounts authorized for payment from one bank account and amounts credited for payment to another bank account. If a bank updates the provider's accounts receivable system with the information in the ERA, the bank is acting as a provider's "back office". This is not a banking function since it can and often is performed by entities other than financial institutions. It is important to note that if a receiving provider has any questions about a particular amount paid on a claim, the only entity that can answer the question is the payor that performed adjudication of the claim. The only function unique to financial institutions is the ability to accurately perform funds transfers from payors to providers. Therefore, any functions other than funds transfer performed by banks on behalf of payors or providers must be subject to the requirements of the Privacy Rule.

***Section 1179 definition of 'payment' does not include Electronic Remittance Advices.***

Banks have stated that all their payment activities, including reconciliation of accounts receivable systems with the information contained in the ERA fall within the definition of "payment" within Section 1179 and are, therefore, exempt. However, payments referred to in Section 1179 of the statute are clearly related to consumer payments and would not include "remittance advices" that contain PHI.

Legislative history supports this interpretation. The Security and Electronic Signature Standards; Proposed Rule; 45 CFR Part 142; (page 43244), states that:

*(Concerning this last provision [Section 1179], the conference report, in its discussion on section 1178, states: "The conferees do not intend to exclude the activities of financial institutions or their contractors from compliance with the standards adopted under this part if such activities would be subject to this part. However, conferees intend that this part does not apply to use or disclosure of information when **an individual** [emphasis added] utilizes a payment system to make a payment for, or related to, health plan premiums or health care. For example, the exchange of information between participants in a credit card system in connection with processing payment for health care would not be covered by this part. Similarly sending a checking account statement to an account holder who uses a credit or debit card to pay for health care services would not be covered by this part. **However, this part does apply if a company clears health care claims, the health care claims activities remain subject to the requirements of this part** [emphasis added].") (H.R. Rep. No. 736, 104<sup>th</sup> Cong., 2<sup>nd</sup> Sess. 268-269 (1996))"*

Clearly Congress intended that activities of financial institutions were to be excluded from the HIPAA regulations governing PHI only to the extent that financial institutions provide consumer oriented payment transactions. However, activities by financial institutions would not be exempt from HIPAA regulations when these activities involve the processing of non-consumer oriented payments such as a remittance advice containing PHI. Therefore, the payments referred to in Section 1179 are clearly related to

consumer payments and would not include “remittance advices” that contain PHI. We urge the Secretary to affirm this position.

***Processing of ERAs is not part of payment transaction and therefore not exempt.***

The preamble of the 2000 Final Rule states that the information contained in the ERA is not part of the EFT and can be separated from the EFT:

*...information to effect funds transfer is transmitted in a part of the transaction separable from the part containing any individually identifiable health information. We note that a covered entity may conduct the electronic funds transfer portion of the two payment standard transactions [Health Care Payment and Remittance Advice (835) and Health Plan Premium Payments (820)] with a financial institution without restriction, because it contains no protected health information. The protected health information contained in the electronic remittance advice or the premium payment enrollee data portions of the transaction is not necessary either to conduct the funds transfer or to forward the transaction. Therefore, a covered entity may not disclose the protected health information to a financial institution for these purposes [electronic funds transfer]...” (p. 82496 , section 164.501) and further, “Because a financial institution does not require the remittance advice or premium data parts to conduct funds transfers, disclosure of those parts by a covered entity to it (absent a business associate arrangement to use the information to conduct other activities) would be a violation of this rule.” (p. 82616)*

The preamble of the 2000 Final Rule clearly lays out that the electronic remittance advice is subject to restriction and not exempt under Section 1179 [42 U.S.C. 1320d-8], which exempts the processing of payments from regulations of the HIPAA Privacy Rule. Specifically, financial institutions are not automatically exempt from the HIPAA Privacy Rule when processing remittance advices as part of payment transactions that contain PHI. We urge the Secretary to re- affirm the law here.

