Consumer Compliance Outlook®

Fourth Quarter 2012

Inside

A federal reserve system publication with a focus on consumer compliance issues

Smartphone interactive scan

Vendor Risk Management – Compliance Considerations

By Cathryn Judd, Examiner, and Mark Jennings, Former Examiner, Federal Reserve Bank of San Francisco

On May 2, 2012, the Federal Reserve System hosted an *Outlook Live* webinar titled *Vendor Risk Management – Compliance Considerations*.[1] The speakers addressed a number of compliance-related risks associated with using third-party service providers. This article reinforces the best practices discussed during the webinar and reviews the risks of using third-party vendors.

QUESTIONS ABOUT THIRD PARTIES

What Are Common Types of Third-Party Relationships?

Some common third-party relationships include:

- *Third-party product providers* such as mortgage brokers, auto dealers, and credit card providers;
- *Loan servicing providers* such as providers of flood insurance monitoring, debt collection, and loss mitigation/foreclosure activities;
- *Disclosure preparers*, such as disclosure preparation software and third-party documentation preparers;
- *Technology providers* such as software vendors and website developers; and
- *Providers of outsourced bank compliance functions* such as companies that provide compliance audits, fair lending reviews, and compliance monitoring activities.

What Are the Risks of Using Vendors?

Third parties present a broad range of risks, including:

- *Compliance risks* such as violations of laws, rules, or regulations or non-compliance with policies or procedures;
- *Reputation risks* such as dissatisfied customers or violations of laws or regulations that lead to public enforcement actions;
- *Operational risks* such as losses from failed processes or systems or losses of data that result in privacy issues;
- *Transaction risks* such as problems with service or delivery; and
- *Credit risks* such as the inability of a third party to meet its contractual obligations.

These risks are heightened when a vendor operates directly between the bank and its customers. Vendors may be heavily involved in delivering prod-

continued on page 10

[1] The webinar has been archived and is available for replay at: http://tinyurl.com/Vendor-outlook

Error Resolution Procedures and Consumer Liability Limits for Unauthorized Electronic Fund Transfers

By Kenneth Benton, Senior Consumer Regulations Specialist, and Robert Sheerr, Research Assistant, Federal Reserve Bank of Philadelphia

Congress passed the Electronic Fund Transfer Act (EFTA) in 1978 to protect consumers engaging in electronic fund transfers (EFTs). The law provides the legal framework for the rights, liabilities, and responsibilities of participants in EFT systems that consumers use such as automated teller machines (ATMs), debit point-of-sale terminals in retail stores, and automated clearing house (ACH) transactions such as electronic payment of a creditor's bill from a consumer's checking account. Regulation E implements the EFTA's requirements.

Among its provisions, Regulation E specifies procedures that institutions must follow for investigating and resolving errors alleged by consumers for EFTs, such as an unauthorized ATM withdrawal. The regulation also specifies the extent to which a consumer can be held liable for unauthorized EFTs. To facilitate compliance, this article reviews the regulation's error resolution and consumer liability provisions.

ERROR RESOLUTION PROCEDURES: 12 C.F.R. §1005.11

Section 1005.11 sets forth the procedures financial institutions must follow after receiving notice from a consumer of an error for an EFT. Before discussing these procedures, it is helpful to identify issues that are deemed "errors." Under §1005.11(a), the term error includes:

- An unauthorized EFT;
- An incorrect EFT to or from a consumer's account;
- An omission of an EFT from a consumer's periodic statement;
- A computational or bookkeeping error by the institution for an EFT;
- A consumer's receipt of an incorrect amount of money from an electronic terminal;[1]
- An EFT that was not identified in accordance with §1005.9 or §1005.10(a); and
- The consumer's request for documentation required by §1005.9 or §1005.10(a) or for additional information or clarification concerning an electronic fund transfer, including a request the consumer makes to determine whether one of the errors listed above actually exists.

The term "error" does not include routine inquiries about a consumer's account balance, requests for information for tax or other record-keeping purposes, or requests for duplicate copies of documentation.[2] Financial in-

[1] The term electronic terminals means electronic terminals through which a consumer may initiate an EFT, such as ATMs, point-of-sale terminals, and cash-dispensing machines; the term does not include telephones operated by consumers. 12 C.F.R. §1005.2(h). However, no error occurs in cases where the institution does not make a terminal receipt available for transfers of $15 or less. Comment 11(a)-6; see also 12 C.F.R. §1005.9(e).

[2] 12 C.F.R. §1005.11(a)(2)

stitutions must follow the required error resolution procedures even if the institution receives notice of an error after the consumer has closed the account.[3]

Notice of Error Requirements

A financial institution must comply with the §1005.11 error resolution procedures with respect to any notice of an error from the consumer that:

- is received by the institution no later than 60 days after transmitting the periodic statement on which the error is first reflected;[4]
- enables the institution to identify the consumer's name and account number;
- indicates why the consumer believes an error exists; *and*
- includes, to the extent possible, the type, date, and amount of the error.[5]

Consumers can provide either written or oral notice. If a consumer provides oral notice, the institution may require the consumer to provide written confirmation of the error within 10 business days after oral notice.[6]

Time Limits for Completing Investigations

Generally, a financial institution must complete its investigation of an error within 10 business days of receiving a notice of error, but it may extend this period to 45 calendar days if certain conditions are met. The 10-business-day limit applies even if an institution received oral notice and required the consumer to provide written notice. The institution must begin the investigation promptly and cannot delay it until it receives written confirmation.[7] In certain circumstances, the 10-day period can be extended to 20 days, and the 45-day period can be extended to 90 days.

10 Business Days After Notice. Unless a financial institution is permitted a longer time period to investigate an error in the circumstances discussed below, the institution has 10 business days after receiving notice from the consumer to investigate if an error occurred. However, if the alleged error involves an EFT to or from the account within 30 days after the first deposit into the account, the investigation period is extended to 20 business days instead of 10.[8]

45 Calendar Days After Notice. If the financial institution is unable to complete its investigation within 10 business days, it may extend the period to 45 calendar days from receipt of notice provided the institution:

- Provisionally credits the consumer's account for the full amount of the alleged error plus interest, if any. However, the institution may withhold a maximum of $50 of the amount credited if the institution has a "reasonable basis" for believing an unauthorized EFT occurred and complies with the limitation on liability rules in §1005.6(a), as discussed later in the article.
- Informs the consumer of the amount and date of the provisional crediting within two business days of the crediting; and
- Allows the consumer full use of the provisional funds during the investigation.[9]

The institution is not required to provisionally credit a consumer's account to extend the time period for investigation to 45 days if the institution requires but does not receive written confirmation within 10 business days of an oral notice of error or the alleged error involves an account that is subject to Regulation T, concerning securities credit by brokers and dealers.[10]

CONTINUED ON PAGE 14

[3] Comment 11(a)-4

[4] When a notice of error is based on documentation or clarification that the consumer requested under §1005.11(a)(1)(vii), notice is timely if received by the institution no later than 60 days after the bank transmits the requested documentation. 12 C.F.R. §1005.11(b)(3)

[5] 12 C.F.R. §1005.11(b). However, the consumer is not required to allege any specific error if the consumer requests documentation or clarification pursuant to 12 C.F.R. §1005.11(a)(1)(vii) to determine whether an error actually occurred. 12 C.F.R. §1005.11(b)(iii)

[6] 12 C.F.R. §1005.11(b)(2)

[7] Comment 11(c)-2

[8] 12 C.F.R. §1005.11(c)(3)(i)

[9] 12 C.F.R. §1005.11(c)(2)

[10] 12 C.F.R. §1005.11(c)(2)(i); see also 12 C.F.R. Part 220 (Securities Credit by Brokers and Dealers).

