

Contents:

<i>New Federal Rules on Electronically Stored Information</i>	1, 2
<i>Revised SAR Form for Financial Institutions</i>	1, 3
<i>California Appellate Court Reverses Judgment against Bank of America</i>	4
<i>Remote Deposit Agreements</i>	5

New Federal Rules on Electronically Stored Information

By: Robert E. Hayes and Mark F. Marshall

Today most information created and received in business is produced electronically in the form of e-mail messages and their attachments, word processing or spreadsheet documents, webpages, and databases. Additionally, many formal documents such as tax returns, permit applications and other documents submitted to regulatory authorities are generated, and may even be filed, in electronic format. New rules governing this "electronically stored information" or "ESI" were adopted for use in the United States Courts effective December 1, 2006. It is only a matter of time before rules governing ESI are proposed and adopted in our state courts.

These rules impose an obligation to preserve ESI as soon as litigation is

reasonably anticipated. The triggering event can be the service of a summons and complaint. Other events, including an audit, a complaint to you or a regulatory agency, or even the decision to terminate an employee may create an obligation to preserve ESI. Once a federal law suit is filed, the new rules require your lawyers to "meet and confer" with opposition lawyers shortly after a case begins to discuss "any issues relating to preserving discoverable information" including ESI. The new rules also require early disclosure of ESI that you may use to support your claim or defense. Neither task is possible unless you know the sources of ESI in your business and have an effective plan to manage that information.

(continued on page 2)

Revised Suspicious Activity Report Form for Financial Institutions

By: Kristina M. Schaefer

On December 21, 2006, the Board of Governors of the Federal Reserve, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, the National Credit Union Administration (collectively, the "Agencies"), and the Financial Crimes Enforcement Network ("FinCEN") announced revisions to the Suspicious Activity Report ("SAR") form currently

utilized by depository institutions. Although FinCEN has not yet determined the effective date for the new form, institutions should become familiar with the revisions in the interim.

The revised SAR now contemplates "joint filing" by institutions, which the Agencies and FinCEN believe will reduce the number of duplicate SARs filed for a suspicious

(continued on page 3)

New Federal Rules on Electronically Stored Information *(continued from page 1)*

If you are like many financial institutions and businesses, your systems automatically delete some ESI on a regular basis. The failure to preserve ESI, or as lawyers say, impose a "litigation hold," can have significant consequences for you. The civil consequences range from the imposition of monetary sanctions not only on you in your individual capacity as well as your business; to an instruction allowing the jury to infer the destroyed information was harmful to your case; and in flagrant cases, to the possibility that a court could direct a finding of liability against your business.

Another rule contains a so-called "safe harbor" provision that states "absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system." There is inherent tension between this "safe harbor" provision and the need to impose a litigation hold. While the "safe harbor" may protect you from sanctions "under these rules", according to some commentators, it will not protect you from other court ordered sanctions that arise from the court's inherent authority. Yet another new provision states that a party need "not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden and cost."

There are also potential criminal consequences. The Sarbanes-Oxley Act of 2002 contains a number of provisions that may apply to anyone who alters or destroys ESI. While much of the Sarbanes-Oxley Act applies only to the accounting profession, two provisions in the Act have broader application. For example, it is illegal to knowingly alter or destroy records with the intent to "impede, obstruct or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States." Another provision of the Act creates criminal penalties against anyone who "corruptly alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with intent to impair the object's integrity or availability for use in

an official proceeding." Violations of these statutes carry a maximum possible sentence of up to 20 years in prison.

We want to help you meet the challenge of managing your ESI so that we may better represent you if you are the target of a lawsuit. We believe that planning can help you identify the reasonably available sources of your ESI, enhance the comfort provided by the safe harbor provision, and minimize the burden imposed by the ultimate need to comply with the rules if you become involved in litigation. We would be pleased to have the opportunity to assist you in addressing this new rule change audits impact on your organization, including your management of electronic information and your record retention policy in general. [DEHS](#)

Revised Suspicious Activity Report Form for Financial Institutions *(continued from page 1)*

transaction, such as situations involving check kiting or fraudulent wire transfers. Institutions should keep several principles in mind when filing a joint SAR. First, if an institution files a joint SAR, both institutions must retain a copy of the SAR and the supporting documentation for the five-year retention period. In addition, institutions are not allowed to jointly file a SAR if the SAR involves an insider relationship. Moreover, although Section 314(b) of the Patriot Act (31 C.F.R. § 103.110) is not addressed by the revised SAR or its instructions, institutions must continue to comply with the voluntary information sharing requirements prior to filing a joint SAR. Failure to comply with Section 314(b) may result in the loss of the safe harbor protections regarding liability for sharing information.

