

## **Be Sure to Timely Remit Employee 401(k) Contributions**

The Department of Labor's (DOL) participant contribution regulation require that participant contributions to a 401(k) plan be deposited to the plan on the earliest date that they can be reasonably segregated from the employer's general assets, but in no event later than the 15th business day of the month following the month in which the participant contributions are deducted from their pay. However, this does not mean an employer can routinely wait until the 15th business day to deposit the funds. The 15th business day is not a safe harbor. Rather, the general rule is that the deferrals be deposited as soon as is reasonably possible after payday. If the employer can segregate and deposit the contributions prior to this deadline, they must do so.

However, the DOL issued an amendment to the participant contribution regulation to create a safe harbor rule under which participant contributions to small plans (with fewer than 100 participants) will be deemed to be made in compliance with the law if those amounts are deposited with small plans within seven business days of withholding or receipt.

## **Are You Compliant with the New Credit Card Rules Yet?**

You undoubtedly have heard about the new "chip cards," and you may recall from earlier newsletters our discussion about the cards and terminals. It's important to remember that October 1, 2015, was the deadline for what the credit card industry calls a "liability shift." This means that as of October 1, how liability falls between credit-card issuers and merchants shifted. Merchants that have not updated their credit card terminals to chip terminals are now liable for any fraudulent transactions, not the bank that issued the card.

The new chip-enabled cards, which are also called EMV cards, are being phased in because they're more secure than the old-style magnetic-strip cards. If someone attempting fraud with a chip card would hit a chip terminal, the merchant is protected from charge-backs by the card issuer. But if the merchant is still using an older magnetic strip reader, the liability for charge-backs falls on the business.

### **What it Means for Your Practice**

If you are not yet compliant with a new machine, then you are in good company. As of March 30, 2016, studies showed only 37% of merchants were equipped to accept chip cards. As for your practice, while it's conceivable that some new patients might be crooks, it's probably not likely patients will use a phony credit card to pay for, say, a dental procedure. You also were not required to take immediate action; this was not a deadline by which you had to act, only the deadline for the liability shift. Patients can, for now, still use the magnetic-strip cards at your risk.

However, there is no sense in taking on a new risk when there is no offsetting benefit, and you should upgrade your terminal as soon as possible.

Additionally, the new standards will eventually become widely adopted and required, at which point the Payment Card Industry Security Standards Council (PCI) will likely start imposing annual fines on non-adopters.

**Connect with PPG  
Partners Online!**



twitter.com/  
PPGPartners



facebook.com/  
PPGPartners



linkedin.com/  
company/ppg-  
partners-llc

## Office Hours Changes Can Help Working Patients

A change from traditional office hours has proved popular with patients, staff and physicians at many practices. It can be difficult for people to get time off work to visit the doctor, and too many such absences can even endanger their jobs.

Consider coming up with a schedule to accommodate patients. While doing so, also make sure that the schedule doesn't create excess overtime for staff.

### *A possible schedule could include:*

1-2 extended hours days  
1 early leave day\*  
1 Saturday a month  
3 "regular days"

*\*While a short Friday is usually welcomed by staff, you may want to avoid this, as Friday afternoons are often the best times for working patients to schedule appointments.*

### *A sample schedule:*

Monday: 7:30 AM-6:30 PM  
Tuesday: 8:00 AM-5:00 PM  
Wednesday: 8:00 AM-5:00 PM  
Thursday: 8:00 AM-2:00 PM (no leaving for lunch)  
Friday: 8:00 AM-5:00 PM  
Saturday (once a month): 8:00 AM-2:00 PM

## IRS Warns of New Scam Variations

Scammers are trying new tactics to convince taxpayers to hand over their personal information, the IRS warns. In a new email scam targeting taxpayers, people are receiving emails that appear to come from the "Taxpayer Advocacy Panel." They try to trick taxpayers into providing personal and financial information. You should not respond or click the links in these emails. If you receive an email that appears to be from TAP regarding their personal tax information, forward it to [phishing@irs.gov](mailto:phishing@irs.gov).

The IRS has seen an approximate 400 percent surge in phishing and malware incidents in the 2016 tax season. The emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. The phishing schemes can ask taxpayers about a wide range of topics. Emails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information.

The IRS said it is also receiving new reports of scammers calling under the guise of verifying tax return information over the phone. The latest variation on this scam uses the current tax-filing season as a hook. Scam artists call saying they are from the IRS and have received the taxpayer's tax return, and they just need to verify a few details to process it. The scam tries to get taxpayers to give up their personal information such as a Social Security number or personal financial information, such as bank numbers or credit cards.

Aggressive and threatening phone calls by criminals impersonating IRS agents remain an ongoing threat. The IRS said it has seen a surge of these phone scams in recent years as scam artists threaten taxpayers with police arrest, deportation, license revocation and more. The con artists often demand payment of back taxes on a prepaid debit card or by immediate wire transfer. Taxpayers should be alert to con artists impersonating IRS agents and demanding payment.

The IRS will never call to demand immediate payment over the phone or call about taxes owed without first having mailed a bill, nor will it threaten to immediately bring in local police or other law enforcement groups to have a taxpayer arrested for nonpayment. The IRS also will not demand payment of taxes without giving the person the opportunity to question or appeal the amount owed or require the use of a specific payment method for taxes, such as a prepaid debit card. The IRS will not ask for credit or debit card numbers over the phone or threaten to bring in local police or other law enforcement groups to have someone arrested for not paying.