Office of Inspector General
Legal Services Corporation

The Fraud Corner

(4/1/2020)

Third Party Payment Services

As part of its Fraud Corner series, the Office of Inspector General (OIG) is providing Legal Services Corporation (LSC) grantees with the following best practices to aid you in preventing and detecting thefts through third party payment (TPP) services. This article provides guidance on risk factors relating to TPP service thefts and measures employees can take to prevent and detect such thefts.

Millions of individuals and businesses use TPP services (or "mobile payment platforms") to make and share payments with friends, family, and businesses. TPP vendors like PayPal, Venmo, and Apple Pay allow payments to be moved electronically between users' accounts via a mobile or desktop application. Once the funds are transferred to a user's account, it is up to that account holder where and when to further transfer the money.

LSC grantees are using TPP services to accept donations and receive private attorney payments, as well as for continuing legal education classes, background check services, and other transactions. Although TPP services are convenient to use, they also pose serious risks for abuse which could lead to the theft of grantee funds. During OIG field visits several grantees have raised questions about the proper handling of TPP transactions and their potential financial impact on grantee programs.

Fraud Risks

In most cases, the person opening a TPP account controls all access to it and will have sole discretion to transfer funds into any other account. The account opener's sole authority to control account access and transfer funds between accounts may give rise to a serious risk to grantees. So long as the TPP funds remain in a transitional account, the account holder can direct payment to any vendor for personal financial gain without his or her employer's knowledge.

On one grantee visit the OIG noted that when grantee senior management opened a TPP account, employees were given access to it in order to transfer funds for deposit

into the grantee bank account. Unfortunately, such a practice may open the grantee up to a fraud risk. Without proper controls, employees could transfer funds meant for the grantee into their personal accounts or into other accounts not associated with the grantee. In the absence of effective grantee policies and internal controls, such fund transfers may go unnoticed or appear to be legitimate payments for vendor invoices.

Fraud Prevention

To prevent employee theft schemes involving TPP services, the OIG recommends LSC grant recipients:

1. Use unique usernames and passwords for TPP accounts;
2. Use the same security precautions with a TPP account as you would with an online banking account;
3. Ensure a proper segregation of duties over a TPP account and require at least two employees to co-manage it in order to maintain checks and balances;
4. Do not provide the account credentials to more employees than necessary;
5. Ensure employee user privileges and account access privileges do not exceed those necessary for employees to carry out their roles;
6. Only log in to a TPP account from a trusted internet connection;
7. Never enter your password, bank account, or credit card number unless you are on the TPP service login page;
8. Set up multifactor authentication to verify all financial transactions;
9. Use reliable security software, preferably software that includes an anti-phishing feature;
10. Always conduct background checks on potential employees under consideration for positions of trust with fiscal responsibilities;
11. Request and review monthly account transaction reports for any TPP account your organization maintains to ensure funds due the program have been recorded in the proper grantee account(s), and retain all statements for future audits either in hard copy or PDF;
12. Determine whether any funds in your program's TPP account(s) were used to pay financial obligations you cannot recognize or identify;
13. Secure access to any electronic device(s) used to input credit card payments to the grantee (and place them in a locked cabinet when not in use);
14. If money mysteriously appears in your TPP account from an unknown sender, do not send it back;
15. Do not permanently link your TPP account to your bank account or debit card (if you link your TPP account to your credit card you will usually have 60 days to refuse charges, whereas you may have only two days to refuse a fraudulent TPP charge on your program's bank account);
16. Immediately report any TPP service theft or malfeasance to the TPP vendor, the Federal Trade Commission, and the LSC OIG.

If you have any questions or comments or would like additional information about this post please contact Daniel O'Rourke, Assistant Inspector General for Investigations at the LSC OIG, (202) 295-1651, or by email at dorourke@oig.lsc.gov.