HMDA Data Collection and Reporting

By Jason Lew, Compliance Risk Coordinator, Federal Reserve Bank of San Francisco

On September 18, 2012, the Federal Financial Institutions Examination Council (FFIEC) announced the availability of data on mortgage lending transactions from 7,632 U.S. financial institutions covered by the Home Mortgage Disclosure Act (HMDA), which is implemented through Regulation C.[1] The data cover 2011 lending activity, including applications, originations, loan purchases, denials, and other actions such as incomplete or withdrawn applications. These data will be used in a number of supervisory processes, including examinations and applications, as well as for public policy purposes. The use of these annual data by various stakeholders is a good reminder to financial institutions covered by HMDA of the importance of collecting and reporting timely and accurate data. This article answers questions frequently asked by institutions regarding the collection and reporting of HMDA data and provides an overview of expected changes to HMDA reporting requirements.

SUBMITTING YOUR 2012 HMDA DATA

The deadline for covered institutions to submit their 2012 HMDA data is March 1, 2013.[2] This section discusses some valuable HMDA resources and some common issues bankers encounter when submitting HMDA data.

Resources

In addition to Regulation C and its Official Staff Commentary (Commentary), the FFIEC's 2010 *A Guide to HMDA Reporting: Getting it Right!*[3] is a good resource for HMDA data collection and reporting. The guide provides a summary of responsibilities and requirements, directions for assembling the necessary tools, and step-by-step instructions for reporting HMDA data.

Other resources include an *Outlook* article in the Fourth Quarter 2009 issue titled "Improving and Using HMDA Data in Your Compliance Program"[4] and a November 2010 *Outlook Live* webinar titled *Tips for Reporting Accurate HMDA and CRA Data*. The webinar and presentation slides are available at http://bit.ly/hmda-outlook-live. *Outlook* subsequently published some of the unanswered questions received during the webinar in an article in the Second Quarter 2011 titled "Home Mortgage Disclosure Act (HMDA) and Community Reinvestment Act (CRA) Data Reporting: Questions and Answers."[5]

Questions and Answers

The webinar and articles addressed a number of questions examiners commonly received from institutions. In this section, we answer some additional HMDA questions that filers frequently raise.

Coverage. Questions often arise as to whether a loan is reportable. One common question concerns a consumer who borrows against property purchased with cash (home equity loan or home equity line of credit (HELOC)). HMDA requires covered depository and nondepository institutions to collect data regarding applications for, and originations and purchases of, home purchase loans, home improvement loans, and refinancings.[6] Because the loan is not being used to purchase the home or refinance an existing loan, it is neither a home purchase loan nor a refinancing. If any portion of the loan proceeds will be used to repair, rehabilitate, remodel, or improve a dwelling or the real property on which the dwelling is located, the loan qualifies as a home improvement loan, and the entire loan amount should be reported.[7] If the loan is a HELOC and any portion of the proceeds will be used for home improvement, the rules are slightly different because HMDA reporting of HELOCs is optional, and the institution reports only the amount of the loan intended for home improvement if it chooses to report

[1] http://www.ffiec.gov/press/pr091812.htm

[2] 12 C.F.R. §1003.5(a)(1)

[3] *A Guide to HMDA Reporting: Getting it Right!* is located on the FFIEC's website at: http://www.ffiec.gov/hmda/guide.htm.

[4] http://tinyurl.com/cco-HMDA2

[5] http://tinyurl.com/cco-hmda

[6] See 12 C.F.R. §1003.4(a).

[7] See *Guide to HMDA Reporting*, p. 28.

the loan.[8] To determine the purpose of the loan, an institution can rely on the applicant's oral or written statement about the proposed use of the loan proceeds. For example, the loan application could contain a check-box or purpose line to indicate if the purpose of the loan is home improvement.[9]

Government Monitoring Information (GMI). GMI continues to be an area in which questions arise. In most cases, errors stem from oversights when information is collected from the loan application; however, here are some recommendations to avoid violations:

- *Use the GMI collection form for all home mortgage loan applications.* Institutions subject to HMDA must use a GMI collection form similar to the one in Appendix B of Regulation C for all loans subject to HMDA, including loan applications taken by mail, Internet, or telephone. "For applications taken by telephone, the information in the [GMI] collection form must be stated orally by the lender, except for information that pertains uniquely to applications taken in writing."[10] If the applicant does not provide the GMI data, institutions should use the code on the LAR corresponding to "information not provided by applicant in mail, Internet, or telephone application."[11] For applications taken in person, the institution reports the information the applicant provides.[12] However, if the applicant fails to provide the requested information for an application taken in person, the institution reports the data based on visual observation or surname.[13] A joint applicant can provide the information on behalf of an absent joint applicant.[14]
- *Don't change the data.* Examiners have noted a number of recent cases in which loan officers changed HMDA data (ethnicity, race, and sex) based on the loan officer's impression that the information was inaccurate. Data provided by the applicant must be reported on the LAR as submitted. As noted in Comment 4(a)(10)-1: "An institution reports the monitoring information as provided by the applicant. For example, if an applicant checks the 'Asian' box the institution reports using the 'Asian' Code."

Unsecured Lines of Credit. Another frequently asked question is whether unsecured lines of credit for home improvement purposes are reportable. Under HMDA, a home improvement loan includes a loan that is not secured by the dwelling but is for the purpose, in whole or in part, of repairing, rehabilitating, remodeling, or improving a dwelling or the real property on which the dwelling is located and that is classified by the financial institution as a home improvement loan.[15] As further explained in Comment 2(g)-1 for home improvement loans: "An institution has 'classified' a loan that is not secured by a lien on a dwelling as a home improvement loan if it has entered the loan on its books as a home improvement loan, or has otherwise coded or identified the loan as a home improvement loan. For example, an institution that has booked a loan or reported it on a 'call report' as a home improvement loan has classified it as a home improvement loan. An institution may also classify loans as home improvement loans in other ways (for example, by color-coding loan files)."

Modular Homes. According to the FFIEC FAQs, an institution may choose to report modular homes on the HMDA Loan Application Register as either a one- to four-family dwelling or as a manufactured home until further guidance on the definition of a modular home is provided. The FAQ discussing modular homes is available at http://www.ffiec.gov/hmda/faqreg.htm#modular.

CONTINUED ON PAGE 19

[8] See Comment 4(a)(7)-3.

[9] See Comment 4(a)(3)-1.

[10] See *Guide to HMDA Reporting*, p. A-5.

