90 Day Note

November 2017 Vol. 31, No. 3

A Young & Associates, Inc. Publication

CECL: What's New, and What Some Community Banks are Doing

By: Tommy Troyer, Executive Vice President

I have been writing about CECL in this newsletter and providing CECL educational programs to community banks for several years. The overall theme I've tried to communicate in all of these settings has been: CECL is manageable for community banks, but it requires planning and preparation starting now.

I'm quite encouraged by the fact that the second part of that message, about the need to actively prepare for CECL now, seems to have been accepted by the majority of community bankers. In this article, I will provide a brief overview of a few noteworthy recent developments related to CECL, as well as some brief comments on what we are seeing from banks with respect to CECL preparation.

Regulatory FAQs Updated

On September 6, 2017, the federal financial regulators released an updated version of the interagency FAQs on CECL that were first issued in December 2016. All CECL FAQs are being consolidated into one document, so the most recent release includes both questions 1-23 from December and new questions 24-37. The information conveyed in the new questions is broadly consistent with the things I have tried to communicate in my articles and in my teaching about CECL and contains no surprises. This lack of surprises from the regulators is, of course, a good thing. I specifically recommend the expanded discussion in questions 28-33 regarding the definition of a Public Business Entity (PBE), as the PBE definition is a FASB concept that is fairly complex. The definition is important to understand because institutions can be PBEs without being "SEC Filers," and PBE status determines the effective date of CECL for an institution. Questions 34-36 also include some helpful and fairly detailed examples of how the transition to CECL should work for call reporting purposes for institutions in various situations with respect to PBE status and whether or not an institution's fiscal year lines up with a calendar year.

These are helpful clarifications since non-PBEs do not need to adopt CECL for interim periods, only for the year-end financials, in the first fiscal year of adoption and because call reports are completed on a calendar year basis irrespective of a bank's fiscal year.

FASB TDR Decisions

The final CECL standard has been in place and has been public for over 15 months at this point. CECL is not going to magically disappear before implementation, and there will not be substantial changes to CECL's requirements. However, there are still some decisions related to CECL that are being made by FASB, specifically through its Transition Resource Group (TRG), which exists to help identify potential challenges to implementing the standard as written. The TRG met in June and a number of issues were

(continued on next page)

Inside This Issue:

discussed, though many of the issues discussed are unlikely to have an impact on the average community bank. However, several issues related to Troubled Debt Restructurings (TDRs) were discussed and ultimately clarified by FASB in September. These issues are relevant to community banks and are worth noting.

The first decision that community banks should be aware of is one that will generally be viewed favorably by community banks. The issue at hand is that CECL requires estimating expected losses over the contractual term of loans and states that the contractual term does not include "expected extensions, renewals, and modifications unless [there is] a reasonable expectation" that a TDR will be executed. The issue FASB considered was just how expected TDRs should factor into an institution's allowance.

The options presented were, essentially, to estimate losses associated with some level of overall TDRs that you expect to have in your portfolio even though you don't know on what loans these TDRs might occur, or to only account for expected TDRs when you reasonably expect that a specific loan in your portfolio will result in a TDR being executed. FASB chose the latter option, which should prove to be much more manageable for community banks.

The second decision that FASB made is one that might generally be viewed less favorably by community banks. The CECL standard, when released, seemed to provide more flexibility around measuring expected losses on TDRs than current rules, which requires a discounted cash flow approach unless the practical expedients related to the fair market value of the collateral or the market price of the loan apply. The CECL rules essentially said that any approach to estimating losses on TDRs that was consistent with CECL's principles was acceptable. However, FASB ultimately decided that the cumulative requirements in the CECL standard and in existing accounting rules for TDRs require that all concessions granted to a borrower in a TDR be accounted for through the allowance. The brief summary of FASB's decision is that, in fact, a discounted cash flow approach to measuring the impact of TDRs will still be required under CECL in any circumstance where such an approach is the only way to measure the impact of the concession (the best example of such a concession is an interest rate concession). The TRG memo dated September 8 and available on FASB's website is a good resource for a more detailed discussion of the above issues.

"Nearly all banks have undertaken at least some educational efforts around CECL, and this is an area of focus that should continue through implementation and even beyond."