**3. Electronic Remittance Advice needs to be encrypted according to the Preamble of the 2000 Final Rule.**

The 2000 Preamble recognizes that a funds transfer transaction that contains the ERA has two intended recipients.

*“[The Standard] ... allows both parts to be transmitted together, even though the intended recipients of the two parts are different (the financial institution and the provider” (p. 82616). The Preamble continues: “...A covered entity may transmit the portions of the transactions containing protected health information through a financial institution if the protected health information is **encrypted** [emphasis added] so it can be read only by the intended recipient. In such cases, no protected health information is disclosed and the financial institution is acting solely as a conduit for the individually identifiable data (p. 82496).*

A receiving financial institution cannot be an intended recipient of the ERA. Therefore, PHI must be sent in a way that does not permit receiving financial institutions to have access to the PHI contained in the ERA. ACH transactions are now encrypted in a way that protects them from external access, but allows receiving financial institutions to decrypt and further process them. *We urge HHS to affirm that PHI contained in banking transactions must be encrypted in a way that does not permit receiving financial institutions to decrypt the PHI.*

#### **4. Disclosure of PHI for funds processing is not consistent with minimum necessary standard.**

We agree with the preamble of the 2000 Final Rule “... *that disclosure of diagnostic and specific treatment information to financial institutions for many banking and funds processing purposes may not be consistent with the minimum necessary requirements of this final rule.*” (p. 82616).

We believe that ERAs should not be accessible to financial institutions unless PHI is encrypted. If PHI is stripped from the funds processing transaction, only the minimum necessary data is transmitted in accordance with the HIPAA Privacy Rule. If PHI is encrypted in a way that only the intended covered entity can decrypt, a financial institution would be acting solely as a conduit and would not be violating the minimum necessary standard.

#### **5. Business Associate Agreements must be required for originating financial institutions if financial institutions engage in activities other than funds processing for covered entities. Transfer of PHI through the ACH network must still be encrypted in a way that makes it accessible only to intended recipient covered entities.**

We further agree with the position expressed by the Department in the Preamble of the 2000 Final Rule that “*financial institutions are business associates if they receive protected health information when they engage in activities other than funds processing for covered entities.*” (p. 82616).

We believe that the Secretary should clarify that business associate agreements must contain a clause that explicitly prohibits the use of any PHI for data mining purposes or any other activities not authorized by the covered entity. In addition, the business associate contract must stipulate that the bank that processes EFTs and ERAs on behalf of a covered entity cannot send unencrypted PHI contained in the ERA through the ACH network. We note that the preamble of the 2000 Final Rule raised concerns that the ACH system is an ‘open network’ similar to the internet ‘*because transmissions flow unpredictably through and become available to member institutions who are not party to any business associate agreements...*’ (p. 82616).

*We are asking the Secretary to affirm that the originating bank can process EFTs and ERAs (under a business associate agreement) without encrypting the PHI contained in the ERAs only as long as it does not send this data through the ACH network.*

## **6. HIPAA Privacy Rule and the Security Rule affirm need to encrypt PHI.**

In addition to the HIPAA Privacy Rule requirements discussed above, the Rule also requires that “*a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.*” (§§ 164.530(c)(1)) This requirement is further amplified in the HIPAA Security Rule, which requires entities that transmit PHI to “*implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network*” (§§ 164.312). The Security Rule makes encryption an ‘addressable standard’ and given that the risk of disclosure of PHI to a financial institution in the ACH network is high, encryption or an equivalent alternative security measure should be applied. *We urge HHS to affirm that effective encryption or an equivalent security safeguard is required.*

## **7. Gramm-Leach-Bliley Act does not put limitations on data mining by banks, and thus the potential for abuse is high.**

We are particularly concerned about access by financial institutions to PHI as part of ERA transactions because the Gramm-Leach-Bliley Act (GLB) only imposes legal duties on financial institutions with regard to personal information of their customers (transmitting payor or receiving provider). GLB does not limit what banks can do with personal information of individuals who are not their customers. The individuals whose PHI is included in the ERA part of the transaction may or may not have any relationship with the bank involved.

