PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Testimony of
Consumer Federation of America
Consumers Union
Electronic Privacy Information Center (EPIC)
Privacy Rights Clearinghouse
Privacy Times
U.S. Public Interest Research Group (U.S. PIRG)
World Privacy Forum
Consumer Action

By

Evan Hendricks, Editor/Publisher
Privacy Times
www.privacytimes.com

Before The House Committee On Financial Services
Subcommittee On Financial Institutions & Consumer Credit
November 9, 2005

Mr. Chairman, thank you for the opportunity to testify before the Subcommittee. My name is Evan Hendricks, Editor & Publisher of *Privacy Times*, a Washington newsletter since 1981. For the past 25 years, I have studied, reported on and published on a wide range of privacy issues, including credit, medical, employment, Internet, communications and government records. I have authored books about privacy and the Freedom of Information Act. I have served as an expert witness in litigation, and as an expert consultant for government agencies and corporations.

I am the author of the book, "Credit Scores and Credit Reports: How The System Really Works, What You Can Do." (2nd Edition, Privacy Times 2005)

Don't Pass HR 3997

HR 3997 does not adequately advance protection for the security and privacy consumer data. In fact, it could weaken existing protections. Worse, its sweeping preemption of State law would interfere with, and in some cases

potentially prevent, States from continuing their vital role of responding to these fast-evolving problems with effective and well-targeted solutions. Therefore, we urge the subcommittee not to move this bill in its current form. No action would be preferable to HR 3997.

Privacy

In the United States and around the world, "Privacy" is defined broadly. As the U.S. Supreme Court has recognized, "To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[1] If consumers' information is not adequately protected by the entities that maintain it, then consumers unreasonably lose control over their information. The same is true if consumers can not gain access to information about them, or are not allowed to correct errors that are later sold to third parties. The same is true if outsiders are able to use consumers' data for impermissible purposes. These are but a few of the subject addressed by long-standing principles of Fair Information Practices (FIPs), 1973 report of the [HEW] Secretary's Advisory Committee On Automated Personal Data Systems[2], the 1977 report of the U.S. Privacy Protection Study Commission (PPSC)[3], and the 1980 principles set forth by the Organization of Economic Cooperation and Development (OECD)[4], which were signed by U.S. Government and some 24 other nations.

Accordingly, the subject matters of HR 3997 are inextricably linked to the fundamental privacy rights of Americans.

www.PrivacyTimes.com P.O. Box 302 Cabin John, MD 20818
(301) 229 7002 (301) 229 8011 [fax] evan@privacytimes.com

[1] U.S. Dept. Of Justice v. Reporters Committee, 489 U.S. 749 (1989)
[2] PPSC Report, Pg. 15.
[3] The five FIP principles of the HEW task force were: (1) there must be no personal data recordkeeping systems whose very existence is secret; (2) there must be a way for an individual to find out what information about him is in a record and how it is used; (3) there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent; (4) there must be a way for an individual to correct or amend a record of identifiable information about him; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.
[4] (1) Collection Limitation; (2) Data Quality; (3) Purpose Specification; (4) Use Limitation; (5) Security Safeguards; (6) Openness; (7) Participation; (8) Accountability

Year of The Data Security Breach: Americans' Demand Protection Grows

The San Diego-based Privacy Rights Clearinghouse has counted 80 data breaches since February, involving the personal information of more than 50 million people. The unfortunate string of highly publicized data-security breaches justifiably has heightened Americans' concerns, as well as their demands for better privacy protections, as reflected by a series of recent opinion polls.

For example, a September 2005 CBS News and *The New York Times* showed that 89 percent were concerned about the theft of their Social Security number, credit card numbers and other identity numbers, while seven percent were "not too concerned," three percent were not "concerned at all," and one percent "did not know."

"At a time when views about so many national issues divide along party lines, this issue transcends partisanship or ideology," CBS News reported. "Democrats, Republicans, liberals and conservatives – all express disapproval of companies collecting personal information, are concerned about privacy rights and identity theft, and call for the government to do more to regulate such activity. In fact, 68% of conservatives (and 69% of liberals) would like to see the government do more to address personal privacy issues."

