

Revisiting the “Red Flag Rule” and its impact on utilities



By Richard Heinemann
Boardman & Clark

Since their inception in 2008, the federal regulations that protect against identity theft, better known as the “Red Flag Rule,” have posed challenges to municipal utilities seeking to navigate between customer service and consumer protection requirements. Over the years, the Consumer Protection Bureau has tightened its enforcement of the Rule and periodically solicited public feedback, but the Rule has not been modified in any meaningful way. Unfortunately, the Rule can appear in some ways to conflict with the Public Service Commission of Wisconsin (PSCW) requirements for opening new customer accounts, particularly when it comes to obtaining appropriate forms of customer identification. MEUW members thus would do well to revisit both sets of rules to ensure they are compliant with both.

What is the Red Flag Rule?

Originally promulgated as an amendment to the Fair Credit Reporting Act, the Red Flag Rule requires certain “creditors” (which includes utilities) to develop written policies designed to detect, prevent and mitigate identity

theft in connection with opening and maintaining customer accounts (see C.F.R. Part 681 (2007)).

Under the Red Flag Rule, creditors who maintain a covered customer account must develop and implement an Identity Theft Prevention Program (ITPP) in connection with both opening new accounts and maintaining existing accounts. The Rule does not delineate the specific elements of the ITTP; instead, it gives creditors discretion to determine what elements make the most sense for their particular business.

The main substantive requirement of the Rule is that the ITTP must address four areas of concern: (1) identifying Red Flags for covered accounts; (2) detecting the Red Flags identified in the ITTP; (3) responding appropriately to any Red Flags that are detected; and (4) ensuring that the ITTP is periodically updated.

The Rule also imposes certain administrative requirements on the creditor, including the need to obtain proper authority for the ITTP, provide adequate staff training, and periodically review policies and procedures.

How the Rule Works

A “Red Flag” is a pattern, practice, or specific activity that indicates the possible existence of identity theft (16 C.F.R. sec. 681.2(b)(9)).

In order to identify relevant Red Flags, utilities have to identify the kinds of accounts they offer; the methods they use to open and provide access to those accounts; and their previous experiences with identity theft. For utilities, categories of Red Flags for covered accounts typically include notifications from credit reporting agencies; suspicious documents obtained from customers who open accounts; suspicious personal identifying information, unusual account activity, or notices of possible identity theft from law enforcement or customers themselves—in short, any pattern, practice or activity that suggests identity theft may have occurred with respect to a customer account.

To detect a Red Flag in any of these categories when opening new accounts, utilities can require certain identifying information and offer various means of verifying customer identity. Identifying information that the utility may want to require can include the customer’s name, date of birth, residential or business address, social security number, or the last 4 digits of the social security number, driver’s license or other forms of identification. For existing accounts, Red Flags can be detected by such activities as monitoring customer accounts, verifying customer IDs when information is requested,

verifying the validity of requests to change billing addresses, or verifying changes in banking information provided for billing and payment purposes.

Once a Red Flag has been detected, utilities can respond in a variety of ways, depending on the facts and circumstances of the detection. For example, if a utility becomes aware that its system has been compromised such that customer account information has been made accessible to third parties, the utility can notify the customer and change passwords. If the customer him or herself appears to have provided false information, the utility can opt to contact law enforcement.

Crucially, it is important to note that none of these actions, including the types of information the utility requires for new or existing accounts, are specifically required. So while some utilities may wish to require a form of photo ID, others may not. All that matters is that the utility itself determines and specifies the kinds of information it wants to require, and that it includes these requirements in a written policy that is properly authorized and appropriate for the particular creditor preparing the program. The MEUW has developed detailed guidelines and templates to assist members in developing and updating these policies.

Continued on page 12

Continued from page 11

Ensuring your utility's Red Flag Rule Complies with PSCW Customer Account Rules

The fact that the Red Flag Rule gives creditors discretion to customize their policies is key because such discretion ensures that utilities can develop policies that remain consistent with PSCW rules regarding customer applications.

Specifically, Wisconsin Admin. Code PSC 113.0408(c)2 (Code) provides that utilities shall accept certain forms of customer identification: a

driver's license number, state ID number, passport number, social security number or the last 4 digits of a social security number. The Code does not permit utilities to require multiple forms of identification for customer applications. So, if a utility wants to provide for additional safeguards in developing its Red Flag policy by requiring a second form of identification for new customer applications, it can only do so if it clarifies on the new customer application that the additional ID is optional.

In addition, the Code does not require new customers

to have a Wisconsin driver's license or Wisconsin ID card, so utilities cannot require that applicants have a Wisconsin ID or require extra forms of identification if the customer does not have a Wisconsin-issued ID. This should not present a problem with a utility's Red Flag policy since the Red Flag Rule does not specifically require creditors to obtain photo IDs when processing new applications. In fact requiring only the last 4 digits of a customer's social security number may be advisable at a time of increased cybersecurity threats.

Conclusion

MEUW members should review their existing Red Flag policies to ensure that they are compliant not only with Federal rules, but also with the Wisconsin Administrative Code. MEUW can be of assistance if members have questions about their policies. ●



Richard Heinemann provides legal services to municipalities and local governments

in Wisconsin and throughout the upper Midwest.