[11] See *Guide to HMDA Reporting*, p. A-6.

[12] See Comment 4(a)(10)-1.

[13] See Comment 4(a)(10)-2.

[14] See Comment 4(a)(10)-4.

[15] See 12 C.F.R. §1003.2 and *Guide to HMDA Reporting, p.8*.

News from Washington: Regulatory Updates*

Consumer Financial Protection Bureau (CFPB) proposes rules for loan origination. On August 17, 2012, the Consumer Financial Protection Bureau (CFPB) proposed rules to implement provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). The CFPB expects to make the rules final by January 2013. The Dodd-Frank Act restricts points and fees for consumer mortgages in which the loan originator's compensation is paid by the creditor. For these mortgages, the Dodd-Frank Act prohibits payment of upfront points. The CFPB is seeking public comment on a proposal that would require lenders to make a no-point, no-fee loan option available but would also allow consumers to accept loans with points and fees if that is what the consumer prefers. The CFPB is also asking for comments on a proposal that seeks to ensure that there is an appropriate interest-rate reduction when consumers elect to pay upfront points or fees. The proposal also affects loan originators' qualifications and compensation and restricts arbitration clauses and financing of credit insurance. The comment period ended on October 16, 2012, and the CFPB expects to issue final rules in January 2013.

CFPB proposes rule to improve consumer access to appraisal reports. On August 15, 2012, the CFPB released a proposed rule that would require creditors to provide home loan applicants with free copies of written appraisals and other home valuations developed in connection with an application for a loan to be secured by a first lien on a dwelling. The proposed rule would also require creditors to inform applicants in writing within three business days of application of their right to receive a free copy of the appraisals and valuations. Creditors would then be required to provide the reports to the applicants as promptly as possible but in no case later than three days before closing, regardless of whether credit is extended or denied or the application is incomplete or withdrawn. Under the proposed rule, creditors could still charge a fee associated with conducting the appraisals and valuations. The proposed rule would amend Regulation B and implement an amendment to the Equal Credit Opportunity Act enacted as part of the Dodd-Frank Act. The comment period ended on October 15, 2012. The CFPB plans to issue a final rule in January 2013.

Agencies issue proposed rule on appraisals for higher risk mortgages. On August 15, 2012, the Federal Reserve Board (Board), the CFPB, the Federal Deposit Insurance Corporation (FDIC), the Federal Housing Finance Agency, the National Credit Union Administration, and the Office of the Comptroller of the Currency (OCC) issued a proposed rule to establish new appraisal requirements for higher-risk mortgage loans. A loan is high risk if its annual percentage rate exceeds the specified threshold. For such loans, the proposed rule would require creditors to use a licensed or certified appraiser who prepares a written report based on a physical inspection of the interior of the property. The proposed rule would also require creditors to disclose to applicants information about the purpose of the appraisal and provide consumers with a free copy of any appraisal report. Creditors would have to obtain a second appraisal at no cost to the consumer for a high-risk home purchase loan if the seller acquired the property for a lower price during the past six months. This requirement would address fraudulent property flipping by seeking to ensure that the value of the property being used as collateral for the loan legitimately increased. The comment period ended on October 15, 2012.

Availability of 2011 small business, small farm, and community development lending data. On August 14, 2012, the Federal Financial Institutions Examination Council (FFIEC), the Board, the FDIC, and the

OCC announced the availability of data on small business, small farm, and community development lending reported by commercial banks and savings associations, pursuant to the Community Reinvestment Act (CRA). Disclosure statements on the reported 2011 CRA data are available in electronic form for each reporting commercial bank and savings association. Aggregate disclosure statements of small business and small farm lending for all of the metropolitan statistical areas and nonmetropolitan counties in the United States and its territories are also available.

The CFPB proposes rules for mortgage servicers. On August 10, 2012, the CFPB issued rulemaking notices under Regulations Z and X to implement provisions of the Real Estate Settlement Procedures Act (RESPA) and Truth in Lending Act (TILA) that impose new requirements for mortgage servicers. The proposed rules would require monthly mortgage statements and written notices before interest rate adjustments and would impose requirements for using force-placed insurance, responding to consumer inquiries, correcting servicing errors, and providing timely payoff information.

In addition to implementing the Dodd-Frank Act's requirements, the CFPB also proposed to use its rulemaking authority to require mortgage servicers to intervene early with troubled and delinquent borrowers. The proposed rule would regulate how servicers respond to consumers that request assistance by seeking foreclosure alternatives. The CFPB's rules would not require servicers to offer loss mitigation options but would mandate procedures and time frames for servicers that do. The rules would not prohibit servicers from using "dual tracking" to continue the foreclosure process while pursuing loss mitigation options. The proposal also includes rules on information management and the duties of a servicer's employees, to ensure that consumers are able to contact personnel who can access the relevant records and provide assistance.

The Board approves final rule permitting debit card issuers to receive a fraud prevention adjustment. On July 27, 2012, the Board approved a final rule that amends the provisions in Regulation II (Debit Card Interchange Fees and Routing) that permit a debit card issuer subject to the interchange fee standards to receive a fraud-prevention adjustment. Under the final rule, an issuer will be eligible for an adjustment of no more than 1 cent per transaction if it develops and implements policies and procedures that are reasonably designed to take effective steps to reduce the occurrence and costs of fraudulent debit card transactions. The final rule simplifies the fraud-prevention aspects required to be included in an issuer's fraud-prevention policies and procedures. The final rule requires an issuer to review its fraud-prevention policies and procedures and their implementation at least annually and to update its policies and procedures as necessary in light of their effectiveness, cost-effectiveness, changes in the types of fraud, and available methods of fraud prevention. An issuer that meets these standards and wishes to receive the adjustment must annually notify the payment card networks in which it participates of its eligibility to receive the adjustment. The final rule also prohibits an issuer from receiving or charging a fraud-prevention adjustment if the issuer is substantially noncompliant with the Board's fraud-prevention standards and describes steps an issuer must take once it becomes substantially noncompliant to become eligible to receive the fraud-prevention adjustment in the future. The amendments were effective October 1, 2012.

* Links to the announcements are available in the online version of *Outlook* at: http://www.consumercomplianceoutlook.org.

On the Docket: Recent Federal Court Opinions*

REGULATION Z – TRUTH IN LENDING ACT (TILA)

The Tenth Circuit rules that borrowers are not required to allege their ability to repay loan proceeds in a rescission lawsuit. *Sanders v. Mountain America Federal Credit Union*, 689 F.3d 1138 (10th Cir. 2012). The borrowers filed a lawsuit to exercise the right of rescission, and the trial court dismissed it because the borrowers did not allege that if the court granted rescission, they had the ability to repay the loan proceeds to the creditor. On appeal, the Tenth Circuit reversed this ruling. The court noted that when a borrower seeks rescission after the normal waiting period of three business days (the right of rescission can be extended up to three years in certain circumstances), the creditor faces the risk of releasing its security interest without adequate assurance that the borrower can return the loan proceeds. The court found that it may be proper in some cases to require debtors to demonstrate that they can repay the loan proceeds before rescinding a loan. However, the lower court erred by requiring *all* borrowers filing lawsuits seeking rescission to allege their repayment ability in their complaint, whether or not the lender had demonstrated that this was necessary. The court noted that neither TILA nor Regulation Z requires borrowers to allege repayment ability in rescission cases. The case was remanded for further proceedings.