Under GLB a financial institution may store information about individuals that may or may not have any relationship with the bank and use that information for its own business interests. For example, a financial institution may use the PHI contained in the ERAs, if not encrypted, as a risk assessment tool in evaluating a loan application. Moreover, under GLB, financial institutions are explicitly permitted to share their customers’ information with their affiliates. For example, a bank can share PHI with an affiliated insurance company or affiliated mortgage lender. In cases where individuals are current or future customers of the financial institution, GLB would not prevent the sharing of PHI between banks and their affiliates, such as mortgage lenders or credit card issuers. As a result, potential for abuse is enormous. *The Secretary should issue guidance that affirms the HIPAA Privacy Rule’s intent that banks cannot access PHI sent through the ACH network.*

## **8. Current legislative discussions on Fair Credit Reporting Act recognizes potential abuse of medical privacy by financial institutions.**

Current legislation pending before Congress seeking to amend the Fair Credit Reporting Act would keep sensitive medical information out of credit reports (HR 2622). The legislation would prohibit affiliates of a corporation from sharing medical information without a customer’s consent and it would require the use of some type of code for any health information that does manage to slip into a credit report. There has been broad support for *this section* of the bill (although the bill as a whole is opposed by several

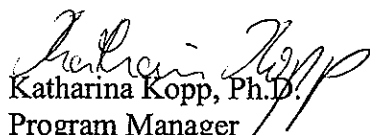
consumer organizations), underscoring the public concern with inappropriate use of medical information by financial institutions. The HIPAA Privacy Rule and the Preamble of the 2000 Final Rule are consistent with Congress' expressed desire to keep medical information out of inappropriate reach of financial institutions.

One of the stated reasons for the promulgation of the Privacy and Security Rules was to increase public confidence - and thus full participation - in the health care system. We believe that achieving this goal requires assurances to the public that PHI will not be misappropriated or misused. When financial institutions are used to forward remittance advices as well as payments, and if remittance advices have not been encrypted, sensitive, confidential patient information is disclosed to financial institutions. Unless the PHI contained in ACH transactions is encrypted, banks have both motive and opportunity to use this PHI for data mining and to deny products and services to (potential) customers based on this analysis. Moreover, since most people know very little about the operation of the banking system, the practice would be almost impossible for individuals to detect. We believe that the way to build public confidence in the privacy and security of PHI is through unequivocal guidance that ensures that financial institutions are acting solely as conduits because the PHI contained in the ERA is encrypted.

The HIPAA Privacy Rule clearly states that covered entities cannot disclose PHI to financial institutions unless the PHI is encrypted in a way that makes it accessible only to intended recipient covered entities or their business associates. We urge HHS not to reverse the Privacy Rule and to reject any requests by financial institutions to weaken it. We are available to work with the Department on this matter, and look forward to your response.

Please contact Katharina Kopp (202-721 5614, [kkopp@healthprivacy.org](mailto:kkopp@healthprivacy.org)) or Janlori Goldman (202-721 5632, [jgoldman@healthprivacy.org](mailto:jgoldman@healthprivacy.org)) at the Health Privacy Project (1120 19<sup>th</sup> Street, NW, 8<sup>th</sup> Floor, Washington, DC 20036) or Anna Slomovic (202- 483 1140, #118, [slomovic@epic.org](mailto:slomovic@epic.org)) at the Electronic Privacy Information Center (1718 Connecticut Ave. NW, Suite 200, Washington, DC 20009).