Another significant change to the SAR will be the addition of detailed instructions, which contain guidance on completing the various fields. For example, certain fields will be marked with an asterisk. If this information is not known or not applicable, an institution must enter “XX” rather than leaving the entry blank. The revised instructions will also provide clarification and guidance regarding what information should be included in the narrative portion of the SAR. For example, the institution should indicate whether law enforcement has been contacted and, if so, the name of the agency and the name of any person contacted, their title, their telephone number, and when they were contacted. Other useful clarifications will include the completion of the SAR when there are multiple suspects involved and calculating the total dollar amount of the suspicious activity. The new instructions provide several illustrations, providing simple answers to common questions that arise while completing a SAR.

The new SAR form will be reorganized and, in some instances, requests slightly different information than the existing form. For example, the new SAR form includes a field for a “designated contact office” of the institution (as opposed to the existing form, which requires the reporting of the name of a contact person). In addition, the institution will enter the date the SAR was filed, as opposed to the date the SAR was prepared. Due to the number of

changes, institutions should review the new SAR form and the instructions carefully to ensure proper completion of the SAR form when it becomes effective.

The revised SAR form was initially scheduled to become effective on June 30, 2007, and mandatory on December 31, 2007. However, FinCEN recently delayed implementation until further notice. In the meantime, institutions should continue to use the existing SAR form, but should become familiar with the proposed form and watch for further information from FinCEN as to its effective date.

While the revised SAR will add some clarity to the completion of a SAR, we would note that Bank Secrecy Act (“BSA”) and SAR requirements are quite complex. Due to the importance of complying with these provisions, we strongly encourage institutions to consult their BSA officer, compliance personnel, and regulatory counsel for any questions involving BSA compliance or the filing of a SAR. DEHS

California Appellate Court Reverses Billion Dollar Judgment Against Bank of America for Applying Social Security Deposits to Overdrafts and NSF Fees

By: Amy M. Ross

In *Miller v. Bank of America*, 2006 WL 3353983, ___WL___ (Cal. Ct. App. 2006), a case being closely monitored by the banking industry, a California appellate court recently reversed the trial court's decision finding Bank of America potentially liable for \$1 billion in civil penalties for applying direct deposits of Social Security payments to overdrafts and related insufficient funds (NSF) fees. The case is currently under review by the Supreme Court of California.

In the *Miller* case, a customer's Social Security disability benefits were directly deposited into his Bank of America (the "Bank") checking account. On three occasions, the Bank automatically balanced the customer's incoming Social Security direct deposits against his overdrafts to reduce the negative balance in his account. Each time, after the customer complained, the Bank reversed the debits and restored the funds to the customer's account. Nevertheless, the customer sued the Bank as lead plaintiff in a consumer class action, using federal law and a variety of California consumer protection statutes as the basis of his claim. The jury found that the Bank violated the California statutes by falsely representing to depositors that it had the right to apply directly deposited Social Security funds to pay overdrafts and NSF fees. Based on that finding, the jury awarded statutory penalties of \$1,000 for each class member, resulting in potential penalties for the Bank in excess of \$1 billion. The Bank appealed.

The appellate court framed the key issue as follows: Does a bank act illegally if, when balancing customer accounts, it applies credits for Social Security benefits and other public benefit payments directly deposited to its customers' checking accounts to cover overdrafts and NSF fees?

Relying on existing case law, the trial court provided instructions to the jury that the Bank was prohibited from collecting overdrafts and NSF fees by debiting directly deposited Social Security and other public benefit payments. In reversing the judgment of the trial court, the appellate court drew a distinction between a bank who uses its setoff right to collect a

non-deposit account debt, as was the scenario in the case relied upon by the trial court, versus a bank's application of direct deposits to reduce the overdrafts in a customer's deposit account, as are the facts in *Miller*. Another part of the appellate court's decision in *Miller* focused on the public policy implications of this case. The appellate court concluded that disallowing bank reduction of customer overdrafts by the application of Social Security deposits would cut against good public policy by forcing banks to impose numerous restrictions on accounts containing government benefits (e.g., refusing to honor any NSF checks of those who directly deposited benefit payments, preventing customers from using ATM cards at other banks, placing the longest permissible hold on all deposited checks to minimize the incidence of returned items, and restricting or disallowing the use of debit cards). The appellate court in *Miller* concluded its opinion by stating that the decision as to whether to prohibit banks from offsetting directly deposited public benefit payments against overdraft and NSF fees would be better accomplished by statute or regulation authorized by statute than by *ad hoc* decisions of the courts.

