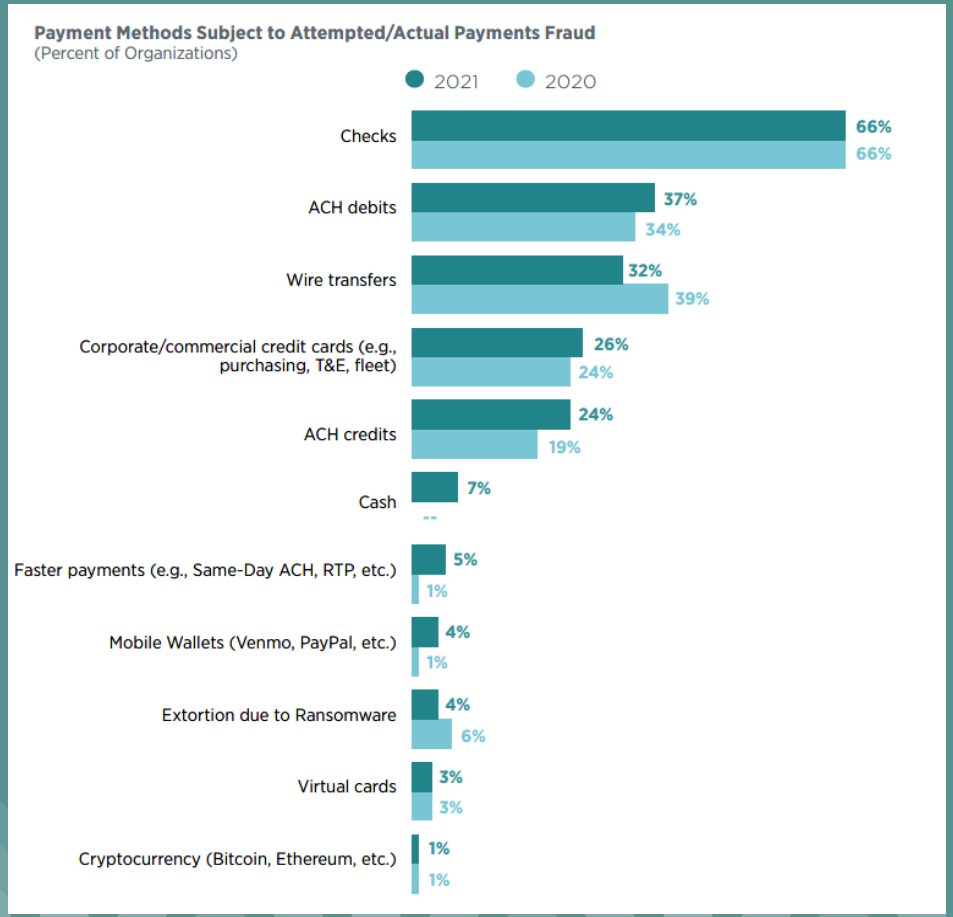
Credit Card Fraud Prevention and ACH Do's and Don'ts

The School Business Office Professionals Conference

December 8, 2022

Targeted Payment Types



In 2021, checks and ACH debits were the payment methods most impacted by fraud activity. Checks continue to be the payment method most often used by organizations. However, many companies are shifting checks to digital payment methods.

While most financial institutions maintain industry standard anti-fraud measures, they cannot guarantee your account will never be affected by fraud.

Organizations need to be extremely vigilant when monitoring their bank accounts for any transactions that appear to be out of the norm or unexpected.

Source: www.AFPonline.org

Common Fraud Schemes

- ✓ **EMAIL IMPERSONATION**
  Fake email from CEO requesting an urgent transfer of funds.

- ✓ **SUPPLIER IMPERSONATION**
  Fraudulent "change banks" notice from supplier.

- ✓ **STOLEN ACCOUNT INFORMATION LEADING TO COUNTERFEIT CHECKS**
  Checks that may not look like your checks, but have your account information and are either being cashed, paying bills or used to make purchases across the country.