Sincerely,

  
Katharina Kopp, Ph.D.  
Program Manager  
Health Privacy Project



AFFIRM - Alliance for Fairness In Reforms to Medicaid  
Patricia C. Thompson, Executive Director

American Association of People with Disabilities  
Helena Berger, COO

American Federation of State, County and Municipal Employees – AFSCME  
Barbara Coufal, AFSCME Legislation

American Mental Health Counselors Association  
Beth Powell, Director, Public Policy and Professional Issues

American Psychiatric Association  
Nancy Trenti, Associate Director, Division of Government Affairs

Anxiety Disorders Association of America  
Michelle Alonso, Director, Communications & Membership

Bazelon Center for Mental Health Law  
Chris Koyanagi, Policy Director

Center for Democracy and Technology  
Paula Bruening, Staff Counsel

Center on Disability and Health  
Bob Griss, Director

Citizen Action of New York  
E. Joyce Gould, RN, MSN, Health Care Project Director

Communications Workers of America  
Rosie Torres, CWA Representative- Legislation

Consumer Federation of America  
Brad Scriber

Consumers Union  
Janell Mayo Duncan, Legislative and Regulatory Counsel

Electronic Privacy Information Center  
Anna Slomovic, Senior Fellow

Family Violence Prevention Fund  
Anna Marjavi, Program Specialist

Hadassah  
Shelley Klein

International Association of Machinists and Aerospace Workers  
Hasan Solomon, Esq., Legislative Rep.

Narcolepsy Network  
Florence McArdle, Vice President and Acting President

National Association of Social Workers  
David Dempsey, Manager, Government Relations and Political Action

National Consumers League  
Linda Golodner, President

National Coordinating Committee for Multiemployer Plans  
Randy G. DeFrehn, Executive Director

National Multiple Sclerosis Society  
Susan Sanabria, Vice President, Advocacy Programs Department

National Organization for Rare Disorders (NORD)  
Abbey S. Meyers, President

Privacy Rights Clearinghouse  
Tena Friery, Research Director

Society for Women's Health Research  
Melissa Kaplan, Government Relations Coordinator

U.S. Public Interest Research Group  
Edmund Mierzwinski, Consumer Program Director

The International Union, United Automobile, Aerospace and Agricultural Implement  
Workers of America (UAW), Mary Rouleau, Deputy Legislative Director

United Church of Christ  
Pat Conover, M. Div., Ph. D., Legislative Director

USAction  
Helen Gonzales, Policy Director

Enclosures

cc:

Doug Badger, White House, Senior Advisor to the President on Health Policy

Richard Campanelli, Director, HHS Office for Civil Rights  
Susan McAndrew, HHS Office for Civil Rights

Sen. Judd Gregg, Chairman, Senate Committee on Health, Education, Labor and Pensions  
Sen. Edward Kennedy, Ranking Member, Senate Committee on Health, Education, Labor and Pensions

Sen. Jon Kyl, Chairman, Senate Committee on Finance  
Sen. John D. Rockefeller, IV, Ranking Member, Senate Committee on Finance

Sen. Richard Shelby, Chairman, Senate Committee on Banking, Housing and Urban Affairs  
Sen. Paul. S. Sarbanes, Ranking Member, Senate Committee on Banking, Housing and Urban Affairs

Sen. Robert F. Bennett, Chairman, Senate Subcommittee on Financial Institutions  
Sen. Tim Johnson, Ranking Member, Senate Subcommittee on Financial Institutions

Sen. Larry Craig, Chairman, Senate Special Committee on Aging  
Sen. John Breaux, Ranking Member, Senate Special Committee on Aging

Rep. Michael G. Oxley, Chairman, House Committee on Financial Services  
Rep. Barney Frank, Ranking Member, House Committee on Financial Services

Rep. Spencer Bachus, Chairman, House Subcommittee on Financial Institutions and Consumer Credit  
Rep. Bernard Sanders, Ranking Member, House Subcommittee on Financial Institutions and Consumer Credit

Rep. Nancy L. Johnson, Chairman, Subcommittee on Health  
Rep. Pete Stark, Ranking Member, Subcommittee on Health

## **Mining ACH Transactions**

### **A Mother Lode of Solid Sales Leads**

*By Pat Dalton*

If solid sales leads are worth their weight in gold, most banks could hit the mother lode simply by mining their own customers' automated clearing house transactions, says Michael Uline, senior partner at Insight Financial Marketing LLC, Farmington, Minn.

