Chapman and Cutler LLP

To the Point!

March 23, 2016 Legal, Operations and Strategy Briefs for Financial Institutions

Use of Property Evaluations

The OCC, the FRB, and the FDIC recently issued an advisory to clarify expectations for banks' use of property evaluations rather than appraisals to estimate a property's market value for certain real estate-related transactions. The advisory states that an evaluation is not required to be completed by a state-licensed or state-certified appraiser or to comply with the Uniform Standards of Professional Appraisal Practice. Property evaluations can be completed by a bank employee or by a third party.

Under the appraisal rule the following transactions do not require an appraisal, but do require a property evaluation:

- Transactions in which the "transaction value" (generally the loan amount) is $250,000 or less;
- Certain renewals, refinances, or other transactions involving existing extensions of credit; and
- Real estate-secured business loans with a transaction value of $1,000,000 or less and when the sale of, or rental income derived from, real estate is not the primary source of repayment for the loan.

Whether an appraisal or evaluation is used, it must contain sufficient information and analysis to support the value conclusion and the bank's decision to engage in the transaction.

A Bank Customer's Guide to Cybersecurity

The FDIC continues to focus on cybersecurity. Following up on its Winter 2015 Supervisory Insights, which included a discussion of the cyber-threat landscape and how financial institutions can enhance their information security programs to address cybersecurity risk, the FDIC has now published "A Bank Customer's Guide to Cybersecurity," a special edition of its Consumer News focusing on what consumers *and small businesses* can do, and what banks and regulators are doing, to prevent online fraud and theft (the *"Guide"*).

The Guide includes customer safety tips for online banking, steps to take to ensure mobile devices remain secure, and advice on how to avoid identity theft. It advises use of "strong" usernames and passwords for logging into accounts or conducting financial transactions (*i.e.,* passwords that include a combination of lower-case letters, upper-case letters, and symbols) and identifies the importance of maintaining up-to-date security software (including effective anti-virus programs), using a firewall to screen out unauthorized users, and ensuring that online transactions are conducted only with reputable businesses. Finally, the Guide points out the inherent risks customers accept in using public computers and wireless networks.

In the Guide, the FDIC summarizes customers' liability under federal law for unauthorized transactions using debit cards, credit cards, and prepaid cards. In addition, specific information is provided for small business owners, identifying their unique risks, including the inapplicability of federal law limiting liability for unauthorized transactions and the risks posed by employee access to a company's network and to its accounts.

Banks should become familiar with the Guide. It identifies a number of additional resources for customers, such as those specific to small businesses regarding cybersecurity issues. We believe the Guide could be a valuable resource for a bank in its efforts to educate customers in the role they can play in protecting their accounts against online fraud and theft.

Certain Prepaid Cardholders Treated as Customers for CIP Requirements

On Monday, March 21, the Federal regulatory agencies issued guidance (the *"Guidance"*) clarifying when prepaid cards and other prepaid access products are subject to the customer identification program (*"CIP"*) requirements set forth in Section 326 of the USA PATRIOT Act (the *"CIP Rule"*). The Guidance is effective immediately and describes the agencies' view that prepaid cards pose unique risks that make them vulnerable to criminal abuse, such as the potential for anonymous use and for high volumes of funds that flow through pooled prepaid access accounts.

A bank's CIP requirements must be applied to all prepaid products that create an "account" relationship as defined in the CIP Rule. The Guidance clarifies that prepaid cards should be treated as "accounts" for purposes of the CIP Rule if they provide a cardholder with (i) the ability to reload funds or (ii) access to credit or overdraft features. This includes prepaid cards sold and distributed by third-party program managers and prepaid access products offered through mobile phones or Internet sites that are used to access funds.

The CIP Rule requires banks to verify the identity of an accountholder when an account is established, including the accountholder's name, date of birth, address, and tax identification number. In the prepaid card context, the person who has the ability to add value to the card or to access credit features is treated as the bank's customer for purposes of the CIP Rule. Thus, when a prepaid cardholder has the ability to add value to a card or to access credit features, that person should be treated as the bank's customer—even if the cardholder obtained the card from an intermediary who uses a pooled account with the bank. In this scenario, the Federal regulatory agencies view the third-party program manager as the bank's agent rather than its customer, and the bank will be responsible for compliance with the CIP Rule even if the CIP verification of cardholders is performed by the third-party program manager. Where a prepaid cardholder does not have the ability to add value or to access credit, such as in the case of a payroll card where only the employer is able to deposit funds into the payroll account, the employer rather than the cardholder is treated as the bank's customer under the CIP Rule. The Guidance also describes how this analysis would be applied in the context of government benefit cards and health benefit cards, including health savings accounts (HSAs) and flexible spending arrangements (FSAs).

Banks partnering with third-party program managers are reminded to review their agreements and revise, if required, to (i) clearly define the role of each party in their contracts, including outlining the CIP obligations of each party; (ii) allow access to CIP information held by third-party program managers; (iii) provide audit rights for the bank; and (iv) provide the authority of the relevant bank regulatory body to examine the third-party program manager as a bank service company. Banks should be aware that prepaid cardholders that are treated as customers for purposes of the CIP Rule may also be customers for purposes of the Privacy Rule, which could increase banks' privacy compliance requirements.

Chapman and Cutler LLP

Attorneys at Law · Focused on Finance®

To the Point! is a summary of items of interest and current issues for financial institutions with primary focus on regulatory, consumer, and corporate issues. Chapman maintains a dedicated practice group with the experience to counsel on these issues and other enterprise risk management matters facing financial institutions. If you would like to discuss any of the items contained in these briefings or other legal, regulatory, or compliance issues facing your institution, please contact one of the members of our Bank Regulatory Group:

Marc Franson • 312.845.2988
Heather Hansche • 312.845.3714
John Martin • 312.845.3474
Scott Fryzel • 312.845.3784
Dianne Rist • 312.845.3404
Lindsay Henry • 312.845.3869