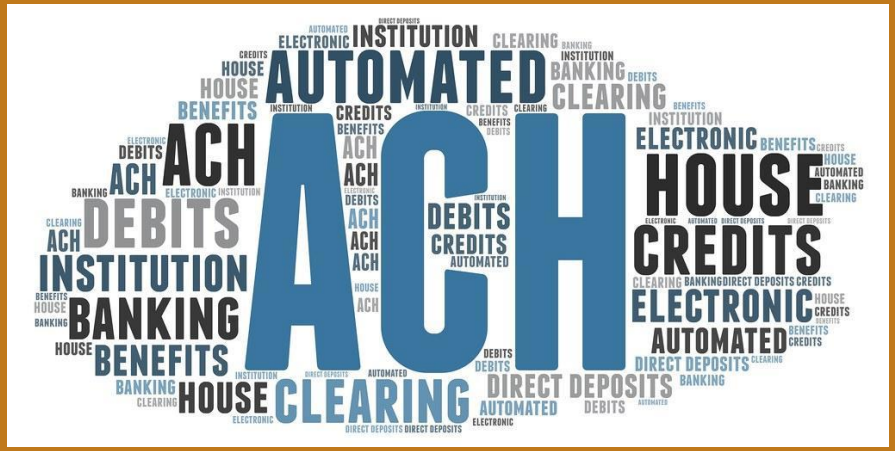
- ✓ **ALTERED CHECKS**
  Checks made out to Five Sons Painting for $500 is changed to payable to Five Sons Painting for $5,500.

- ✓ **FRAUDULENT DEPOSITS/INBOUND WIRES**
  You received a wire or check from an unknown 3rd party. They ask for the money back so you send them a wire. Shortly thereafter, the initial wire or check is rescinded by the issuing bank. You receive a payment from an unknown customer. They say you can keep the payment if you send them back a fee. The deposit ends up bouncing.

- ✓ **SPYWARE AND MALWARE AS A RESULT OF PHISHING AND SOCIAL ENGINEERING**
  Click on the wrong links and software is downloaded which will hijack your computer for passwords and copy keystroke activity.

- ✓ **INTERNAL EMBEZZLEMENT**
  Non suppliers are loaded into your accounting systems and paid for personal gain without appropriate oversight. A check to pay your company phone bill is taken by your employee to pay their personal phone bill.

ACH Do’s and Don’ts



ACH Origination:
What you need to know

ACH or Automated Clearing House is the official U.S. financial network used for electronic payment and money transfers. Also known as “direct payments”: ACH payments are a way to transfer money from one bank account to another without using paper checks, credit card networks, wire transfers, or cash.

An **ACH Originator** is any person or entity that creates the ACH transaction

Historically, ACH has been a next day or 2-day settlment process, but Same-Day ACH is now available. Typically you enroll with your Financial Institution and then control the settlement (standard vs. same-day) with the effective date. *Current per transaction limit is $1,000,000.00

Methods of Initiating ACH:

1) online banking portals including: one-off transactions, template storage or file upload
2) direct transmission such as SFTP
3) API's
4) integrated/consolidated payables services

*Files typically need to be CSV, EDI, or Nacha formatted

Nacha is the governing body of the ACH network:

https://nacha.org

The ACH Network touches nearly all Americans, and the Nacha Operating Rules direct how the ACH Network is operated. Everyone using the Network, from consumers and financial institutions to businesses and governments, has responsibilities.