Moreover, 83% of respondents said that it was "mostly a bad thing" that companies collect their personal information, including what they buy, their credit histories, and income information.

A Few Good Items

Whenever possible, I prefer to emphasize the positive. HR 3997's proposed provision of free monitoring to victims of data-security breaches is an important step forward, though I think one-year would be a preferable term to six months. I also favor making notices distinctive, with "exclusive color and titling," thereby increasing the chances that a notice will be noticed, and not discarded as "junk mail."

Disappointing Start

However, given the mounting evidence of glaring privacy problems, and the growing demand among Americans for stronger safeguards, HR 3997 is a most disappointing "first pass" at the issues raised by "The Year of the Data Security Breach."

Because of its shortcomings, it would appear to do more weaken, rather than strengthen, Americans' right to privacy. If HR 3997 represents as far as the subcommittee can go, then I would urge the subcommittee to refrain from further action. I am confident that, like me, millions of Americans would like to see a strong bill that would substantially broader their rights to improve control over their personal information. However, one now has to wonder at this point if that is a realistic prospect.

Here are a few problems with HR 3997:

- It fails to expand important privacy rights, like extending FCRA-styled rights to information brokers, or creation of a right to freeze disclosure of one's own credit report

- It would appear to dramatically weaken California's original breach-notification standard, which has proven very effective in ensuring that individuals (including non-Californians) were notified that they might be at risk.

- It would appear to weaken the straightforward data security standards of Gramm-Leach-Bliley by overlaying vague and potentially confusing standards that allow for broad exceptions and "safe harbors."

- Worst of all, it would appear to broadly preempt State action in this area at a time when States consistently have responded to these fast-evolving problems with effective solutions. If interpreted in a draconian fashion, it would conceivably preempt some 12 State laws allowing consumers to "freeze" disclosure of their credit reports – without even mentioning the term "freeze" in the bill.

Chicken Little

These concerns are not without foundation. While leading companies like ING Direct and E-Loan support new privacy rights for consumers, other financial services companies do not favor stronger privacy. In opposing them, they are known to predict hardship, or otherwise dissemble. In 2001, for example, when North Dakota voters became the first Americans to have the chance to vote for a statewide ballot initiative on an opt-in financial privacy law, the financial industry spent over $150,000 in advertising money attempting to convince the voters that the measure would result in economic doom for North Dakota. But North Dakotans didn't buy it: The privacy initiative won 72% to 27%.

In California, when faced with a similar statewide ballot initiative, the financial services industry reached a compromise with State Sen. Jackie Speier and her colleagues, resulting in enactment of SB 1. The bill created an "opt-in" standard for selling of bank data to third parties, and an "opt-out" standard for affiliate sharing. The ballot initiative was withdrawn.

Spokesmen for major banks said they could live with the bill. Jon Ross, a Citigroup lobbyist, told *The American Banker* on August 25, 2003, "We were part of this and are pleased with the work done—it's a good fair result for everyone."

In an August 14, 2003 press release, the California Bankers Association (CBA), said, "We believe that, with the latest changes, this proposal qualifies as both reasonable and workable in many, but not all, aspects… We want to be clear that CBA would much prefer a national standard to a patchwork of state or local privacy laws."

However, the financial services industry was successful in litigating against affiliate sharing, as a federal court said these important State-based protections for consumer privacy were preempted by federal law.

It is also worth noting that the credit reporting industry generally opposed the FACT Act proposal to entitle Americans to one free credit report per year. Congress wisely disregarded this opposition. Moreover, it appears that the increased attention to credit reports and to identity theft has proven to be a marketing boon for the credit reporting agencies, which appear to be expanding the sale of high-priced credit-monitoring services. In other words, by doing what was right for Americans, Congress appeared to help the credit reporting industry.

Accordingly, industry protestations over stronger privacy rights should be viewed with skepticism.

HR 3997

Notice. The California notice requirement is straightforward and workable: a notice requirement where there has been an unauthorized acquisition of an individual's name along with a Social Security Number, a driver's license number, or an account number and corresponding access code.

But under HR 3997, it appears that notice would only have to be if the company decides that the information obtained "is reasonably likely to be misused in a manner causing substantial harm or inconvenience against consumers" to commit either "identity theft" or to "make fraudulent transactions on financial accounts."