REGULATION B – EQUAL CREDIT OPPORTUNITY ACT (ECOA)

The Ninth Circuit reverses dismissal of ECOA case against two auto dealers. *U.S. v. Union Auto Sales, Inc.,* 2012 WL 2870333 (9th Cir. 2012). In 2007, the Federal Reserve Board referred a bank under its supervision to the U.S. Department of Justice (DOJ) for fair lending issues involving indirect auto lending. The referral alleged that the bank and two automobile dealers discriminated against non-Asian borrowers, many of whom were Hispanic, by charging them overages more frequently and in higher amounts. The DOJ subsequently settled with the bank and proceeded against two of the automobile dealers, Union Auto Sales, Inc. and Han Kook Enterprises, Inc. in federal court. The trial court dismissed the lawsuit. The Ninth Circuit reversed the dismissal of the case against Union Auto Sales, holding that the complaint adequately alleged facts sufficient to establish a plausible claim under ECOA at the pleading stage. In particular, the complaint alleged that the dealer charged overages of approximately 35 to 155 basis points higher than those of Asian borrowers and that the differences were statistically significant and could not be explained by nondiscriminatory factors such as differences in the customers' creditworthiness. The case was remanded for further proceedings consistent with the decision.

REGULATION E – ELECTRONIC FUND TRANSFER ACT (EFTA)

Two federal courts rule in class action cases seeking statutory damages for inconspicuous or missing fee notice on automated teller machines (ATM). *Brown v. Wells Fargo & Co.*, 284 F.R.D. 432 (D. Minn. July 25, 2012) and *Charvat v. First National Bank of Wahoo*, 2012 WL 2016184 (D. Neb. June 4, 2012). The EFTA and Regulation E require ATM operators to provide two fee notices: one on the ATM itself and one on the ATM screen that must be displayed before a fee can be imposed. Several class action lawsuits have been filed when operators failed to display the fee notice on the machine or placed it in an inconspicuous location. In *Brown*, the plaintiff alleged that Wells Fargo Bank and its holding company, Wells Fargo & Co., violated the EFTA and Regulation E by posting an inconspicuous fee notice on the ATM. The court dismissed Wells Fargo & Co. from the case because the notice requirements apply only to ATM operators and the holding company is not an operator. As to Wells Fargo Bank, the operator of the ATM, the court examined the factors relevant to conspicuousness and prominence, including the location of the disclaimer, the type size used, whether the notice was set off in some way (e.g, capital letters), and the location of the warning, and found a violation because Wells Fargo's notice "did not stand out relative to other information on or near the ATM." However,

the court denied the plaintiff's motion for class certification because of the plaintiff's claim for actual damages, which are available under the EFTA only if a plaintiff suffers harm by relying on a violation. Because the ATM screen displayed the fee notice and required the plaintiff's consent to the fee to complete the transaction, he could not establish any damages resulting from the inconspicuous on-machine fee notice. He therefore did not satisfy the class certification requirements under Rule 23(a) of the Federal Rules of Civil Procedure that his claim is typical of the class and that he would be an adequate representative of the class.

In *Charvat*, the plaintiff alleged EFTA and Regulation E violations because the bank failed to post a fee notice on an ATM. The bank moved to dismiss the case for lack of standing because the plaintiff conceded that he saw the second fee notice on the ATM screen and thus was not harmed by the violation. The EFTA allows a plaintiff to recover any actual damages resulting from a violation as well as statutory damages in the minimum amount of $100 and the maximum amount of $1,000. The district court considered whether a plaintiff who suffers no actual harm from a violation of a statute or regulation has standing to proceed because Congress has provided a minimum recovery for a violation through statutory damages. The court concluded that to satisfy the constitutional standing requirement necessary for filing a lawsuit, the plaintiff must have suffered an actual injury resulting from the ATM operator's failure to post the fee notice on the ATM. Because the plaintiff did not satisfy this requirement, the court dismissed the lawsuit. On a related note, the House of Representatives passed HR 4367 in July 2012, which would amend the EFTA to eliminate the requirement that ATM operators must post a fee notice on ATMs. ATM operators would still be required to display a fee notice on the ATM screen that must be read and consented to before an ATM fee could be imposed. On December 11, 2012, the Senate unanimously passed HR 4367 and sent it to the President for signature.

FEDERAL ARBITRATION ACT (FAA)

The Eleventh Circuit upholds a bank's arbitration agreement but finds the cost and attorney's fee provision unconscionable and unenforceable. *Barras v. Branch Banking & Trust Co.*, 685 F.3d 1269 (11th Cir. 2012). Beginning in 2009, the federal Judicial Panel on Multidistrict Litigation consolidated more than 30 lawsuits on overdraft fees into a single case, *In re: Checking Account Overdraft Litigation* (MDL No. 2036), for purposes of resolving common pre-trial issues. The lawsuits allege that the banks' overdraft fee practices, including some banks' practice of processing checks and debit transactions from highest to lowest, violate consumer protection laws. Branch Banking & Trust Company (BB&T), one of the defendants, filed a motion to enforce the mandatory arbitration clause in its account agreement. The trial court found that the arbitration agreement was unconscionable and unenforceable because it required the customer to pay the costs and fees of the arbitration, including attorney's fees, regardless of whether the customer lost. BB&T appealed, and the Eleventh Circuit directed the trial judge to reconsider his decision in light of the new arbitration decision from the Supreme Court in *AT&T Mobility LLC v. Concepcion*, 131 S. Ct. 1740 (2011). On remand, the trial judge again found that the arbitration agreement was unenforceable, and BB&T appealed. The Eleventh Circuit agreed with the trial court's ruling that the costs-and-fees provision was unconscionable under South Carolina state law because it appeared on page 14 of the agreement and was not included with the arbitration information at the beginning of the agreement. The court also found that requiring customers to pay the bank's costs and attorney's fees, even if the customers prevail, was unreasonable and contrary to well-established doctrine that losing parties cannot collect costs and attorney's fees from the prevailing party. However, the arbitration agreement contained a severability clause stating that if any provision in the agreement was struck down, all other provisions remained in effect. Accordingly, the court ordered the parties to arbitrate their dispute but struck down the provision requiring the consumer to pay the bank's fees and costs.

* Links to the court opinions are available in the online version of *Outlook* at: http://www.consumercomplianceoutlook.org.

CONTINUED FROM PAGE 1...

Vendor Risk Management – Compliance Considerations

ucts and services to an institution's customers, but their actions or activities may not be adequately monitored. These risks have been manifested most significantly through deceptive vendor marketing, credit discrimination, data loss leading to privacy issues, and unfair or deceptive acts or practices (UDAP).

