



Don't Fall Prey to EFT Fraud

There has been a substantial increase in Electronic Funds Transfers (EFT) fraud attacks recently, especially through social engineering. Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. During the pandemic environment, in which much of our business is now conducted on-line, social engineering acts of manipulating someone to “voluntarily” electronically send a perpetrator money are increasing in size and frequency. These EFT fraud attacks often start with a phishing email or phone call to check if the unsuspecting

Sample Incident

Acme Construction is a known vendor performing modernization and construction projects for your district. You make regular large wire transfer payments to ACME. The ACME CEO, John Brown, calls you stating his bank account has been compromised so he is opening a new account and requests future payments be sent to it. You tell Mr. Brown he must complete an EFT form from your district's website. It is completed and submitted during the call. Mr. Brown even cc's your district's CBO in the email. Soon you receive an email from the CBO approving the change. You make the change in the system. Next month, Mr. Brown calls your office stating he never received last month's payment. Upon investigation, you discover that the real John Brown never called. That was a fraudulent caller who provided fraudulent routing information using a similar, but false email address. The email from the CBO was also from a false, but very similar, email address.

- Implement a two-factor authentication process to approve any financial transaction changes by having a second staff person call to verify changes.

Continued on page 2



Simplifying Access to Mental Health Resources

The COVID-19 pandemic has introduced new financial and emotional stresses for many employees, students and their families, and connecting individuals with appropriate mental health resources in a timely way can be confusing. In response, ASCIP is offering Care Solace, a concierge service that provides a single point of contact for local mental health, substance abuse and counseling programs. Care Solace screens local behavioral health providers for quality and availability, helps families determine insurance coverage, and facilitates access to care.

Behavioral health provider access is available 24/7 by contacting the Care Solace team via phone or their website. The program includes training for school psychologists, counselors, and HR staff. The team of care coordination experts guides and supports district students, staff and families through the entire process including identifying appropriate resources, navigating insurance coverage, and even scheduling appointments. ASCIP has negotiated a discounted rate of \$2.00 per student per year for this valuable program. To get started contact Dan Sanger at (562) 677-2032 or sanger@ascip.org.

individual will “take the bait”. EFTs include Automated Clearing House (ACH) transactions, wire transfers, electronic checks, credit/debit card payments and payroll direct deposits. These fund transfer methods are fast and generally safe to send and receive payments. The danger comes in the act of setting up and making changes to the bank account information for each of these.

Tips to Avoid EFT Fraud

- Beware if someone says they need to change the way they receive payments due to the current pandemic. Everyone has adapted to this pandemic and can still both issue and receive checks. Occasionally remind vendors and staff that your organization will never ask for any financial or personal data via email.

WHAT'S NEW AT ASCIP?

New Resources:

- Remote Instruction & Keeping Students Safe Guidelines
- Special Ed Class Action-Risk Alert
- Musical Instrument Handling – COVID Resource
- Don't miss the [Reopening Schools Planner](#) to guide you through the process

Welcome New Members!

Effective Oct 1, 2020 participating in ASCIP's FSA administration services:

- CODESP
- Rosemead SD

Welcome New Staff!

- Heidi Cisneros - *Student Safety Advocate*
- Carly Weston - *Sr. Risk Services Consultant*

Go to www.ASCIP.org for all this and more!

INSIDE

Don't Fall Prey to EFT Fraud.....1

Simplifying Access to Mental Health Resources.....1

What You Should Know About Handling Lawsuits and Claims.....2

Upcoming Events2

EFT Fraud *continued from page 1*

- Never reply to an email request to change banking information, even if it looks like it's coming from someone inside your entity. Always call the requestor using your known contact information (not the contact information in the email).
- Implement dual control when actually processing any EFT transaction by requiring that at least two people are involved in the process.
- Always perform a validation transfer (or test deposit) with a blind confirmation.
- Always require a signed Form W-9 from every new payee in advance of making any payments. Also require this if they are changing their mailing address. You can confirm this information online or directly with the IRS.
- Implement Positive Pay for both checks and ACH transactions, as well as placing an ACH Debit Block on your accounts.

ASCIP SECURITY ALERT!

No one from ASCIP will ever ask you to pay via a wire or ACH transfer. ASCIP only accepts payments via check or LACOE account transfer.

If Finance, HR and IT staff seem a bit cynical at times, there is good reason - they are the guardians of your entity's financial resources. They take seriously the Russian proverb quoted often by President Ronald Reagan regarding a certain nuclear arms treaty "Trust, but verify."

ASCIP will be publishing a series of tips to help keep members' financial operations safe. Watch for the next in our series, "What's on the Cyber Menu – Spam or Phish?"

What You Should Know About Handling Lawsuits and Claims

Service of Lawsuit

- **Do not waive in-person service.** Individuals and agencies named as defendants have a specific time limit to respond to lawsuits. The response

time is triggered once the lawsuit has been "properly" served. Proper service is when the lawsuit is *handed* to the named defendant or its designated representative if the defendant is a school district, college or other entity. A cost and time saving tactic that Plaintiff attorneys are using is to serve lawsuits upon defendants via email and asking districts to "waive" the in-person service requirement due to COVID-19. ASCIP recommends districts and individuals do not waive the in-



person service requirement.

- No action needs to be taken on a lawsuit until it is "properly" physically served upon the District (leaving a lawsuit on a counter in the District office is not proper service).

Reporting P&L Claims

Notify ASCIP immediately of:

- **Any claim or lawsuit** even if the lawsuit was not properly served.

ASCIP P&L Claims Reporting

Email claims and backup to:

claims_info@ascip.org

Noel Waldvogel, Claims Manager –
Office: (916) 245-3523
For emergency after hours call –
Cell: (916) 591-3598

- **All childhood sexual assault (CSA) allegations.** Do not wait for receipt of the claim or lawsuit. Notify ASCIP of CSA allegations involving an employee or volunteer that include:
 1. Arrest or criminal complaint;
 2. Investigation by the member, or any governmental agency;
 3. Verbal or written disciplinary action taken; or
 4. Any matter reported to, or should have been reported to California Commission on Teacher Credentialing.
- **Significant Events** - those that involve a fatality, hospitalization of a third party (student, parent, non-district employee, etc.) or have the potential to incur large monetary losses. Don't wait for the injured party to file a claim!
- Injuries or damages caused by your organization. Don't wait for a claim to be filed. Notify ASCIP right away so resolution can be reached prior to incurring costly litigation.

Upcoming Events *(for updates and details go to www.ascip.org/training/seminars-webinars/)*

Event	Date	Time	Link to Register
CCD Roundtable	Wed Nov 4	1:30-3:30 pm	REGISTER
HR Roundtable-Bullying: What Administrators Need to Know	Thu Nov 5	1:00-2:30 pm	REGISTER
MOC Updates-Understanding You ASCIP Coverage	Tue Nov 10	1:30-3:00 pm	REGISTER
Codes, Regulations and Compliance Review	Tue Nov 10	10:00 am-Noon	REGISTER
Contracts Review	Thu Nov 12	1:00-3:00 pm	REGISTER
Cybersecurity Roundtable	Wed Nov 18	1:30-3:30 pm	REGISTER
IT Contracts Insurance Requirements	Thu Nov 19	1:00-2:30 pm	REGISTER
SAVE THE DATE ASCIP Annual Membership Meeting	Fri Mar 5	TBD	Coming soon!