As my colleague Ed Mierzwinski, of U.S. PIRG, testified recently, "The best way to convince companies to keep data secure in the first place is to require notices whenever they do not. The fact that the company doesn't yet know whether or how the information will be misused should not be enough to excuse notice. Companies that lose information should not get to decide whether consumers need to take further action to protect their privacy. Consumers should be warned. As to the industry's so-called "sky is falling" argument that consumers might face too many notices, we are unaware that the California law has resulted in any frivolous notices. Below we also describe ways to make the notices clear."

Defining Substantial Harm Or Inconvenience. The bill would define "substantial harm or inconvenience" as a material financial loss to or civil or criminal penalties imposed on the consumer, or the need for the consumer to expend significant time and effort to *correct erroneous information* relating to the consumer . . . but does not include other harm or inconvenience that is not substantial, including changing a financial account number or closing a financial account.

This is a cramped view of the kinds of harms or inconveniences that consumers experience following security breaches. Apart from direct financial loss or correcting erroneous data, victims of security breaches typically must endure other inconveniences, such as more closely monitoring their monthly statements, or ordering credit reports, regularly monitoring their credit and other time-consuming chores. Perhaps the greatest harm or inconvenience is enduring the uncertainty of whether your information has fallen into the hands of criminals. If the data includes Social Security number (SSN), then the uncertainty can last a lifetime. If it includes credit card numbers or other identifiers, such information can sometimes be "leveraged" into obtaining SSNs. Either way, the consumer is at the short end of the stick.

In its enforcement action against BJ's Wholesale Club, the Federal Trade Commission further articulated why inconvenience arising from inadequate security was damaging to consumers.

> After the fraud was discovered, banks cancelled and re-issued thousands of credit and debit cards, *and consumers experienced inconvenience, worry, and time loss dealing with the affected cards*. Since then, banks and credit unions have filed lawsuits against BJ's and pursued bank procedures seeking the return millions of dollars in fraudulent purchases and operating expenses. According to BJ's SEC filings, as of May 2005, the amount of outstanding claims was approximately $13 million.

> The FTC alleges that BJ's failure to secure customers' sensitive information *was an unfair practice because it caused substantial injury that was not reasonably avoidable by consumers* and not outweighed by offsetting benefits to consumers or competition. [Emphasis added][5]

I strongly urge the subcommittee to hear directly from victims of data security breaches in reconsidering its definition of these terms.

Weakening Data Safeguards Standards?

Section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLB) mandated that financial institutions develop and implement administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. Subsequent guidelines require each institution to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities.[6] The GLB data security standards are intended in part to ensure that individuals maintain reasonable control over their personal data, as the standards recognize that failing to secure such valuable information greatly heightens the possibility it will fall into the wrong hands, thereby spiraling further out of the control of the individual.

But HR 3997 would appear to weaken these standards by shifting the focus away from protecting the data to maintenance of "reasonable policies and procedures," or as the bill states, "affirmative obligation to implement, and a continuing obligation to maintain, reasonable policies and procedures to protect the security and confidentiality of sensitive financial personal information...that is reasonably likely to result in substantial harm or inconvenience."

Unfortunately, even in cases where consumers were harmed or inconvenienced by bad security or faulty privacy practices, some financial institutions, in seeking to avoid responsibility, have insisted that their procedures were reasonable.[7]

---

[5] In the Matter of BJ's Wholesale Club, Inc., FTC File No. 042 3160; Also see, "BJ'S Wholesale Club Settles FTC Charges: Agency Says Lax Security Compromised Thousands of Credit and Debit Cards," FTC Press Release, June 16, 2005; http://www.ftc.gov/opa/2005/06/bjswholesale.htm

[6] "Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information," Office of the Comptroller of the Currency, OCC 2001-35, Attachment A; http://www.occ.treas.gov/ftp/bulletin/2001-35a.pdf

[7] In one pending FCRA case in which the plaintiff sued after a credit card company repeatedly "verified" disputed information that was false, the designated expert for the credit card company argued that plaintiff's lawsuit "confuse[d] (1) the requirement that the furnisher ***report accurately the results*** of its investigation (of the disputed data) to the credit reporting agency with (2) the requirement that the furnisher ***report accurately the information*** investigated." The argument put bad form ahead of substance.