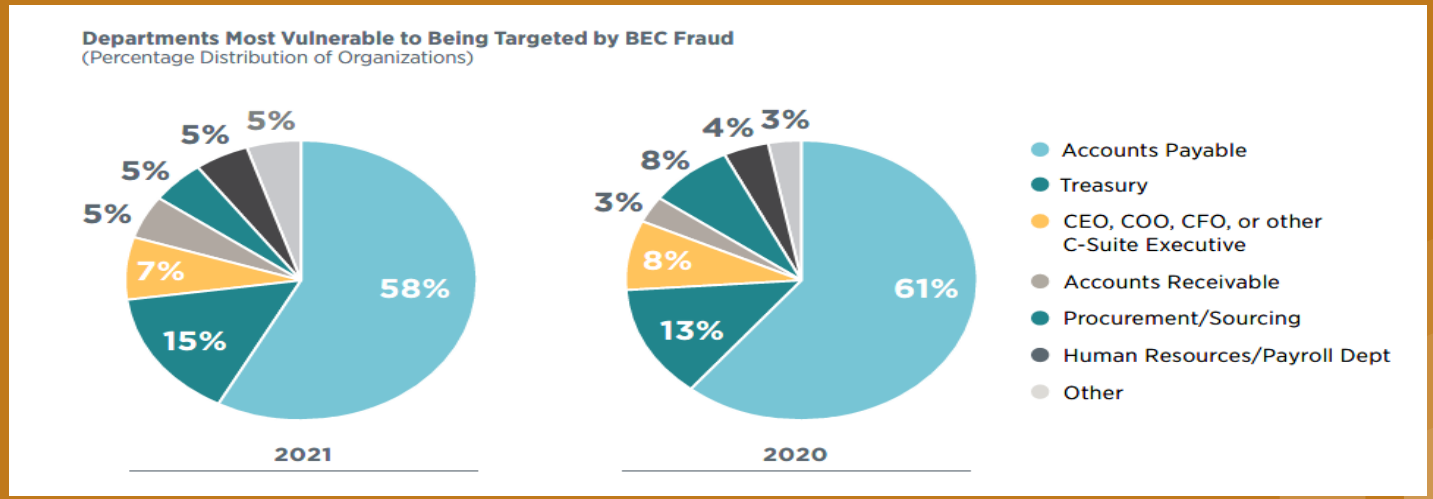
Source: www.nacha.org

Know who you are paying

ACH is still the only irrevocable payment method available today, but it is still important to maintain tight controls around validating, storing, and changing any vendor bank account information. Best practices:

-dual controls on storage/maintenance of vendor payment information
-verification of vendor information or requested changes—always pick up the phone and call (*not the number in the email)
-account validation products

Business email compromise scams continue to take various forms and change as criminals get more creative. While fraudsters might target an entire organization, they generally are more focused on Accounts Payable departments.



Source: www.AFPonline.org

Recommended Security Checklist

Educate your employees. You and your employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

Protect your online environment. It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected internet connections.

Encrypt sensitive data and keep updated virus protections on your computer.

Use complex passwords and change them periodically.

Source: American Bankers Association

Recommended Security Checklist

Partner with your bank to prevent unauthorized transactions. Talk to your Bank about programs that safeguard you from unauthorized transactions. Positive Pay and other services offer call backs, device authentication, multi-person approval processes and batch limits help protect you from fraud.

Pay attention to suspicious activity and react quickly. Look out for unexplained account or network activity, pop ups, and suspicious emails. If detected, immediately contact your bank, stop all online activity and remove any systems that may have been compromised. Keep records of what happened.

Source: American Bankers Association

Tools to Keep Your Business Account Safe

Check Positive Pay. Positive Pay compares checks presented for payment against issued check information you provide in order to identify discrepancies and help protect your accounts. Check number and dollar amount are validated at minimum. Check with your financial institution to ensure payee verification is also included.

Reverse Positive Pay. Review checks before payment, investigate discrepancies, and choose to pay, return, or adjust discrepancy.

Check Blocks. If you don't issue checks from an account, ensure the proper controls are in place with your financial institution to block all check debits.

ACH Positive Pay. Only allow authorized partners to debit your account. You have control over adding, modifying and deleting any authorized partners. Any items not on the authorization list will be presented for review with the option to return.

Dual Control. Having one user initiate and a separate user approve all outgoing transactions is always recommended as a best practice.