While vendors often provide value through their expertise and experience, the bank's board and senior management are ultimately responsible for all aspects of the bank's operations, including products and services provided by vendors. Accordingly, effective risk management is required to mitigate the risks associated with the loss of control and close oversight that often occurs with a vendor relationship. A good rule of thumb is to oversee vendors as you would any other department in your bank, regardless of the vendor's reputation or apparent ability to comply with consumer protection laws and regulations.

PRACTICES THAT INCREASE THE RISK OF VIOLATIONS

Vendor risk management problems often involve one or more of the following issues:

- *Overreliance on third-party vendors.* A common root cause of vendor problems is the overreliance, and sometimes complete reliance, on a third-party vendor. Third parties can provide staffing and expertise but do not assume ultimate responsibility for compliance violations involving products or services offered by an institution.
- *Failure to train new staff or retain knowledgeable staff.* Institutions may believe they can avoid hiring, retaining, or training staff because of a vendor's expertise. Although an institution may be leveraging a third party's expertise, staff at the institution must be knowledgeable about vendor activities and the compliance requirements for that activity to facilitate monitoring. Specifically, proper staffing or specialized training for existing personnel may be required. Similarly, banks should consider evaluating activity at the vendor's location to ensure that risks are understood and that staff has sufficient knowledge of vendor processes and controls.
- *Failure to adequately monitor the vendor.* Ongoing monitoring is necessary to ensure compliance and to prevent potentially costly regulatory violations.
- *Failure to set clear expectations.* An institution must ensure that the information provided to third-party vendors is complete and accurate and that expectations for vendor performance are communicated clearly and included in the contract with the vendor. Vendor contracts should also include detailed consumer protection requirements to ensure that the vendor is aware of the applicable requirements.

EXAMPLES OF VENDOR RISK MANAGEMENT COMPLIANCE ISSUES

An institution's failure to maintain a strong vendor management program presents significant risks. Here are some examples noted during recent examinations.

Flood Insurance Monitoring

Banks often use vendors to ensure that all loans secured by properties located in special flood hazard areas have adequate flood insurance, that all insurance amounts are correct for the specific property covered, and that appropriate insurance coverage remains in effect during the life of such loans. A vendor's error in calculating the amount of insurance required can result in significant flood insurance violations involving multiple properties and civil money penalties (CMPs). Under the Biggert-Waters Flood Insurance Reform Act of 2012 (Biggert-Waters Act),[2] which was signed into law on July 6, 2012, CMPs against regulated lending institutions with a "pattern or practice" of violating certain flood insurance requirements were increased from $385 to $2,000 for each violation. In addition, the Biggert-Waters Act removed the $135,000 statutory cap on the amount of CMPs that may be assessed against an individual financial institution in a single calendar year. This change was effective on July 6, 2012.[3]

[2] Pub. L. 112-141, Div. F, Tit. II, Subtit. A

[3] *Outlook* summarized the Biggert-Waters Act in the Third Quarter 2012 issue. The act was also discussed during the December 4, 2012 *Outlook Live* webinar "Consumer Compliance Hot Topics—2012 Year in Review," which is available at: http://www.visualwebcaster.com/FederalReserveBankSF/91056/event.html.

Loan Modifications

Given the complexity of loan modifications, vendors are often used to process loan modification requests under the Home Affordable Modification Program (HAMP). Vendors sometimes fail to process HAMP requests in accordance with their agreements with the bank. In other cases, vendors delay the processing of loan modifications by sending borrowers duplicate document requests, causing hardships for the borrowers. If bank management is not monitoring a vendor's activity, it will not be aware of problems that may be occurring with the vendor.

The failure to monitor vendors has resulted in significant examination findings, including concerns that borrowers were treated unfairly by the vendor. In one case, bank management was required to conduct a file search and offer borrowers whose request had been incorrectly handled by the vendor the option of re-applying for a loan modification. The bank had to absorb the costs associated with the new application and make significant changes to its compliance program.

Credit Card Administration

Some banks hire vendors to administer and market credit card programs. In one case, a vendor was marketing a balance transfer credit card program as a way for bank customers to obtain a new credit card while paying down the balance on an existing one. However, the vendor did not properly disclose all of the fees connected to the product. Bank management was not monitoring or reviewing the vendor's activities and did not identify the errors.

This action by the vendor ultimately resulted in a finding of deceptive marketing practices based, in part, on the vendor's failure to correctly disclose fees. Violations of Regulation Z's credit card requirements were also identified. In short, customers did not have all the information they needed about the product to make an informed decision and did not learn about certain features until after they had been assessed nonrefundable fees. Bank management assumed that the vendor was responsible for compliance because the vendor made the credit decisions and owned the credit card receivables. However, the bank's name was on the credit cards, and under the agreement between the parties, the bank was deemed a creditor in the transaction. The bank was therefore accountable for the compliance violations, not to mention the reputation risk of having its name associated with a deceptive practice. It is also noteworthy that the Consumer Financial Protection Bureau undertook three enforcement actions against three major credit card issuers this year, all of which involved compliance issues with vendors hired by the card issuers. The enforcement orders contained specific provisions requiring the issuers to change their compliance management systems concerning oversight of vendors.[4]

If bank management is not monitoring a vendor's activity, it will not be aware of problems that may be occurring with the vendor.

Disclosure Software

Many banks use vendor software to generate consumer disclosures for various loan and deposit products. After amendments to disclosure regulations in the last several years, some vendors failed to update their software, resulting in various errors on disclosure forms. Problems of this nature occur when bank management relies solely on the vendor without conducting its own independent review of disclosure requirements to ensure that the required changes are implemented.

Revenue Enhancements

Examiners are increasingly seeing cases in which third parties offer "revenue enhancement" services. While these services may appear desirable, bank management should always conduct due diligence with every vendor prior to entering into a third-party relationship, develop a risk assessment of the proposed vendor processes, and understand the vendor activities. Bank management must fully consider the compli-

[4] http://tinyurl.com/cfpb-EO1, pp. 22-23; http://tinyurl.com/cfpb-EO2, pp. 17-19; http://tinyurl.com/CFPB-Enf3, pp. 13-14

ance implications associated with these new products and services. In addition to complying with the technical requirements of existing rules, bankers should be particularly mindful of the possibility of UDAP issues related to vendor products. Generally speaking, management should ensure that marketing materials and disclosures are accurate and provide information necessary for the customer to make an informed decision about the product or service and that there are viable options available to the consumer.