People First

When fashioning privacy legislation, it is vital that the priority be increasing Americans' control over their personal information. Proposals that tilt toward the prerogatives of large organizations that wish to traffic in individuals' data will not solve the problem and ultimately require that Congress revisit these issues in the near future.

In addition, if we are to have national privacy standards, they must reflect a high level of protection. If uniformity is a priority, then Congress must get out in front of issues and, working with the States, establish high levels of privacy protection through national law.

As a practical matter, this has proven difficult. For instance, when I appeared before a House Financial Services subcommittee in April 2003, when the California breach notification was the only State law of its kind, I recommended that Congress adopt it as a national standard.[8] In hindsight, it might have been easier for Congress to do so at that time.

Instead, however, the States have continued to take the lead in protecting consumer privacy. I believe that at least 20 States have security-breach notice laws, and some 10 States have credit freeze laws. These laws are clearly having a national impact, benefiting millions of Americans – even where no State law exists.

Thus, if Congress wants to act in these or other areas of privacy, it is essential that it enact a strong federal measure.

Unfortunately, HR 3997 fails to accomplish this. Instead, it appears it would weaken standards and possibly make it easier for some large organizations to avoid their responsibility to protect the privacy of consumers' highly sensitive financial data.

Data Security Concerns Persist

In the October 25 issue of *Privacy Times*, we ran a story based on a former employee's allegations that data security was neglected at NOVA Information Systems, the nation's third largest credit card processor, much as it was at CardSystems Solution, which was hit by a breach and was the topic of a subcommittee hearing this July. As the story notes, NOVA vehemently denied the

[8] Fighting Fraud: Improving Information Security," House Financial Services Subcommittee on Financial Institutions & Consumer Credit, and Oversight, April 3, 2003; http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=202

charges and insisted it was and will continue to be compliant with Visa security standards. At this point, it is basically a "She said, it said" story. (Attached)

What struck me, however, was that it did not seem that any outside entity representing the public's interest would more closely examine NOVA to determine if *any* of the detailed allegations were valid. NOVA processes records on millions of consumers. I urge the subcommittee to look into this to determine if these allegations warrant Congressional oversight or examination by federal or State regulators.

In October, it appeared that a Trans Unions, a major credit reporting agency, suffered significant data breaches. A Midwestern bank was hit in the Spring, but it received little publicity.

Conclusions & Recommendations

If the subcommittee is unable to report out legislation that establishes high levels of protection for consumer privacy, then I see no justifiable reason for moving a bill. The State laws already are having a national impact. In privacy, once the bar is set high, there is a "race to the top." Any federal law that would lower the bar would be counterproductive. Preempting States from continuing their exemplary work would be potentially disastrous.

Here are some of my preliminary recommendations from my April 2003 testimony:

Expand & Improve Consumer Access to Their Own Financial Data. The FCRA already gives consumers the right to see their credit report and caps how much CRAs can charge. This approach needs to be upgraded to the electronic age and expanded to the entire realm of financial data, especially since large financial institutions are maintaining their profiles on customers, perhaps beyond the reach of the FCRA. In the meantime, Congress could pass a Resolution or Sense of the Congress that as a matter of principle and fundamental fairness, Americans should have a right to see and correct information about themselves. In light of ChoicePoint and Lexis Nexis, these rights should extend to information brokers as well.

Impose A General Duty To Notify Consumers After Data Leakages. The new California law provides a model starting point.

State Attorney General Enforcement. The State AGs consistently have brought important enforcement actions in a number of areas to ensure consumers' privacy rights. Failure to include State AG enforcement would leave a glaring hole and prove to be a major mistake.

Curtail The Use of SSNs as a personal identifier. Rep. Clay Shaw and others have introduced legislative proposals to this effect.

Create An Independent Privacy Office Most people don't realize that Sen. Sam Ervin originally proposed such an office along with the Privacy Act. Now, every advanced nation has one except the United States.

Create A Private Right Action So People Can Enforce Their Own Rights. Privacy affects virtually all 200 million adult Americans. In this electronic age, they must have rights, and those rights must be enforceable. You will never be able to build a bureaucracy big enough to adequately enforce Americans' right to privacy, nor should you want to. Thus, the private right of action is essential.