"[Our company] looks for sales opportunities using ACH and debit card transaction information. We basically rake the transactions and run them against our knowledge base that we have built for a lengthy period of time," says Uline, who will teach at the ABA School of Bank Marketing and Management, May 30-June 6, at the University of Colorado in Boulder, Colo. (For more information, call 1-800-BANKERS.)

Insight Financial Marketing ([www.infimark.com](http://www.infimark.com)) has spent a lot of time building up its extensive proprietary knowledge base by deciphering arcane ACH coding and then determining what that information represents and from where the transaction is being transmitted.

"Then when we see a transaction at your bank that matches our knowledge base we can say ahhh! -- this is a mortgage or this is a mutual fund investment with this bank or this investment house," he says.

The company generates databases for client banks every quarter that, in essence, tell them what their customers are doing -- and with whom.

"We can literally tell you where they're employed, what their annual income is, whether they have mortgages, investments and installment loans [at other institutions], and if they are Internet users," Uline says. "The granularity is incredible. We can even tell you if they're involved in any kind of debt counseling, [and] you could use that in a protective position."

The information is also very user-friendly, especially for community banks. "We make certain that the data we have can be populated in an MCIF [marketing customer information file] -- if the bank has one -- or directly into their CIF if they use that, or in their Excel spreadsheets or wherever," he says.

But what about the ever-present P-word -- as in privacy?

"The process falls under Regulation P, where we cannot share the information or results with anyone except the [source] bank," Uline says. "We return all results back to the banks. We know that 99.9 percent of all bank privacy statements state that they will look at transaction information only to better represent the bank in marketing products to customers. That's what we're doing for the bank.

"I want to emphasize that we have no relationships with any marketing companies -- and I want to underline 'no' 300 times -- nor do we promote any marketing campaigns except directly for the client bank," he adds. "We're very discreet and security is very high. Banks don't want their customers to think that they're invading their privacy, and we work very closely with banks on that."

Uline says that banks can use the information gleaned from the analysis of ACH transactions in many ways:

- Home equity loan campaigns. "What we can immediately identify for the banks is the customers who have mortgage or home equity relationships with other banks," he says. "So now instead of recirculating their own mortgage base and trying to refinance mortgages they currently hold, they can bring in new mortgage and home equity relationships."

- Large deposit sales opportunities. At one community bank, Uline's company quickly identified a customer who had made an ACH deposit of more than \$1 million. "We were able to immediately notify the bank that 'Bob Johnson just made a large deposit electronically,'" he says. "This was a payroll deposit and it was his bonus check." Although a \$1 million-plus deposit is rare, Uline says, flagging any large deposit enables the bank to congratulate the customer, especially if it is a bonus check, and, more important, offer him opportunities to invest in CDs and money market funds, talk to the institution's investment brokers or perhaps use its private banking services.

- Internet banking. Uline points out that while community banks are spending a lot of money on Internet banking, few are realizing more than a modest return on it. But ACH transaction analysis can help to target-market the service. "One of the things we can see are all the bank's customers who are doing Internet transactions -- either purchasing products on the Internet or banking on the Internet elsewhere," he says. "What we do is go to the bank and say, 'Here are all of your customers who are currently on the Internet, but are not doing online banking with you.' Now, instead of marketing Internet banking to every single customer, you focus only on those who are comfortable with Internet banking and are doing transactions on it."

- Automatic utility payments. "This is one of the programs we've really promoted ... because it's an easy implementation, it's somewhat nonthreatening and it locks that customer in for a longer relationship," Uline says.

- Insurance prospecting. Analyzing ACH data identifies bank customers who have insurance policies or annuities with other providers. Uline calls ACH transaction analysis "incredibly powerful." It enables you to build "a better understanding of your customer makeup and how they use the bank, as well as if they are investing their money elsewhere."