ACH resource: provided by Wintrust Government Funds

Recommended Security Checklist

Understand your responsibilities and liabilities. The account agreement with your bank will detail what commercially reasonable security measures are required in your business. It is critical that you understand and implement the security safeguards in the agreement. If you don’t, you could be liable for losses resulting from a takeover.

Create account alerts. Custom alerts can be set to monitor account balances and activity including deposit and withdrawal notifications as well as security alerts to monitor changes to your address, password, or if your account has been locked out. Available by text, email, push or phone alerts.

Source: American Bankers Association

Recommended Security Checklist

NACHA requires that all participants in the ACH process (including merchants initiating ACH transactions via a third party processor) implement processes, procedures and controls to protect sensitive ACH data (Protected Information), and to put access controls in place to safeguard Protected Information.

The ACH Rules define “Protected Information” as, “the non-public personal information, including financial information of a natural person used to create, or contained within, an entry and any related addenda record.”

The definition…not only covers financial information, but also includes sensitive non-financial information (such as non-financial account information contained in addenda records for bill payments).

The ACH Rules require that any transmission of banking information, such as a customer’s bank account and routing number, be encrypted using “commercially reasonable” encryption technology if transmitted via an unsecured network, like the Internet. (This is similar to the PCI Requirement to use “Strong Cryptography” for transmission of cardholder data.)

ACH resource: paysimple.com

Recommended Policies and Procedures

Require an Authorization Form signed between you and your employee or vendor. A confirmation letter from the bank and/or copy of a check is recommended to assist you in collecting correct information.

- All forms should be kept on file for two years after the last transaction.
- Recommended that the Authorization Form has terms and conditions that allow for debit corrections if needed.

Recommendation: A callback should be required and documented for each Authorization Form received not in person for verification in an attempt to avoid impersonation.

Pre-notes are recommended to ensure the accuracy of the account information provided prior to sending funds: note that this information will not confirm that the account information belongs to the payee which is why the callback is important.

Resource: School District of Denmark

Recommended Policies and Procedures

- An originator of a debit entry to a Receiver's consumer account must obtain a written authorization that is signed or similarly authenticated by the Receiver, except as otherwise expressly permitted by the Rules.

- Minimum Requirements for the debit authorization:
  - Language clearly stating whether the authorization obtained from the Receiver is for a single entry, recurring entries, or one or more subsequent entries initiated under the terms of a standing authorization
  - The amount of the entry or entries, or a reference to the method of determining the amount of the entry(ies)
  - The timing of the entries, including the start date, number of entries, and frequency of entries
  - The Receiver's name or identity
  - The account to be debited (this should include whether the account is a demand deposit account or savings account)
  - The date of the Receiver's authorization
  - Language that instructs the Receiver how to revoke the authorization directly with the Originator

ACH resource: 2022 Nacha Operating Guidelines

AUTHORIZATION FORM SAMPLE

DENMARK SCHOOL DISTRICT
BUSINESS SERVICES
450 NORTH WALL STREET
DENMARK, WISCONSIN 54208-9416
Phone (920) 863-4006

ELECTRONIC TRANSFER SIGN-UP AUTHORIZATION FORM AND AGREEMENT

After completing the form, please email to marotzj@denmark.k12.wi.us or mail to Denmark School District, Business Services, 450 N Wall St, Denmark, WI 54208. *If you are currently employed by the District, you complete the banking portion of this form because we already have it on file for payroll.

Name (Print)
_____
Address
_____
City, State, Zip
_____
Phone (area code)
_____
*E-Mail Address

*Your email address is required so we can notify you electronically with payment details.

Financial Institution (Print)
_____
Street Address
_____
City, State, Zip
_____
Phone (area code)

Check One Start ☐ Change ☐ Cancel ☐
Account Number_____
Routing Number_____
(First 9 digits on check)

Check One Checking ☐ Savings ☐

The principal purpose for requesting this information on this form is to verify your identity and establish your account to receive EFT payments. Furnishing your name, address, and bank account information is mandatory. Failure to provide such information will delay or may even prevent the payment for which this form is being filled out. Information on this form is used by DSD for non-payroll payments, and may be transmitted to the State [illegible] payment as required by law.