I'd be happy to answer any questions.

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Volume 25 Number 20 October 25, 2005

CAPITAL INSIGHTS: Telecommunications firms, nonprofit organizations and educators are asking the U.S. Court of Appeals in Washington to overturn rules that would extend federal surveillance capability to the Internet. Authored by the Federal Communications Commission, the rules would extend the mandates of the Communications Assistance for Law Enforcement Act (CALEA). The 1994 law required telephone companies to rewire their networks and switches to make them "wiretap-friendly" to law enforcers. "The FCC simply does not have the statutory authority to extend the 1994 law for the telephone system to the 21st century Internet," said Marc Rotenberg, director of the Electronic Privacy Information Center. . . . Sen. Maria Cantwell (D-WA) has introduced a bill in the Senate Judiciary Committee that asks the Justice Department to investigate a link between ID theft and Methamphetamine use. "The meth epidemic is creating a wave of identity theft," she says. Meth addicts – already adept at stealing personal information from mailboxes to finance drug habits – now are hacking PCs to steal information, Bob Gauthier, a detective in the Edmonton, Alberta, Police Service's meth project team, told USA Today.

MAJOR STORIES IN THIS ISSUE

NOVA, U.S. BANCORP DENY CHARGES OF FORMER DATABASE ADMINISTRATOR

A former employee of NOVA Information Systems, the nation's third largest credit card processor, has charged that the company has neglected rudimentary data security safeguards, leaving vulnerable more than one billion credit card numbers and millions of business owners' Social Security numbers. In response to *Privacy Times* inquiries, the company denied the charges

and expressed confidence that a Labor Dept. administrative law judge would dismiss her whistleblower-retaliation complaint.

Nell Walton, a database administrator (DBA) who took disability leave from her NOVA job in March, said that throughout 2004 and until her departure, she tried repeatedly to convince the company to bolster security for its mammoth computer systems so they would comply with Gramm-Leach-Bliley (GLB) rules, as well as audit standards of Visa Intl., the credit card association. (NOVA disagreed, insisting it was compliant with both GLB and Visa standards.)

However, the company disregarded her concerns and retaliated by increasing her workload, assigning menial tasks and with verbal harassment, she charged. Walton said the mounting stress forced her departure.

Walton's charges were listed in a July 2005 complaint to the Labor Dept.'s Occupational Safety and Health Administration (OSHA). It essentially alleged that she was retaliated against in violation of Section 806 of the Sarbanes-Oxley Act, the corporate governance law, for being a whistleblower. According to her complaint, the retaliation began shortly after a June 2004 meeting with Executive Vice President Erik Toivonen in which she outlined her concerns about data-security inadequacies. NOVA, which services more that 650,000 small and mid-sized merchants and banks, is owned by U.S. Bancorp, a publicly traded company. Walton's complaint seeks reinstatement and $1 million in damages.

This summer, an OSHA regional office dismissed her complaint, finding that Sarbanes-Oxley offered her no relief. Walton has appealed the dismissal to a Labor Dept. administrative law judge. She is represented by Thad Guyer, a private attorney who formerly worked for the Government Accountability Project (GAP), which specialized in whistleblower cases.

"The allegations are not true; they do not accurately reflect what her job duties were or the reaction of her supervisors," said Eric Savage, an attorney with the Newark, N.J. office of Littler Mendelson, representing NOVA. "The original decision to dismiss the complaint was correct and at the end of the day, we think the administrative law judge will come to the same conclusion."

Frank Erjavec, one of Walton's supervisors who was named in her complaint, flatly disputed her charges. "I don't think her charges are valid at all. We are VISA- and MasterCard-compliant. We are audited all the time. If you want to be in business with Visa and MasterCard, you have to take security seriously. We are constantly working on security issues," Erjavec told *Privacy Times*.

The largest potential security breach this year – 40 million credit card accounts – involved CardSystems Solutions, an Arizona-based credit card processing company. The highly publicized case prompted a Congressional hearing (see *Privacy Times*, Vol. 25 No.12, June 22, 2005). At one point, the transgressions prompted Visa to cancel the company's contractual right to process credit cards. (After passing subsequent audits, the company announced Oct. 15 it was acquired by "Pay By Touch," a payments technology firm.)

