ARE YOU LEAVING MONEY ON THE TABLE?

Using Regulation E More Effectively Can Reduce Operating Losses

By Kelli Schoon-Saxsma and Heidi Wier, CrossCheck Compliance

As financial institutions shifted their attention to the onslaught of new regulations over the last few years, regulations such as the Electronic Funds Transfer Act (Regulation E), may not have been getting enough focus. Since the use of electronic payments has grown to an all-time high, a lack of focus or dedication of resources toward Regulation E and claims processing could lead to unintended errors, or even 'over compliance,' which may increase operating losses and leave money on the table.

Regulation E provides certain protections to consumers against an unauthorized electronic funds transfer (EFT) and provides guidance to institutions on how to resolve those disputed transactions or errors. An error as defined by the regulation at §1005.11(a) includes:

An unauthorized EFT transaction;

- An incorrect EFT to or from a consumer's account;
- An omitted EFT from a periodic statement;
- A bookkeeping or computational error made by the institution relating to an EFT;
- A consumer's receipt of an incorrect amount of money from an electronic terminal, i.e., ATM;
- A transaction that is not properly identified, i.e., on an ATM receipt, or on a periodic statement as required; and
- A consumer request for more information or documentation about an EFT transaction, including a request for information to determine if an error actually occurred.

A periodic review of the bank's procedures and practices for processing these transactions will help ensure that consumers receive prompt and accurate service, and save the bank money through efficiencies while complying with the related regulatory requirements. Below are some common practices that may help save money.

COLLECTING THE RIGHT INFORMATION UP-FRONT

An important aspect of processing an EFT error is ensuring bank employees are properly trained in the error resolution process which starts with the first consumer contact. It is important to train employees to ask the right questions and document the information. This will provide support in case the "story" changes and will help determine if the consumer is liable for any of the disputed transactions.

In addition to the typical questions around the consumer's identity, account information and the transaction(s) being disputed, consider whether the claim involves unauthorized activity with an access device, e.g., debit card or ATM card. Ask if the card was lost or stolen and when the consumer first determined that it was lost or stolen. Knowing when the consumer first noticed the card was missing will be useful later in determining if the consumer reported the information in a timely manner, and if the consumer is liable for any of the activity.

If the consumer alleges someone known to him has made unauthorized transactions, e.g., roommate, or friend, be sure to establish whether the consumer had ever given the card and/or PIN number to that person. If so, that person was actually authorized to use the card under the regulation, and therefore, the transactions are not considered unauthorized unless the consumer previously informed the institution that the individual was no longer authorized to use the card.

CHARGEBACKS AND MINIMUM THRESHOLDS

Establishing a minimum chargeback amount may reduce operating expenses. The merchant chargeback process allows the bank to require a merchant to investigate and refund any losses for fraudulent or disputed charges claimed by the consumer. Banks incur a fee to process chargebacks, and that fee, along with the time and resources it takes to process the claim, may not be worth the effort. By conducting a cost-benefit analysis of the chargeback process and time spent by employees, a bank may find that processing claims under a certain threshold costs more money than paying out the disputed item.

Additionally, a little research may also allow the bank to deny a claim without incurring chargeback fees. For example, if a consumer states he canceled a service ten days prior to the disputed transaction and was still charged, a quick visit to the merchant website may lead you to their terms and conditions that require cancellation within 30 days, and therefore, the claim can be denied without further processing.

INVESTIGATING LARGER CLAIMS AND AUTO-PAYING SMALLER CLAIMS

As stated previously it is important to conduct a cost-benefit analysis to determine if it is more cost-effective to pay claims under a certain amount without investigating them or going through the chargeback process. However, the reverse may also be true. Setting the threshold too high may also cost money. Some banks arbitrarily set a dollar threshold, below which they just pay the claim and do not bother to investigate it. Many small claims throughout the year can lead to significant operational losses. Be sure to conduct a thorough analysis to determine the desirable breakeven point.

CONSUMER LIABILITY

Another way to make sure the bank does not lose money on Regulation E error claims is to fully understand and take advantage of the constumer liability allowed by the regulation. The bank will also need to understand any zero liability agreements with debit card providers that may limit consumer liability.

Once an unauthorized EFT is confirmed, a refund may not be due to the consumer. Assuming the bank provided the required disclosures under §1005.7(b) of the regulation including a summary of the consumer's liability, who to notify in case of an error, your business days, etc., and that the activity involved an accepted access device such as an ATM card, there are three levels of consumer liability outlined by the regulation. Each level depends on when the consumer identified the unauthorized activity, when the consumer notified the financial institution and when the last periodic statement showing the activity was provided to the consumer. Understanding and properly executing on each of these levels of liability may help to reduce over refunding claims.

- $50 Maximum: If the consumer notifies the bank within two business days of determining an access device was lost or stolen, the consumer may be held liable for a maximum of $50.
- $500 Maximum: If the consumer learns that the access device was lost or stolen, but does not notify the bank within two business days, the consumer can be held liable for more of the transactions that would have been prevented if the consumer had notified the bank in a timely manner. Specifically, the consumer may be held liable for the unauthorized transfers that occurred after the close of two business days and before notice to the bank, provided the bank establishes that these transfers would not have occurred had the consumer notified the bank within that two-day period.
- Unlimited Consumer Liability: If the consumer does not notify the bank of unauthorized activity within 60 days after they received a periodic statement showing the first unauthorized EFT, the consumer may be liable for the total amount of all unauthorized activity that occurred more than 60 days after the provided statement, as well as the amounts determined in both the $50 and $500 levels above.

OVERDRAFT FEE WHEN REVERSING PROVISIONAL CREDITS

Another way the bank may be losing money is by honoring transactions and waiving overdraft fees on more items than necessary after investigating a claim. When an error claim is denied because the investigation showed that no error occurred, the regulation requires the bank to honor items and waive any related overdraft fees for five business days after providing notification of the denial. To prevent foregoing additional overdraft fees, it is important to send the notice out immediately. Additionally, the regulation only requires the bank to honor and waive fees for items that it would have normally paid if the provisionally credited funds had not been debited. Be sure that fees are not waived for items that would not have been honored regardless of the claim.

CONCLUSION

EFT usage, along with corresponding operational losses, are on the rise. A robust set of procedures, periodic training of both front line and operations personnel, and periodic monitoring of these processes can help to ensure a solid understanding of the regulatory requirements without "over complying" or leaving money on the table.

About the Authors: ***Kelli Schoon-Saxsma*** *is a manager with CrossCheck Compliance, kschoon-saxsma@crosscheckcompliance.com.* ***Heidi Wier*** *is a managing director with CrossCheck Compliance, hwier@crosscheckcompliance.com. Both authors can be reached at 312 346-4600.*
IBA ASSOCIATE MEMBER