Los Angeles County Office of Education

INFORMATIONAL BULLETIN # 5354

9300 Imperial Highway, Downey, California 90242-2890 • (562) 922-6111

Debra Duardo, M.S.W., Ed.D., *Superintendent*

April 9, 2021

TO: Business and Accounting Administrators
Los Angeles County K-12 School and Community College Districts
Regional Occupational Centers/Programs (ROC/Ps),
Other Local Educational Agencies (LEAs), and Selected Charter Schools

FROM: Sachiko Enomoto, School Accounting and Finance Manager
Jenny Zermeño, Disbursements and Financial Systems Manager
Division of School Financial Services

SUBJECT: Urgent Warning Regarding Processing Requests to Change Electronic Funds Transfer (EFT) Vendor Setup

On May 6, 2020, the Division of School Financial Services (SFS) issued Bulletin #5213 *Electronic Funds Transfer (EFT) Vendor Setup Warning*, highlighting the increase in unauthorized personnel posing as vendor contacts and **emailing** school districts requesting changes to EFT vendor account information. Included in the bulletin were suggestions noted to mitigate risk of fraudulent transactions.

The purpose of this bulletin is to remind District business staff to be cautious in processing requests for vendor setup and changes. It is crucial that Districts are wary of any unsolicited communication of this nature and are strongly encouraged to develop procedures for authenticating all EFT requests before entering/changing information in either PeopleSoft Financial System (PSFS) or BEST Advantage Financials (FIN). This is necessary to ensure safeguarding of public funds.

Business Email Compromise (BEC) is an electronic scam to obtain confidential, personal or financial information from the Districts through email. The following are examples of BEC that the Los Angeles Treasurer and Tax Collector (TTC) has provided:

- **Email Spoofing/Masking** – A spoofed/masked email that contains a forged email header that hides the true origination of a message. Scammers will trick District employees into divulging sensitive information and/or initiating payments based on fraudulent instructions.
- **Client Email Compromise** – Scammers compromise an employee's email at the District, often referred to as account takeover or hacking. Scammers leverage access to an email account or District's network to gain an understanding of the communication style, and ultimately send an email to an employee with fraudulent payment instructions.
- **Vendor Email Compromise** – Scammers impersonate a District's vendor rather than a District's employee. A vendor's client (the District) receive requests with updated accounts, then send funds to what is believed to be a valid account from their trusted vendor.

- **Lookalike Domain** – Scammers purchase/register a domain closely resembling that of a legitimate company, then set up a related email account to target the victim District. Victim Districts' employees often do not notice the difference between their legitimate corporate domain and the lookalike, which is very similar visually.

The following are additional best practices that should be considered for implementation:

- Train employees who process payments to properly verify by calling a known contact on file with the district for all payment account changes rather than solely reply to email instructions
- Consider available email security solutions to defend against lookalike domains
- Enable controls so all emails from outside your District are marked as external
- Train all employees on suspicious email trends and have the District's technology unit send test e-mails regularly
- Consider signing up for the LA County Early Warning Service to additionally verify a payment account number. Please contact Sachiko Enomoto if interested.

Initial Steps Taken When District Discovers that a Fraudulent EFT/ACH Transaction Occurred:

1. Immediately contact SFSBanking@lacoe.edu and SFSAccountsPayable@lacoe.edu to alert SFS of the fraudulent ACH transactions that has occurred.
2. Districts should file a police report with their local police.
3. SFS staff will continue communication with the District to request information needed in order to make efforts to recover the funds.
4. SFS staff in partnership with TTC will make recovering efforts for the funds lost.

NOTE: Although every effort will be made to recover the funds lost, there is no guarantee that any of the funds will be recovered. If a district experiences a fraudulent incident, it may then be required for LACOE to review and approve any future vendor account changes.

For more suggestions on security set-up procedures, please see Bulletin #5213 *Electronic Funds Transfer (EFT) Vendor Setup Warning*.

If you have any questions regarding this bulletin, please feel free to contact Sachiko Enomoto at (562) 922-6191 or via e-mail at Enomoto_Sachiko@lacoe.edu or Jenny Zermeño at (562) 940-1649 or via e-mail at Zermeno_Jenny@lacoe.edu.

Approved:
Nkeiurka Benson, Director
Division of School Financial Services

SE/JZ:lt

SFS-A44-2020-2021