## Can you see it?

**BANKSYSTEMS  
& TECHNOLOGY**

**[www.banktech.com](http://www.banktech.com)**

Critical Technology  
Management Information

### Data Mining on Check Images OK, Says Legal Expert

By Ivan Schneider, BankTech

Jul 28, 2003 (2:11 PM)

URL: <http://www.banktech.com/story/BSTeNews/BNK20030728S0003>

Banks that create and maintain check image archives on behalf of their customers have control over a potentially valuable source of marketing information. But tapping into that information requires careful consideration of state laws and national laws such as the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA). According to W. John Funk, Esq., shareholder and director at Gallagher, Callahan & Gartrell, a Concord, N.H.-based law firm, the overlapping provisions of GLBA and FCRA do not necessarily prohibit certain types of data mining activity.

For instance, suppose a customer writes a check to an insurance company or a stockbroker, helpfully including a detailed notation on the memo line. "We believe it's perfectly permissible to use that type of information to market products and services to your customer," said Funk. "The Gramm-Leach-Bliley Act does not restrict how you can use your own customer information that you develop as a result of your relationship with your customer, provided that you inform your customers of your practices in your privacy notice."

Furthermore, information about the counter-party to a check transaction may fall outside the scope of GLBA provisions. "Under Gramm-Leach-Bliley, your legal duty is to your customers," said Funk. "To the extent that the check images contain information about persons who are not your customers, you don't have any legal duty under the Gramm-Leach-Bliley scheme as to how you treat that information."

FCRA also contains relevant exemptions. "It exempts the sharing of 'transactional or experience information' from the definition of what is a consumer credit report," said Funk. "It basically says that that type of [transaction or experience] information can be shared without the limits that are imposed by the FCRA."

"The information from checks fits within this exclusion," added Funk.

Nevertheless, banks would have to state its practices within its privacy notices to consumers, and provide opt-out provisions if any information were to be shared outside of the bank. "You want to make certain that your privacy statement is broad enough to encompass data mining that you might include in the future," said Funk.

There's also the open question of whether bank regulators would take kindly to data mining on check image data. "We haven't gotten an opinion yet," said Funk. "I'd expect that it might involve somewhat of a long deliberative process in dealing with the regulators in this practice area."

In the meantime, it might be safest to wait. "Privacy isn't an area that you mess with at all," said Frank

Mukri, spokesman for the Office of the Comptroller of the Currency. "All the regulators - the Fed, the OCC, the FDIC - are really going to crack down if you cross that line."

Funk spoke at a Webcast sponsored by Orbograph, a Billerica, Mass.-based check recognition technology provider that works with AFS, Jack Henry and Wausau Financial.



**CMP**

United Business Media

[Copyright © 2003 CMP Media LLC // Privacy Statement](#)

**Want to increase your ROI? \$\$\$**

PERSONAL FINANCE

# Medical Data Can Show Up in Credit Reports

*Congress Moves to Limit Access to Information; Some Rules Already Exist*

By SEAN MARCINIAK

It isn't supposed to be there, but medical data can show up in your credit report. It means your banker, after seeing that credit-card payment you made to the local psychiatrist, might decide he would rather not give you a loan.

Congress is attempting to come to the rescue. Last month, the House Committee on Financial Services resoundingly approved a bill that would keep sensitive medical information out of credit reports. The Fair and Accurate Credit Transactions Act, slated for a vote in the full House this fall, would prohibit affiliates of a corporation from sharing medical information without a customer's consent. The act also seeks to require the use of some type of code for any health information that does manage to slip into a credit report.

The medical-privacy issue is one of many that have arisen as part of a larger debate in Congress over renewing sections of the Fair Credit Reporting Act, which sets national standards on the content of credit reports and regulates how companies can buy, sell and share that information. Certain sections are set to expire Jan. 1. In addition to the medical-privacy section of the bill, lawmakers are seeking to add provisions intended to curb identity theft and credit-reporting errors.

It's unclear how many creditors, if any, evaluate a consumer's risk on the basis of health. In 1993, a government report referred to a case of a banker, operating out of the Midwest, who used medical data to determine which of his customers suffered from disease, then called due the mortgages of those customers who had cancer. However, the government's source of this anecdote, C. Peter Waegemann, executive director of the Boston-based Medical Records Institute, acknowledged recently that he heard the story from a source he trusts but was never able to verify it. "I tried many times for many organizations to retrace it, but I never found the banker," he said.