What Community Banks are Doing

What are some of your peer community banks doing to prepare for CECL? There does of course remain a wide range of preparation and some banks still haven't gotten started in any serious way. However, many banks have at least informally assembled the team that will work on CECL, and while not as many have adopted simple project plans as we might wish, many do at least have informal steps and deadlines in mind. Many have started giving thought to data availability and needs, though again perhaps not enough have yet gotten very serious about fully evaluating the data they have, how they will store and use it on an ongoing basis, and what additional data they would like to begin capturing. Nearly all banks have undertaken at least some educational efforts around CECL, and this is an area of focus that should continue through implementation and even beyond. Options for third-party solutions are being explored by some banks, though in order to make sure that an informed decision is made, it is critical that banks go into these explorations with a good fundamental understanding of CECL as well as with an awareness of the regulatory position that such solutions are perfectly fine options but are neither required nor necessary for CECL implementation.

How We Can Help

We have presented and will continue to present webinars, seminars, and talks on CECL. Please visit our website or call or email me for an overview of these sessions, which are specifically designed for the community banker and which are not designed to try to sell any particular software solution.

↓ *(continued on next page)*

Additionally, we are ready and willing to work with banks in a consultative role on CECL. Like everything else we do, there is no fee associated with an initial phone conversation or email exchange about CECL, and if we can help provide you with clarity about something related to CECL, then we are happy to do so. We are of course also happy to discuss various approaches in which we might provide consulting support in one or more capacities to assist your institution in preparing for CECL.

To discuss CECL further, contact Tommy Troyer at ttroyer@younginc.com or 330.422.3475. ❑

Network Vulnerability Management

Don't Be a Soft Target for Attackers

By: Mike Detrow, CISSP, Senior Consultant and Manager of IT

As the recent Equifax breach illustrates, failing to remediate known vulnerabilities in a timely manner can have significant consequences. In the case with Equifax, reports indicate that a patch was issued approximately two months prior to the May 2017 breach for the vulnerability that was exploited during this breach. While financial institutions have been quick to criticize Equifax for their vulnerability management practices, they should also take some time to evaluate their own vulnerability management practices and enhance them as needed to help prevent a breach at their own institutions.

"... an attacker may purposely go after a soft target like a community bank with poor vulnerability management practices that makes it easier to accomplish his or her mission."

During the vulnerability assessments that we perform for community banks, it is not uncommon to see systems that are missing patches that have existed for a year or more. While these are typically internal systems, this can still present a significant risk to the bank based on the role(s) of the affected systems. It should also be noted that vulnerability management for internal systems is as critical as ever, as attackers are able to use social engineering tactics to bypass perimeter controls such as firewalls and gain direct access to the internal network by compromising an employee's workstation. In addition, many community banks are only having vulnerability assessments performed on an annual basis, which means that a number of vulnerabilities may go undetected for nearly a year.

Community banks need to improve their vulnerability management practices to remediate vulnerabilities in a timely manner rather than allowing them to exist for months or even years. We often hear community bankers comment that they are too small to be the target of an attack, but they must also consider that an attacker may purposely go after a soft target like a community bank with poor vulnerability management practices that makes it easier to accomplish his or her mission.

Patch Management Vs. Vulnerability Management

Patch management is a significant aspect of vulnerability management, but patch management alone will not mitigate every vulnerability on the bank's network. An example of this is an internal server that houses reports from the core system and allows anonymous access, meaning that no username and password is required to access this data using a File Transfer Protocol (FTP) client. In this example, the server may be completely up-to-date with the latest security patches, but this insecure configuration may allow unauthorized access to the data on this system. Another concern is the systems and applications that may be missing from a bank's patch management program. We still see banks that are only performing Microsoft and limited third-party patching. Failing to patch the software on other devices such as ATMs, routers, switches, and printers will leave these devices vulnerable to attacks.

Developing a Vulnerability Management Program

The process to develop a vulnerability management program starts with a complete inventory of the devices connected to the bank's network. Even small

(continued on next page)

community banks now have a significant number of network-connected devices such as ATMs, DVRs, alarm panels, time clocks, and environmental monitors in addition to the commonly known devices such as workstations, servers, printers, and routers. During this step, it may be helpful for the bank's staff to scan the network with a network mapping tool to help identify devices that may not be included in the current network inventory. At a minimum, the inventory should identify the location, IP address, manufacturer, and model for each device. In the case of servers, workstations, and mobile devices, the bank must understand what applications are installed on each device to ensure that each application is patched in addition to the operating system.