CardSystems was found to have improperly kept credit card data, and well beyond the contractual time limit. Walton accused NOVA of doing the same thing. The company denied this.

Walton said NOVA's security woes were the result of a combination of inadequate management attention, and staff training and resources, and outdated equipment. She said that several databases were vulnerable, including one housing more than 1.5 billion credit card numbers or authorizations, and another containing 650,000 to 1 million merchant records that included an owner's SSN, date of birth, home address, bank account and routing numbers. Walton also expressed concern about NOVA systems used by merchants to support e-commerce transactions, including "shopping carts."

Walton's complaint argued that Sarbanes-Oxley "requires publicly traded corporations to implement computerized safeguards or controls, both preventative and detective, against internal or external tampering, and against adulteration or negligence in the maintenance of its computer systems that create financial and operational records."

"[Walton] persisted in voicing and seeking resolution to concerns pertaining to [NOVA's] failure to comply … [She] attempted to motivate compliance by disclosing these failures to corporate managers and was about to make said disclosures to external auditors. In retaliation for raising those concerns, [NOVA] subjected [Walton] to a continuing hostile and discriminatory work environment," the complaint alleged.

One oversight mechanism for NOVA's systems was the Visa audit process known as Customer Information Security Program (CISP). Walton praised the CISP standards, stating that compliance with them would greatly enhance security and help ensure compliance with other standards like GLB.

Walton's complaint stated that her concern over security heightened in early 2004 when NOVA assigned her to a CISP-compliance project with a Sept. 30, 2004 deadline.

"As the September 2004 completion date approached, [Walton's] security concerns led her to begin researching requirements for 'CISP' compliance," her complaint stated. "On November 2, 2004**,** Norman and Erjavec were found to have effected an unapproved database change, that is, one outside of the procedures and approvals prescribed in the Change Control Process."

Visa's "List of Compliant Service Providers" shows that NOVA was validated on Nov. 30, 2004. V.P. Erik Toivonen said NOVA was on target to pass the PCI Security audit next month. (Go to www.visa.com/CISP, then find on the left side the button for "Service Providers," and click; then find on the right side the "List of CISP-compliant service providers.")

Visa does not conduct audits. Instead, it has qualified about 20 companies to perform what it calls "onsite PCI Data Security Assessments for Level 1 Merchants and Levels 1 and 2 Service Providers and complete the Report on Compliance according to the PCI Security Audit Procedures and Reporting document." (Follow the link instructions above but instead of "List of CISP-compliant service providers," click on "Qualified Data Security Company List")

Toivonen said that Verisign conducted the Visa/CISP audits of NOVA in recent years. Steve Dale, a U.S. Bancorp spokesperson, along with attorney Eric Savage, said it was doubtful

that NOVA would provide *Privacy Times* with audit reports. Toivonen said that NOVA is subject to GLB, and has passed annual audits conducted by examiners from the Federal Reserve Board and the Office of the Comptroller of the Currency.

Citing OSHA's dismissal of Walton's charges and its Visa-compliant status, Dale said there was no merit to her allegations. "NOVA is and has been committed to protecting cardholder information in its internal and third party environments," he said.

A Federal Reserve spokesman said the board has jurisdiction over "holding companies" that own financial institutions. An OCC spokesman said he believed his agency also would have jurisdiction. Both spokesmen declined specific comment on the Walton case.

U.S. BANKING AGENCIES BACK TOUGHER ONLINE SECURITY

A federal panel composed of major U.S. banking agencies has issued new guidelines aimed at overhauling security in Internet-based banking and financial services, mandating stronger customer authentication requirements by next year.

Citing the growing threat posed by "phishing," identity theft, and other forms of online fraud, the U.S. Federal Financial Institutions Examination Council (FFIEC) said authentication of a customer via simple password and ID alone was "inadequate for high-risk transactions involving access to customer information or the movement of funds to other partners."

The council, which has broad regulatory powers over the banking sector, updated its guidance from 2001. The FFIEC is composed of member agencies that include the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the