BEST PRACTICES

Several best practices can reduce the risk of violations from vendor relationships. These include:

- *Due diligence.* Before selecting a vendor, bankers should conduct due diligence, which includes obtaining references, particularly from other financial institutions. In addition, the vendor's audited financial statements should be reviewed. Also, ensuring that the vendor has data back-up systems, continuity and contingency plans, and proper management information systems is also an important step. Finally, researching the background, qualifications, and reputations of the vendor's principals and the vendor's overall reputation, including lawsuits filed against it, should be part of the due diligence.
- *Risk assessment.* A detailed risk assessment should be developed based on the initial due diligence review. It should be provided to senior management and the board of directors prior to engaging in a new activity. The risk assessment should identify all categories of potential risk faced by a vendor's activity, including compliance, reputational, operational, credit, and transaction risks. It should also identify all applicable consumer laws and regulations to ensure compliance.
- *Clear contractual expectations.* Contract provisions should be based on identified risks, contain expectations for complying with applicable consumer protection laws and regulations, and contain the right to request information that demonstrates compliance, such as audit and monitoring reports. Important provisions that a vendor contract should address include but are not limited to:
    - the scope of outsourced services;
    - the procedures the vendor must follow;
    - the bank's service-level expectations;
    - the bank's approval of a vendor's use of subcontractors;
    - the bank's right to conduct audits or request third-party reviews;
    - the confidentiality of data;
    - the vendor's warranties, liability, and disclaimers;
    - dispute resolution mechanisms;
    - default and termination provisions; and
    - customer complaints and responsibility for responses.
- *Comprehensive monitoring program.* Risk-based monitoring derived from the risk assessment developed during due diligence is very important. The frequency and type of monitoring should be documented for each vendor. To conduct proper monitoring, staff must be trained and familiar with the vendor to ensure that they fully understand the risks and can conduct thorough monitoring. Monitoring of vendor performance should incorporate a review and tracking of consumer complaints related to the vendor's activities. Complaints are an excellent indicator of problems with a vendor. Finally, the risk assessment should be periodically updated based on the results of the vendor monitoring.
- *Board oversight.* Keeping the board of directors properly informed about the vendor management program is key to ensuring that they can provide proper oversight and that the bank's management process addresses the risks inherent in third-party relationships. The board should review the vendor management policy, due diligence reports, risk assessments, and monitoring results.

CONCLUSION

Vendors provide value in the expertise and experience they offer; however, financial institutions must still maintain active oversight. It is important to remember that when a vendor performs a service or function, the institution bears ultimate responsibility for compliance. Because varying levels of risk remain with the institution that offers the product or service, a strong vendor risk management program is key to maintaining compliance and avoiding claims of improper treatment of bank customers. With good vendor management, banks can minimize the risk of less direct oversight or control and maximize the benefits gained through a well-managed vendor relationship. Specific issues about vendor risk management should be raised with your primary regulator.

Resources

These resources focus on overall vendor risk management, UDAP risks from using vendors, and best practices for mitigating risk when outsourcing. Expectations for vendor risk management are part of every agency's agenda. Financial institutions should contact their primary regulator to understand its expectations for vendor risk management.

Federal Reserve Resources

Vendor Risk Management, *Outlook* Article, 2011
http://www.philadelphiafed.org/bank-resources/publications/consumer-compliance-outlook/2011/first-quarter/vendor-risk-management.cfm

Third–party service provider risk and the Unfair and Deceptive Acts and Practices rule, Retail Payments Risk Forum, Federal Reserve Bank of Atlanta, February 2011
http://portalsandrails.frbatlanta.org/third-party-service-provider/

Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks, Federal Reserve Bank of New York, October 1999
http://www.ny.frb.org/banking/circulars/outsource.pdf

Interagency Review of Foreclosure Policies and Procedures, Federal Reserve Board, April 2011
http://www.federalreserve.gov/boarddocs/rptcongress/interagency/interagency.htm

Other Agency Resources

FFIEC Guidance: Outsourced Cloud Computing, July 10, 2012: http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf

CFPB Bulletin 2012-2 on Service Providers: http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf

FIL 44-2008 – Third-Party Risks: Guidance for Managing Third-Party Risk
http://www.fdic.gov/news/news/financial/2008/fil08044.html

OCC Bulletin 2001-47 – Third Party Relationships: Risk Management Principles
http://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-47.html

CONTINUED FROM PAGE 3...

Error Resolution Procedures and Consumer Liability Limits for Unauthorized Electronic Fund Transfers

If the error involved an EFT that was not initiated within a state, resulted from a point-of-sale debit card transaction, or occurred within 30 calendar days after the first deposit into the account, the financial institution can take up to 90 calendar days, provided the conditions discussed above for extending the time period to 45 calendar days for other transactions are satisfied.[11]

After completing its investigation, a financial institution must:

- Correct an error within one business day after determining that an error has occurred; and
- Report the results of its investigation to the consumer (either orally or in writing, unless the institution concludes that no error or a different error occurred, in which case the results must be in writing) within three business days after completing its investigation.[12]

Procedures If No Error or Different Error Occurred

If a financial institution concludes that either no error or a different error than the one alleged occurred, the institution must:

- Include in the institution's report of the results of the investigation a written explanation of the findings and a disclosure of the consumer's right to request the documents upon which the institution relied;
- Upon debiting a provisionally credited amount:
  - Notify the consumer of the date and amount of the debit; and
  - Notify the consumer that the institution will honor checks (or similar instruments payable to third parties) and preauthorized transfers from the consumer's account — without charging overdraft fees — for five business days after the notification, provided that the items honored would have been paid if the institution had not debited the provisionally credited funds.[13]

If the consumer reasserts the error and the institution completed the initial investigation in compliance with the regulation, the institution has no further responsibilities to the consumer, except when a consumer asserts an error after receiving documentation requested under §1005.11(a)(1)(vii). See 12 C.F.R. §1005.11(e).

CONSUMER LIABILITY FOR UNAUTHORIZED EFTs: 12 C.F.R. §1005.6

If an institution concludes from its investigation that an unauthorized EFT occurred, a consumer can be held liable within the limitations described in §1005.6.

Conditions for Liability

The regulation does not permit an institution to impose liability on a consumer for an unauthorized transaction unless the institution previously provided the consumer with three disclosures required under §1005.7(b): a summary of the consumer's liability for unauthorized transactions, the telephone number and address of the person or office to be notified of an unauthorized EFT, and the financial institution's business days. In addition, if the unauthorized transaction involved an access device, it must be an accepted access device and the financial institution must have provided a means to identify the consumer to whom it was issued.[14] An access device becomes an accepted access device when the consumer: requests and receives, or signs, or uses the device to transfer money between accounts or to obtain money, property, or services; requests the validation of an access device issued without solicitation; or receives a renewal of, or substitute for, an existing accepted ac-

[11] 12 C.F.R. §1005.11(c)(3)(ii)

[12] 12 C.F.R. §1005.11(c)(1); Comment 1005.11(c)-1. Comment 1005.11(c)-5 states that an institution may include the notice of correction on a periodic statement that is mailed or delivered within the 10-business-day or 45-calendar-day time limits and that clearly identifies the correction on the consumer's account.

[13] 12 C.F.R. §1005.11(d)

[14] 12 C.F.R. §1005.6(a)

cess device from either the financial institution that issued the original access device or that institution's successor.[15]

Notice Requirements

A consumer's liability for unauthorized EFT depends on whether an access device is involved and when the consumer notifies its financial institution of the theft or loss of the device or the unauthorized EFT. The consumer's notice is effective "when a consumer takes steps reasonably necessary to provide the institution with the pertinent information, whether or not a particular employee or agent of the institution actually receives the information."[16] Consumers may give notice in person, by phone, or in writing.[17] Written notice is effective when the consumer mails the notice.[18]

Other rules regarding notification include:

Notice by Third Party. For purposes of the limitations on liability under §1005.6, notice provided by a third party on the consumer's behalf is valid.[19] A financial institution may require "appropriate documentation" from the third party to ensure that the person is acting on the consumer's behalf.