The second step is to ensure that a comprehensive patch management program is in place at the bank. As noted above, a bank's patch management program may not currently include all network-connected devices. Special attention should be given to devices that are connected to the bank's network that are vendor-managed to ensure that the vendor has appropriate patch management procedures in place. Some examples of vendor-managed systems include: routers that are managed by the core system provider, DVRs, ATMs and alarm panels.

A comprehensive patch management program will include all devices that are connected to the network, and it will prescribe:

- A method to identify the availability of new patches that apply to the devices on the bank's network
- An evaluation and testing process for each patch
- A procedure to backup critical systems before installing a patch
- Timing for the installation of each patch based on its risk rating

The third step is to identify the vulnerabilities that currently exist on each device. This is most easily accomplished by performing a vulnerability scan on the internal network and against any internet-facing devices that are owned by the bank. The vulnerability scan can be performed by a consulting firm or the bank's staff can perform the scan using an automated vulnerability scanner.

There are typically two basic types of vulnerability scans that can be performed, credentialed and un-credentialed. A credentialed scan uses administrative credentials to log on to each device to perform a more in-depth evaluation of the vulnerabilities that may exist. An un-credentialed scan does not use credentials and therefore only identifies vulnerabilities that can be detected without logging on to each device.

The number of vulnerabilities identified by a credentialed scan will typically be significantly higher than those identified by an un-credentialed scan. It is important to note that if the bank only performs un-credentialed scans, the vulnerabilities that would have been identified by a credentialed scan will still exist on the network; they just will not appear in the un-credentialed vulnerability scan report. In addition, a credentialed scan will typically identify many privilege escalation vulnerabilities that an un-credentialed scan is unable to detect.

The results of the vulnerability scan will be provided within a report that the bank's staff or managed services provider can work through to install patches or make configuration changes to remediate the detected vulnerabilities. The vulnerability scan report will assign a risk rating to each vulnerability that is identified to help the bank's staff prioritize its response to each vulnerability.

As the bank's staff or managed services provider works through the list of vulnerabilities, a tracking process should be in place to identify the patches that are installed and configuration changes that are made to remediate each vulnerability. Once the tracking document identifies that all of the vulnerabilities are remediated, it is time to perform another vulnerability scan to verify that all of the previously identified vulnerabilities are remediated. If this is the first or most recent vulnerability scan, this process will help the bank's staff establish a baseline to work from as they continue to identify vulnerabilities and correct them.

(continued on next page)

The fourth step is to determine the frequency with which vulnerability scans will be performed. The scan frequency will be dependent on the size and complexity of the bank; however, based on the rate at which vulnerabilities are being discovered, a minimum scan frequency of once each quarter should be strongly considered. Monthly or even weekly vulnerability scans are highly recommended for more complex environments.

Summary

Once the steps listed above are complete, the bank should have established:

- A complete network device inventory that must be maintained as changes occur within the bank's network
- A comprehensive patch management program
- A schedule for performing automated vulnerability scans
- Procedures to review the vulnerability scan reports and remediate the identified vulnerabilities

As I mentioned in "The Changing Role of the Community Bank IT Manager" in last quarter's *90 Day Note*, community banks must adapt to the changing threat landscape and budget for additional information security resources. While some may view these additional expenses as unnecessary, they will most likely be miniscule in comparison to the costs associated with a data breach at the bank.

Young & Associates, Inc. can assist your bank with its vulnerability management program by performing quarterly or monthly vulnerability assessments to identify the vulnerabilities that exist on your network and recommend remediation procedures. Please contact Mike Detrow for more information about our vulnerability assessment services at mdetrow@younginc.com or 330.422.3447. ❑

CFPB Amends HMDA Rule

By: William J. Showalter, CRCM, CRP; Senior Consultant

The Consumer Financial Protection Bureau (CFPB) issued a final rule making several technical corrections and clarifications to the expanded data collection under Regulation C, which implements the Home Mortgage Disclosure Act (HMDA). The regulation is also being amended to temporarily raise the threshold at which banks are required to report data on home equity lines of credit (HELOC).

These amendments take effect on January 1, 2018, along with compliance for most other provisions of the newly expanded Regulation C.