Given the importance of this case and the large number of *amicus curiae* briefs filed on both sides, we may not see a final decision on this case any time soon. In the meantime, depository institutions may want to consider amending the terms and conditions of their deposit agreements to include language by which the customer would specifically consent to the application of directly deposited public benefit payments to overdrafts and corresponding NSF fees. Otherwise, depository institutions should proceed with caution in determining whether to offset these types of deposits against overdraft and NSF fees. DEHS

Remote Deposit Agreements

By: Matthew W. McNamee and Keith A. Gauer

The Check Clearing for the 21st Century Act (codified at 12 U.S.C. §4001 *et seq.*), also known as “Check 21” became effective on October 28, 2004. Generally speaking, Check 21 permits banks to convert checks to images and transfer them electronically through the check clearing system. Taking advantage of technological innovations and applications, a bank (or its customer) may now convert a paper check into an electronic image. A number of our clients have started offering remote deposit capture services to commercial customers. Under a typical remote deposit arrangement, the commercial customer prepares its daily check deposit by scanning the checks to convert them to images, preparing an electronic deposit ticket, and transferring the information to its bank electronically.

Almost universally, banks turn to third party vendors to provide support for remote deposit services. Some vendors will offer “turn key” systems for the bank to use, including hardware and software solutions. Others will simply sell a software package for the bank to use. In any event, the bank must carefully review the contract with the vendor to be certain the bank understands the products and services to be provided by the vendor as well as the technical support provided. The bank should also pay close attention to the term of the agreement, including the duration of any software license and any commitment of the provider to update the software (and the costs of such updates).

As part of the package, these vendors will often provide forms of electronic check processing agreements. These agreements document the understanding between the bank and the customer in connection with the services being provided by the bank, and the responsibilities of the parties. As such, they should be reviewed by the bank and legal counsel to determine that they accurately set forth the bank’s intentions. One size does not fit all for these type of agreements. The bank needs to keep in mind the type of customer to whom it intends to market the service.

Remote deposit services should not be offered to all customers. As a result of the “outsourcing” of the bank’s normal check deposit functions, and the increased opportunity for customer fraud associated therewith, remote deposit services should only be of-

fered to seasoned bank customers. Start ups or thinly capitalized companies should not be considered and caution should also be exercised in offering the service to new customers.

With respect to the customer agreement itself, the bank should review the agreement to be certain that it addresses several key points. The agreement must precisely define the duties of the customer in scanning the checks and preparing the electronic deposit ticket. The agreement will also set out the technological requirements for the customer’s computer system and describe the software and hardware, if any, to be provided, licensed, or leased from the bank. The bank’s fees in connection with the service must also be explained in detail and may vary by customer. Frequently, we have seen banks provide remote deposit functions without fee in an effort to win the business of customers.

The customer agreement should also set forth detailed requirements for the scanning, retention, and destruction of the original checks. Since the “double” depositing of the checks presents the greatest risk of fraud in these arrangements, the bank will want to insure that the original checks are handled properly after the scan is accomplished and that appropriate security measures are put in place by the customer to secure the system from fraud. The agreement may designate the deposit cut-off times, file size limits for the customer, and the procedures describing the bank’s rejection of checks and the bank’s ability to force the paper deposit of drafts if appropriate. The agreement should also include appropriate warranties obligating the customer to warrant and represent the validity of any check sent through the system.