Constructive Notice. According to §1005.6(b)(5)(iii), notice can be provided constructively, regardless of when the consumer provides actual notice, "when the institution becomes aware of circumstances leading to the reasonable belief that an unauthorized [EFT] to or from the consumer's account has been or may be made."

Liability for Unauthorized EFTs Involving an Access Device

Regulation E establishes three tiers of liability for unauthorized EFTs involving an access device. The applicable tier depends on when the consumer learned of the loss or theft of an access device, when the financial institution received notice, and when the financial institution transmitted the periodic statement showing the first unauthorized transaction to the consumer.

First-Tier Liability ($50 Maximum): §1005.6(b)(1). If the consumer notifies the financial institution within two business days after learning that the access device was

Example 1: First-Tier Liability	
Monday	Consumer's debit card is stolen
Wednesday	Consumer learns of theft
Thursday	Unauthorized EFT of $100 (using debit card)
Friday	Consumer notifies financial institution of theft
Financial institution may not hold the consumer liable for more than $50 of the $100 transfer	

Example 2: First-Tier Liability	
Monday	Consumer's debit card is stolen
Tuesday	Unauthorized EFT of $35 (using debit card)
Wednesday	Consumer learns of theft
Friday	Consumer notifies financial institution of theft
Financial institution may hold the consumer liable for the $35 transfer.	

Example 3: First-Tier Liability	
Monday	Consumer's debit card is stolen
Tuesday	Unauthorized EFT of $35 (using debit card)
Wednesday	Consumer learns of theft
Thursday	Unauthorized EFT of $100 (using debit card)
Friday	Consumer notifies financial institution of theft
Financial institution may hold the consumer liable for only $50 of the total $135 in transfers.	

[15] 12 C.F.R. §1005.2(a)(2)

[16] 12 C.F.R. §1005.6(b)(5)

[17] 12 C.F.R. §1005.6(b)(5)(ii)

[18] 12 C.F.R. §1005.6(b)(5)(iii)

[19] Comment 6(b)(5)-2

lost or stolen, the financial institution may only hold the consumer liable for the lesser of (a) $50 or (b) the amount of unauthorized EFTs that occurred before the institution was notified.

Example 1: Second-Tier Liability[20]	
Monday	Consumer's debit card is stolen AND consumer learns of the theft
Tuesday	Unauthorized EFT of $100 (using debit card)
Thursday	Unauthorized EFT of $600 (using debit card)
Friday	Consumer notifies financial institution of theft. Bank's systems are set up to immediately freeze an account after notice of unauthorized EFT. If consumer had provided notice on Wednesday, the $600 transfer would not have occurred.
Financial institution may hold the consumer liable for $500, calculated as follows: • $50 of the $100 transfer, plus • $450 of the $600 transfer	

Example 2: Second-Tier Liability[21]	
Monday	Consumer's debit card is stolen AND consumer learns of the theft
Tuesday	Unauthorized EFT of $600 (using debit card)
Thursday	Unauthorized EFT of $100 (using debit card)
Friday	Consumer notifies financial institution of theft
Financial institution may hold the consumer liable for only $150, calculated as follows: • $50 of the $600 transfer, plus • Entire $100 transfer	

Second-Tier Liability ($500 Maximum): §1005.6(b)(2). If a consumer fails to notify the financial institution within two business days after learning that the access device was lost or stolen but notifies the institution of the loss or theft within 60 days of the financial institution's transmittal of the statement containing the error, the institution may hold the consumer liable for the lesser of (a) $500 or (b) the sum of: (i) the consumer's first-tier liability, i.e., the lesser of $50 or the amount of unauthorized EFTs that occur before the end of the second business day after the consumer learns of the loss or theft; and (ii) the amount of unauthorized EFTs that occur after the end of the second business day after the consumer learns of the loss or theft and before notice to the institution, provided the institution establishes that the unauthorized EFTs would not have occurred had the consumer provided notice within two business days after learning of the loss or theft.[22]

Third-Tier Liability (Unlimited): §1005.6(b)(3). If the consumer fails to notify the financial institution of the theft or loss within 60 days after the financial institution transmits to the consumer a periodic statement showing the first unauthorized EFT, the financial institution may impose liability on the consumer up to the total amount of all unauthorized EFTs occurring more than 60 calendar days after transmitting the statement and before notice to the financial institution, provided that the institution establishes that the unauthorized EFTs would not have occurred had the consumer notified the institution within the 60-day period. For unauthorized transactions that occurred *before* this period, the consumer is liable only to the extent that the banks could impose first- and second-tier liability under §1005.6(b)(1) and (2).

Extension for Extenuating Circumstances. Section 1005.6(b)(4) requires financial institutions to extend the time limits discussed above for each liability tier if the consumer failed to notify the institution because of "extenuating circumstances." When this occurs, the institution must extend the limits to "a reasonable period of time." Comment 6(b)(4)-1 of the

[20] Comment 6(b)(2)-1

[21] Comment 6(b)(2)-1

[22] 12 C.F.R. §1005.6(b)(2)

Example 1: Third-Tier Liability	
Jan. 1	Consumer's debit card is stolen AND consumer learns of the theft
Jan. 2	Unauthorized EFT of $100 (using debit card)
Jan. 6	Unauthorized EFT of $600 (using debit card)
Jan. 30	Periodic statement is transmitted showing unauthorized EFTs of $100 and $600
Apr. 10	Unauthorized EFT of $400
Apr. 11	Consumer notifies financial institution of theft
Financial institution may hold the consumer liable for $900, calculated as follows: • $50 of the $100 transfer, plus • $450 of the $600 transfer, plus • $400 of the $400 transfer	

Example 2: Third-Tier Liability	
Jan. 1	Consumer's debit card is stolen AND consumer learns of the theft
Jan. 2	Unauthorized EFT of $100 (using debit card)
Jan. 6	Unauthorized EFT of $600 (using debit card)
Jan. 30	Periodic statement is transmitted showing unauthorized EFTs of $100 and $600
Feb. 5	Unauthorized EFT of $400
Feb. 20	Consumer notifies financial institution of theft
Financial institution may hold the consumer liable for $500, calculated as follows: • $50 of the $100 transfer, • $450 of the $600 transfer, plus • $0 of the $400 transfer	

Official Staff Commentary lists hospitalization and extended travel as examples of extenuating circumstances.