Background

Since the mid-1970s, HMDA has provided the public and public officials with information about mortgage lending activity within communities by requiring financial institutions to collect, report, and disclose certain data about their mortgage activities. The Dodd-Frank Act amended HMDA, transferring rule-writing authority to the CFPB and expanding the scope of information that must be collected, reported, and disclosed under HMDA, among other changes.

In October 2015, the CFPB issued the 2015 HMDA Final Rule implementing the Dodd-Frank Act amendments to HMDA. The 2015 HMDA Final Rule modified the types of institutions and transactions subject to Regulation C, the types of data that institutions are required to collect, and the processes for reporting and disclosing the required data. In addition, the 2015 HMDA Final Rule established transactional thresholds that determine whether financial institutions are required to collect data on open-end lines of credit or closed-end mortgage loans.

The CFPB has identified a number of areas in which implementation of the 2015 HMDA Final Rule could be facilitated through clarifications, technical corrections, or minor changes. In April 2017, the agency published a notice of proposed rulemaking that would make certain amendments to Regulation C to address those

(continued on next page)

areas. In addition, since issuing the 2015 HMDA Final Rule, the agency has heard concerns that the open-end threshold at 100 transactions is too low. In July 2017, the CFPB published a proposal to address the threshold for reporting open-end lines of credit. The agency is now publishing final amendments to Regulation C pursuant to the April and July HMDA proposals.

HELOC Threshold

Under the rule as originally written, banks originating more than 100 HELOCs would have been generally required to report under HMDA, but the final rule temporarily raises that threshold to 500 HELOCS for data collection in calendar years 2018 and 2019, allowing the CFPB time to assess whether to make the adjusted threshold permanent.

In addition, the final rule corrects a drafting error by clarifying both the open-end and closed-end thresholds so that only financial institutions that meet the threshold for two years in a row are required to collect data in the following calendar years.

With these amendments, financial institutions that originated between 100 and 499 open-end lines of credit in either of the two preceding calendar years will not be required to begin collecting data on their open-end lending (HELOCs) before January 1, 2020.

Technical Amendments and Clarifications

The final rule establishes transition rules for two data points – loan purpose and the unique identifier for the loan originator. The transition rules require, in the case of loan purpose, or permit, in the case of the unique identifier for the loan originator, financial institutions to report "not applicable" for these data points when reporting certain loans that they purchased and that were originated before certain regulatory requirements took effect.

The final rule also makes additional amendments to clarify certain key terms, such as "multifamily dwelling," "temporary financing," and "automated underwriting system." It also creates a new reporting exception for certain transactions associated with New York State consolidation, extension, and modification agreements.

In addition, the 2017 HMDA Final Rule facilitates reporting the census tract of the property securing or, in the case of an application, proposed to secure a covered loan that is required to be reported by Regulation C. The CFPB plans to make available on its website a geocoding tool that financial institutions may use to identify the census tract in which a property is located. The final rule establishes that a financial institution would not violate Regulation C by reporting an incorrect census tract for a particular property if the financial institution obtained the incorrect census tract number from the geocoding tool on the agency's website, provided that the financial institution entered an accurate property address into the tool and the tool returned a census tract for the address entered.

Finally, the final rule also makes certain technical corrections. These technical corrections include, for example, a change to the calculation of the check digit and replacement of the word "income" with the correct word "age" in one comment.

The HMDA final rule is available at www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/regulation-c-home-mortgage-disclosure-act/.

Updated HMDA Resources

The CFPB also has updated its website to include resources for financial institutions required to file HMDA data. The updated resources include filing instruction guides for HMDA data collected in 2017 and 2018, and HMDA loan scenarios. They are available at www.consumerfinance.gov/data-research/hmda/for-filers.

For More Information

For more information on this article, contact Bill Showalter at 330-422-3473 or wshowalter@younginc.com.

For information about Young & Associates, Inc.'s newly updated HMDA Reporting policy, click here. In addition, we are currently updating our HMDA Toolkit. To be notified when the HMDA Toolkit is available for purchase, contact Bryan Fetty at bfetty@younginc.com. ❑

On November 13, 2017, Young & Associates, Inc. celebrated our 39th Anniversary. We would like to express our sincere appreciation to our valued clients and business partners with whom we have worked over the years, and look forward to establishing new relationships in the years to come.

