Cash/Mobile Apps Use According to the State Auditor

Email from February 15, 2023

Regional Directors and County Directors,

In the past 2-3 weeks, we've had a couple of counties ask about cash/mobile apps and if they can be used. We know the Auditor's Office has shared their concerns in the past, even referencing them as a red flag in a training video to elected officials that manage public funds. I revisited the issue with them and they listed their concerns below.

1. If the vendor (Venmo/Paypal/cash app or mobile payment) sets up their own internal account that your funds stay on deposit with until action is taken to move them to your bank (which could be for an unlimited amount of time) that is circumventing fiscal policy and Iowa Code 12C on official depositories. In effect, those funds are off-books, not in an official depository, not a part of the balance sheet and difficult to track. (She noted that unlike cash/mobile apps, typical credit card/merchant processing companies will batch payments once per day and are automatically deposited into your bank account - that frequent and automatic activity is in compliance.)

   Many cash apps allow for deposits held in their accounts to also be spent using their app. Those transactions are never included in a voucher report or carried to the balance sheet. Some companies (PayPal for Business, for example) will even send a plastic debit card to you to (unsolicited) to use to access those funds that they have on account. The auditor strongly objected to allowing funds to be held and then spent off-books and outside of an auditable accounting system, and noted that debit cards should not be allowed since they circumvent the council approval process.

2. According to the auditor's office, there is significant risk in using cash apps and mobile payment in regards to setting up similar accounts with the same name. A individual can set up a near identical account and call it "XX County Extension" or "@XXCoExt" and payees would think the payment is going to an "official" entity. Even staff using the app (but not a part of the setup) would think they are using a legitimate account, or could inadvertently direct people to use an unofficial account. Your customer that used the app to pay you wouldn't be able to tell the difference on their statement, since the name would appear legitimate.

   Furthermore, the auditor specifically cited an example of how a legitimate account can be set up, however, the bank account connected to it for deposit can be easily changed to an unauthorized bank account (and even changed back) making it difficult to catch any missing transactions/deposits. This is because the bank account information can be changed by anyone with the login information, and often those types of accounts are targeted by scammers to change the account information. She noted that this is even a concern for some merchant processors like Square.

   She went on to describe that depending on assigned responsibilities, the individual collecting payments could also manipulate related records so that any diverted collections would not show in a reconciliation. For example, a staff member could redirect collections to an unauthorized bank account, then record legitimate payments collected during that period as "credit memos" or "adjustments" in the district's accounting system if she/he also had access to that system. Because a payment would not be recorded, a reconciliation would not catch it. If a true, timely reconciliation is not performed, any irregularities would not be caught.

   In contrast, typical credit card/merchant processing companies have much stricter requirements to set up account, verify officers or guarantors, and provide fraud protection.

The auditor recommends with the quickly changing landscape of how electronic payments are evolving, we need policies and procedures to prohibit or protect against risk. Some risk could be accepted by a county office, however, it would require reconciliation of the daily activity be performed along with an independent

review. The auditor was not comfortable with making any recommendations currently since they have not found a secure cash/mobile app vendor to date.

In the end they recommended reviewing requests for implementing electronic payments on a case-by-case basis and to consider depository and reconciliation risks very closely before changing practices.

Although the conversation with the auditor's office did not include discussion about insurance, I would caution moving forward with a cash/mobile app if you as the individual are the responsible party. Cash/mobile apps often require an individual to setup an account before you can connect a business. This may make sense for a small business, but it would not work well with government (or even corporate) accounts. You may in effect be making yourself the guarantor and you may be operating outside of what liability coverage for the office can cover since it would be your account on your own personal insurance.

Many things to think about. I appreciate this group for asking questions to keep us up to date on current trends. Reach out if you have more questions in the future.

Andrea

Andrea R. Nelson | **County Services**
Iowa State University Extension and Outreach
Assistant Vice President

2280 Beardshear
515 Morrill Road
Ames, Iowa 50011
nelsonar@iastate.edu
515.294.0013
www.extension.iastate.edu/countyservices

IOWA STATE UNIVERSITY
Extension and Outreach