Still, the potential exists for databases to flow into one another. "I think it's part of a broader concern of access to information and who controls information," said Raphael Bostic, an economist at the University of Southern California. "So I think in that context it makes sense that people should be mindful of this issue."

As a practical matter, however, Mr. Bostic said that due to limited time and resources, most bankers make credit decisions with a quick look at a credit score.

Others, however, see the potential for abuse and don't like it. "Fifteen years ago, it was virtually unheard of for insurers to use consumer credit histories to determine insurance premiums or whether to cancel or renew an insurance policy," said Joy Pritts, an assistant research professor at Georgetown University, during a congressional hearing in June. "Now, it is becoming increasingly commonplace. Who can say whether med-

ical information for credit decisions will develop along the same lines?"

Numerous studies on credit, including one by the Federal Reserve, have found that a substantial amount of health data could be inferred from entries on a credit report. Specifically, financial institutions and other creditors list the names of medical providers to whom their customers owed money. Credit experts said a banker could infer a customer had a particular illness if the credit report showed the customer had paid money to a certain cancer center, AIDS clinic, neonatal clinic, psychiatrist or alcohol abuse center.

Another way financial institutions come across medical data stems from the loosely regulated data-sharing that goes on between affiliates of the same company. Whereas credit bureaus and creditors must exchange data under strict rules that largely prohibit the trafficking of medical information, affiliates can share records of their own transactions and experiences with customers without restriction. That can include medical information. A life insurer, for example, which asks for medical information in its application, legally could share what it discovers with an affiliated bank. A credit-card issuer with a complete history of a customer's payments could show it to an affiliated mortgage lender.

Some big financial institutions have their own rules against this, however. For example, both Citigroup Inc. and Bank of America Corp., which each have several units that deal with consumers, have policies that allow affiliates to share medical information only when it is used to process transactions and maintain ac-

counts. They say consumers can "opt out" of the sharing agreement. "We use it strictly to process a specific transaction, such as an insurance policy approval," said Bank of America spokeswoman Eloise Hale.

The bill now under consideration in the House expressly prohibits bankers from using medical information to make credit decisions and would subject affiliates to the same standards as credit bureaus when it comes to sharing information. In addition, every information exchange for credit purposes would require a customer's written consent.

The bill, however, has one big hole, some critics and even some supporters concede.

It lurks in the definition of "medical information." Susan Henrichsen, a supervising deputy attorney general in California, said the Fair Credit Reporting Act narrowly defines medical information as records obtained from sources like doctors and hospitals. That means any information originating from a life insurer wouldn't be subject to any new rules about sharing medical information with nonaffiliates.

Under the new bill, a life insurer would still need only disclose to consumers that it might share information with a nonaffiliate and then offer them an opportunity to opt out, a clause that usually is buried in fine print, experts said. "There's just not good coverage here, not the kind you would want if you care about medical-information privacy," Ms. Henrichsen said.

Rep. Barney Frank (D., Mass.), ranking member in the Committee on Financial Services, said the issue could be reviewed on the House floor.

## College Gain

By K. Dou

Parents are getting more money for assistance. More states are adding programs to what some are overwhelmed by. Others contend it is more aggressive. One thing is clear: Parents are gaining at 20% of new 529 plans. Chased through the market. Those who when 64% of parents according to a survey by the Fair Credit Reporting Act Corp., a Boston, Mass., research firm, said that 80% of new 529 plans are through brokers. Named after the code that governs the plan, all 50 states and the District of Columbia have some type of 529 plan. Money must be used for education. Expenses could be as high as \$10,000 a year. New York state moving to allow 529 funds to be used for five years, the first time. Do-it-yourself fund firm TIAA-CREF in favor of the plan. Includes a low-cost group. Broker-sold plan. Management fee. Financial advisor. New York state to capture a large broker.