Unauthorized EFTs Not Involving an Access Device: Comment 6(b)(3)-2

The consumer liability rules are slightly different when an unauthorized EFT does not involve an access device. Most important, the first two tiers of liability do **not** apply; that is, the institution may not hold a consumer liable for any portion of any unauthorized EFT not involving an access device that occurred on or before the 60th calendar day after the institution's transmittal of the periodic statement showing the first unauthorized EFT.[23]

Instead, an institution may only hold the consumer liable for an unauthorized EFT not involving an access device if the transfer occurred more than 60 calendar days after transmittal of a periodic statement showing the first unauthorized EFT out of the consumer's account and before the consumer gives notice to the financial institution, provided the institution estab-

Example of Liability for Unauthorized EFTs Not Involving an Access Device[24]	
Mar. 15	Consumer's account is electronically debited without authorization for $200
Apr. 2	Financial institution transmits periodic statement containing unauthorized EFT
June 2	Unauthorized EFT of $400 (61 days after periodic statement transmittal)
June 4	Consumer notifies the financial institution
Financial institution may hold the consumer liable for only $400 of the total $600 in transfers, calculated as follows: • $0 of the $200 transfer, and • $400 of the $400 transfer.	

[23] Comment 6(b)(3)-2

[24] Comment 6(b)(3)-2

lishes that the unauthorized EFT would not have occurred had the consumer notified the institution within the 60-day period.

Liability Under State Law or Agreement: §1005.6(b)(6)
If either a state law or the agreement between the financial institution and the consumer provides less liability than the provisions of §1005.6, the consumer's liability cannot exceed the limits under the state law or the agreement.

To facilitate compliance for the institutions it supervises, the Federal Reserve Board published the chart below summarizing circumstances in which the consumer has liability for unauthorized EFTs under Regulation E.[25]

CONCLUSION

Financial institutions should review and test their policies and procedures regarding error resolution investigations and consumer liability for unauthorized transactions to ensure that they comply with Regulation E's requirements. Specific issues should be raised with the Consumer Financial Protection Bureau or your primary regulator.

Summary of Consumer Liability for Unauthorized EFTs

Event	Timing of Consumer Notice to Financial Institution	Maximum Liability
Loss or theft of access device	Within two business days after learning of loss or theft	Lesser of $50 or total amount of unauthorized transfers
	More than two business days after learning of loss or theft up to 60 calendar days after transmittal of statement showing first unauthorized transfer made with access device	Lesser of $500 or the sum of: (a) $50 or the total amount of unauthorized transfers occurring in the first two business days, whichever is less, *and* (b) The amount of unauthorized transfers occurring after the two business days and before notice to the financial institution.
	More than 60 calendar days after transmittal of statement showing first unauthorized transfer made with access device	For transfers occurring within the 60-day period, the lesser of $500 or the sum of: (c) The lesser of $50 or the amount of unauthorized transfers in the first two business days, whichever is less, *and* (d) The amount of unauthorized transfers occurring after two business days. For transfers occurring after the 60-day period, unlimited liability (until the financial institution is notified).
Unauthorized transfer(s) not involving the loss or theft of an access device	Within 60 calendar days after transmittal of the periodic statement on which the unauthorized transfer first appears	No liability

[25] Federal Reserve Board, *Consumer Compliance Handbook*, Regulation E at 13, available at http://www.federalreserve.gov/boarddocs/supmanual/cch/efta.pdf

CONTINUED FROM PAGE 5...

HMDA Data Collection and Reporting

Rate Spread. For certain loans, the spread between the loan's annual percentage rate and the average prime offer rate for a comparable transaction must be reported ("rate spread loans"). A number of bankers have recently asked whether rate spreads are reported for withdrawn and/or rescinded transactions. In the case of a withdrawn application, there is no loan origination and no rate spread is reported (see Regulation C, Appendix A, §I.G.1.c, stating that "n/a" should be used). For loans that have been rescinded after closing, Comment 4(a)(8)-2 states that the institution may choose to report the transaction as either an origination (with the rate spread) or as an application that was approved but not accepted. If the institution chooses to report the rescinded transaction as "approved but not accepted," it reports "n/a" in the rate spread field.[16]

Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) Changes

The Dodd-Frank Act amended HMDA to require data that will better serve the purposes of HMDA. Section 1094 of the Dodd-Frank Act requires financial institutions subject to HMDA to collect new information about mortgage loans, including the following fields:[17]

- Age
- Application channel (i.e., broker)
- Credit score
- Loan originator identifier (SAFE Act)[18]
- Loan term
- Negative amortization
- Prepayment penalty term
- Property's parcel number[18]
- Property value
- Rate spread for all loans
- Term of introductory rate period
- Total origination points and fees
- Universal loan identifier[18]

and any other fields the CFPB may require.

Section 1094 states that institutions will not have to begin reporting the new HMDA data fields until January 1 of the year in which it has been at least nine months since the CFPB issued a final rule. As indicated in its rulemaking agenda,[19] the CFPB in the second quarter of 2013 expects to begin developing proposed regulations concerning the data to be collected and appropriate procedures, information safeguards, and privacy protections for gathering information under this section.

CONCLUSION

HMDA data enable regulators to assess how lenders are meeting housing needs, investing in their communities, and complying with anti-discrimination laws. It is therefore essential that these data be accurate and that the data fields provide a meaningful picture of the mortgage market.

Although HMDA changes are on the horizon, institutions should continue to rely on existing data reporting rules and guidance for ensuring compliance with reporting requirements. Specific issues and questions regarding the collection of HMDA data or other consumer compliance matters should be raised with the CFPB or your primary regulator.

Resources

Additional resources for HMDA data reporting are available on the *Outlook* website.

[16] See 2013 HMDA Edits, p. 7: "If action taken type = 2-8, then rate spread must = na." http://www.ffiec.gov/hmda/pdf/edit2013.pdf.

[17] These new fields were also addressed in the *Outlook Live* webinar titled *Tips for Reporting Accurate HMDA and CRA Data*, held on November 17, 2010. The presentation and PowerPoint slides are available at: http://tinyurl.com/hmda-cra.

[18] As the Consumer Financial Protection Bureau (CFPB) may determine to be appropriate

[19] The CFPB posted its semi-annual rulemaking agenda on July 16, 2012 at: http://www.consumerfinance.gov/blog/cfpbs-rulemaking-agenda/.

Consumer Compliance Outlook®

Ten Independence Mall
Philadelphia, Pennsylvania 19106-1574
www.consumercomplianceoutlook.org

ADDRESS SERVICE REQUESTED

PRESORTED STANDARD
U.S. POSTAGE

PAID

PHILADELPHIA, PA
PERMIT #7046

Calendar of Events

February 5-7, 2013	**Restoring Household Financial Stability After the Great Recession: Why Household Balance Sheets Matter** Federal Reserve Bank of St. Louis St. Louis, MO
February 17-20, 2013	**ABA National Conference for Community Bankers** JW Marriott Orlando Grande Lakes Orlando, FL
February 28, 2013	**2013 Banking Outlook Conference** Federal Reserve Bank of Atlanta Atlanta, GA
March 11-13, 2013	**CBA Live 2013: The Future of Money** Consumer Bankers Association JW Marriott Desert Ridge Phoenix, AZ
March 15-21, 2013	**ABA National Compliance School** Doubletree Hilton-Mission Valley San Diego, CA
April 11-12, 2013	**Resilience and Rebuilding for Low-Income Communities: Research to Inform Policy and Practice** Federal Reserve System Renaissance Hotel Washington, D.C.