ADA Website Compliance Notes from the Field

By: Mike Lehr, Human Resources Consultant

About this time last year, the topic of website accessibility and accommodation under Title III of the Americans with Disabilities Act (ADA) hit the community banking industry with full fury. Since that time both banks and service providers have upped their game. So, now is a good time for us to assess and share what we have learned in our ADA website audits.

There are two ways to assess sites. The more common and less expensive way involves scanning the site using software. Based on the logic coded into it, the software identifies potential issues. The second, less common, and more expensive way involves professionals or sight-impaired people using the site with a screen reader. A screen reader is software that converts a site page to text and reads it to the user.

Both ways involve a professional overseeing the process to interpret the results. Yet, something else drives both ways that tend to lead clients astray – measurability. The old adage of "what gets measured gets done" hits full force here. However, just because it's a number doesn't mean it's more important. We are finding that the software scan, because of its beautifully quantifiable graphics, is causing many of our clients to focus on minor, even insignificant aspects of their sites that have little to no impact on the site's overall accessibility.

In the end, if a bank ever ends up in court, it's not about software being able to access the site. It's about individuals with disabilities. Yet, it is much harder to quantify that into an eye-catching chart. For instance, a client called worried about their PDFs. The software scan showed them inaccessible. Moreover, they spent a lot of time trying to fix them. The nature of the documents were such that they required a professional printer. In short, it wasn't a Word document. Upon closer look, there were only a dozen of them. All but one were on the same page of the site. Furthermore, the page saw little traffic from customers and prospects. Plainly, the page wasn't important.

Yet, since bankers can be conscientious to a fault, it bugged them that these PDFs kept showing up "red" as an issue. By itself it's not bad. In context of the whole site though, it is. This was energy, time, and money diverted from far more important issues. One was whether a sight-impaired person can navigate the site. Software can't determine this. One can only determine this reliably by using a screen reader or by observing a sight-impaired person trying.

For instance, it's not uncommon these days to find sites that have multiple ways to navigate them. On one hand, you have the traditional horizontal navigation. On the other, you have the more recent mobile friendly navigation ("hamburger menu"). Still yet, some sites use vertical left-hand (or less common right-hand) navigation. That's three ways to navigate the site. We've seen these on a couple of sites already. This doesn't even include all the links and smaller menus that might be contained within the page.

Now, to a sight-impaired person, this is nothing but chaos. Keep in mind, a non-sight-impaired person can see the whole site at once. It's two-dimensional. He/she can select whatever menu they like. A sight-impaired person doesn't have this luxury. That's because a screen reader can only read one word at a time. It's a linear process, one-dimensional.

Also, he/she might tell the screen reader to only read navigation menus. So, if he/she starts hearing two or three different menus, it becomes hard to visualize in his/her mind how he/she might use the site. To a sight impaired person, they blend together as one. That's frustrating. It's also something else . . . inaccessible.

Yet, in most cases, as long as these menus are coded and tagged right, the software scan won't catch them. Moreover, and back to the original point about measurability, it's hard to quantify this user experience. The solution then is to code

(continued on next page)

one of these menus invisible to screen readers. Of course, that means the remaining one has to be comprehensive and robust.

In the end, it's a battle between easily measurable but unimportant PDFs and unmeasurable but important navigation. What gets measured gets done. Thus, the unimportant gets done and the important doesn't. That's why we can give compliance ratings to clients who still have issues on their software scans and non-compliant ones to clients whose scans show no issues.

In short then, invest in a screen reader. If not, partner with someone who has one. Banks can generate much goodwill by reaching out to groups and societies that support Americans with Disabilities. Remember, computers don't use sites. People do. People also testify in court.

For more information on this article or to learn how Young & Associates, Inc. can assist your bank with its ADA website compliance, contact Mike Lehr at 1.800.525.9775 or mlehr@younginc.com. ❑

Experiencing Difficulty Finding the Right Candidate To Meet Your Staffing Needs?

Executive Search and Recruitment Services

If your bank is finding it hard to identify and screen candidates to meet your staffing needs, consider Young & Associates, Inc. While we are qualified to help with all levels of staffing within your organization, we have more typically been called upon to help staff the following positions: President/CEO, Chief Financial Officer, Lending Officer, and Compliance Officer.