Remote deposit services provide an exciting new product in the array of financial services banks can offer to commercial customers, particularly those outside of your normal geographic footprint. A successful program will, however, require careful selection of the third party vendor providing the hardware and software for the program, selective underwriting of the customers to be offered the service, and appropriate legal review of the vendor and customer agreements governing the program. DEHS

**DAVENPORT
EVANS
HURWITZ &
SMITH LLP
LAWYERS**

206 West 14th Street
P.O. Box 1030
Sioux Falls, SD 57101-1030

Phone 605.336.2880
Fax 605.335.3639
www.dehs.com

Davenport, Evans, Hurwitz & Smith, LLP was founded in 1939. Since that time, the firm has grown steadily and is now one of the largest firms in South Dakota. For more than fifty years, the firm has assisted clients in banking and financial services matters. The firm acts as counsel to many South Dakota banks, financial institutions, and holding companies. Davenport, Evans also regularly acts as counsel to businesses who contract with banks, including various servicing and marketing firms.

The firm handles all aspects of banking law, from entity formation, acquisitions, and branching to operational issues involving lending, compliance, creditors' rights, payment processing (check, ACH, wire transfer), general commercial law, and trust administration. The firm represents banks in all phases of state and federal banking regulation and deals extensively with state and federal banking regulators. The firm understands that keeping up with new regulatory developments is a major challenge for banks today and helps its clients respond to that challenge effectively and efficiently.

South Dakota has become a major center for financial services, with approximately a half dozen credit card processing centers located in the Sioux Falls area alone. The firm has served as counsel to many of these entities and has particular experience and expertise in the areas of credit card and stored value card issuance, compliance, and receivables securitization.

The firm also represents its bank clients in bankruptcy matters and complex mediations, foreclosures, and commercial litigation on a regular basis. Davenport, Evans often acts as counsel to lenders in loan workouts and bankruptcy cases filed in South Dakota. The firm's banking and financial services lawyers, together with the firm's strong litigation practitioners, also handle commercial litigation such as bank shareholder disputes, complex lender liability cases, bank-marketer disputes, federal compliance cases, employment disputes and many other litigation cases. Our employment law attorneys assist clients with personnel issues and discrimination claims while our benefits lawyers develop both qualified and non-qualified benefit and retirement plans.

Numerous out-of-state and nationwide lenders also retain the firm for review of loan documents, compliance with state and federal law, and assistance in completing major real estate and commercial loans. The firm also assists out of state individuals and entities in the formation and operation of trust companies.

If you have any questions or desire assistance on any matter, please feel free to contact us at your convenience.

<u>Attorney</u>	<u>Telephone</u>	<u>@dehs.com</u>
Scott B. Anderson	605-357-1225	sanderson
Jean H. Bender	605-357-1224	jbender
Jonathan P. Brown	605-357-1271	jbrown
Rochelle R. Cundy	605-357-249	rcundy
P. Daniel Donohue	605-357-1226	pddonohue
Edwin E. Evans	605-357-1219	eevans
Thomas M. Frankman	605-357-1217	tfrankman
Keith A. Gauer	605-357-1256	kgauer
Timothy M. Gebhart	605-357-1243	tgebhart
Cheryle Wiedmeier Gering	605-357-1251	cgering
Charles D. Gullickson	605-357-1270	cgullickson
Mark W. Haigh	605-357-1220	mhaigh
Douglas J. Hajek	605-357-1227	dhajek
Sandra Hoglund Hanson	605-357-1253	shanson
Robert E. Hayes	605-357-1260	rhayes
Dixie K. Hieb	605-357-1277	dhieb
Melissa C. Hinton	605-357-1262	mhinton
Kristi Geisler Holm	605-357-1221	kholm
Eric R. Johnson	605-357-1259	ejohnson

<u>Attorney</u>	<u>Telephone</u>	<u>@dehs.com</u>
David L. Knudson	605-357-1222	dknudson
Roberto A. Lange	605-357-1232	rlange
Sarah Richardson Larson	605-357-1228	slarson
Michael L. Luce	605-357-1231	mluca
Mark F. Marshall	605-357-1246	mmarshall
Matthew W. McNamee	605-357-1229	mmcnamee
Rick W. Orr	605-357-1292	rorr
Dana Van Beek Palmer	605-357-1250	dpalmer
Mitchell A. Peterson	605-357-1242	mpeterson
Brendan W. Reilly	605-357-1254	breilly
Amy M. Ross	605-357-1273	aross
Kristina M. Schaefer	605-357-1213	kschaefer
Eric C. Schulte	605-357-1241	eschulte
Susan Brunick Simons	605-357-1263	ssimons
Catherine A. Tanck	605-357-1223	ctanck
Robert L. Thomas	605-357-1214	rthomas
Monte R. Walz	605-357-1266	mwalz
Annette M. White	605-357-1258	awhite