Specialists in the Banking Industry: Unlike many traditional search firms that do not specialize in staffing banking positions, Young & Associates, Inc. is very knowledgeable about the skills necessary to be successful in your banking environment. In addition, we will utilize our experts internally through the prescreening and interviewing process to verify skills, experience, etc.

Search Goal/Objective: Our objective throughout the search will be to provide you with 2-3 highly-skilled, thoroughly-screened, and motivated candidates to fill your opening(s).

Multiple Options: Our Executive Search Services provide a number of options, from resume generation to full placement, depending upon your needs.

Thorough and Effective: We will help you ensure the "right" candidate is sourced and referred to you by carefully and thoroughly prescreening and interviewing, verifying employment/work history, and obtaining 2-3 professional and/or character references.

Extensive Database: Through our long history working with banks, we have developed an extensive network of contacts and resumes of individuals interested in furthering their career(s). In addition, we can employ direct sourcing to banks and other financial institutions, as well as utilize internet advertising to generate additional qualified candidates.

Timeline: Once we begin the search and receive your commitment to staff your opening, we will work quickly and efficiently to staff your needs. Most searches can be completed in thirty to ninety days; however, in unique situations additional time may be necessary.

We truly value the opportunity to provide you with this highly specialized service. For additional information on our Executive Search Services, contact Sharon Jeffries at 330-422-3459 or sjeffries@younginc.com. ❑

Capital Planning System

Assess capital adequacy in relation to your bank's overall risk and develop a customized capital plan for maintaining appropriate capital levels in all economic environments. **Addresses the impact of growing cybersecurity risks, as well as the impact of the anticipated tax reduction from a capital planning perspective.**

Allows you to:

Develop a Base Case Scenario in which minimum capital adequacy standards are established.

Identify and Evaluate Risk for Your Bank. Parameters in this analysis have been field-tested in our work with banks over the years and closely resemble adequacy standards established in consent orders.

Stress Test Capital by loan classification (as recommended by the FDIC and OCC).

Perform Contingency Planning for stressed events. All assumptions are stressed to determine the amount of capital needed and possibilities for increasing capital are examined.

Generate Your Capital Plan in as Little as 1 Day! Data from the Microsoft® Excel spreadsheets can be easily transferred directly into a Word document that can be customized to fit the unique circumstances at your bank. Sample language and suggestions for changing the narrative are provided.

First Year License Fee (#304) – $1,095
Update/Annual License (#306) – $495

Customizable Bank Policies

Young & Associates, Inc. has developed over 95 practical bank policies designed specifically for the community banks that will ease the burden of developing bank policies from scratch.

- **Home Mortgage Disclosure Act Reporting (#119) - $195**
- **ADA General Accessibility Accommodations (#328) - $125**
- **ADA Website Accessibility Accommodations (#327) - $125**
- **Complete List of Available Policies – management/lending/compliance topics**

Updated HMDA Toolkit Coming Soon

To be notified when it is ready for purchase, contact bfetty@younginc.com.

Information Security Awareness Training Toolkit (#276) – $299

Designed to help your bank's Information Security Officer create a customized Information Security Awareness Training Program to educate bank employees on critical information security issues such as:

- Cybersecurity
- Intrusion Response
- Social Media
- Acceptable Use of IT Resources
- Workstation and Mobile Device Security

Includes:

- Training Script (provided in Microsoft Word)
- Customizable PowerPoint Training Presentation

Program Requirements: Training Script and Slides – Microsoft® Word 2007 and PowerPoint 2007 or higher

---

Threat Intelligence Program (#324) – $299

Includes:

- **Threat Intelligence Program:** Documents the requirements for the institution's threat intelligence program, including threat intelligence sources, the monitoring process, the analysis and response process, documentation requirements, and the reporting process
- **Threat Tracking Summary Worksheet:** Microsoft® Excel-based workbook for tracking threat notifications and responses
- **Threat Tracking Detail Worksheet:** Microsoft Word-based worksheet for tracking details about the threat analysis and response process performed for each specific threat
- **Information Systems Event Management Policy:** Policy template that documents the requirements for information systems event management procedures
- **Event Management Procedures for Specific Systems Worksheet:** Excel-based workbook for documenting the event management procedures for each information system

System Requirements: Microsoft® Word 2007 and Excel 2007 or higher