Attach Voided Check Here

If you don't have checks, or choose to use a savings account, please provide a letter from your bank confirming your account information.

DENMARK SCHOOL DISTRICT
TERMS AND CONDITIONS FOR ELECTRONIC FUNDS TRANSFERS (EFT)

By submitting this completed and signed electronic transfer form and agreement, you agree:

A. To accept payments from the Denmark School District through electronic transfer(s).

B. To these terms and conditions for electronic funds transfer payments.

C. That the District can rely on the information supplied on the sign-up form.

These terms and conditions are hereby incorporated into all existing agreements between you and the District.

1. The District will initiate EFT payments to pay all obligations to you arising from existing agreements, and you will accept EFT payments to satisfy all such obligations. EFT payments will be made to the financial institution and account number shown on your enrollment form.

2. Payment will be made in accordance with and governed by the Corporation Trade Rules of the National Automated Clearing House Association (NACHA).

3. You or an authorized representative must communicate any changes within the enrollment information to the District in writing within 7 days of the effective date to allow adequate time to respond to the changes. The District will not be responsible for any loss arising solely from error, mistake, or fraud regarding the information on your EFT enrollment form.

4. These EFT terms and conditions neither enlarge nor diminish the respective rights and obligations contained in the agreement with you. Payment will be considered made when your financial institution has received or has control of a payment transaction from the District.

5. The District has a right to adjust future payments if payments previously made are found to be duplicates, in excess of requirements, fraudulent, in error or requires any other adjustment under the terms of the agreement with you. This may be accomplished by using an ACH debit.

6. The District is responsible for an EFT transaction only to the time your financial institution receives or has control of the transaction. The District will be responsible for loss of data only when the loss is due solely to the negligence of the District. (The District will not be responsible to pay any fees to the bank in relation to the transfer of the funds, or be required to pay any late fees if the funds remitted are not credited to the supplier's account through no fault of the District).

7. Either party may terminate this EFT agreement by sending written notice, effective 10 business days after receipt.

8. **Remittance information will be e-mailed to the address noted on the sign-up form.**

Cyber Enhancements Coverage

Many school districts now purchase cyber liability insurance coverage to assist in protection against cyber liability exposure.

- Policies may include computer and funds transfer fraud, security breach, extortion, threat and ransom coverages.

It has become common for the insurance companies to require many of the security procedures and processes recommended in order to maintain coverage.

ACH Fraud Prevention and Detection Summary

-Conduct daily reconciliations rather than monthly
-Utilization of ACH debit filter/blocks
-Updating company ID's for filters on a timely basis
-Educate employees about risks and fraud attempts
-Dual Controls (for vendor storage/updates and payment initiation
-Hold an independent review of the processes done by internal audit

Compare automated clearing house transactions (ACHs) reported on bank statements each month to ACHs recorded in the accounting records.

- Are there any ACHs to unknown vendors/payees?
- Are there any larger, even dollar amounts?
- Are there ACHs to vendors/payees that are different than the vendors/payees recorded in the accounting records?
- Are there any omitted ACHs from the accounting records?

Credit card fraud can occur when using a lost or stolen card or by making transactions without ever having the credit card in their possession.

The most effective way to protect yourself from **credit card fraud** is by taking preventative measures wherever possible.

Credit Card Fraud: What you need to know

Types of Credit Card Fraud

Are you who you say you are?

- Identity Theft
- Account Takeover
- Business email scams
- Phishing
- Hacking

Is this an authentic account?

- Counterfeit
- Skimming

Is the transaction legitimate?

- Lost or stolen cards
- Mail order & telephone order fraud
- Friendly fraud-employee misuse

Is the vendor reputable?

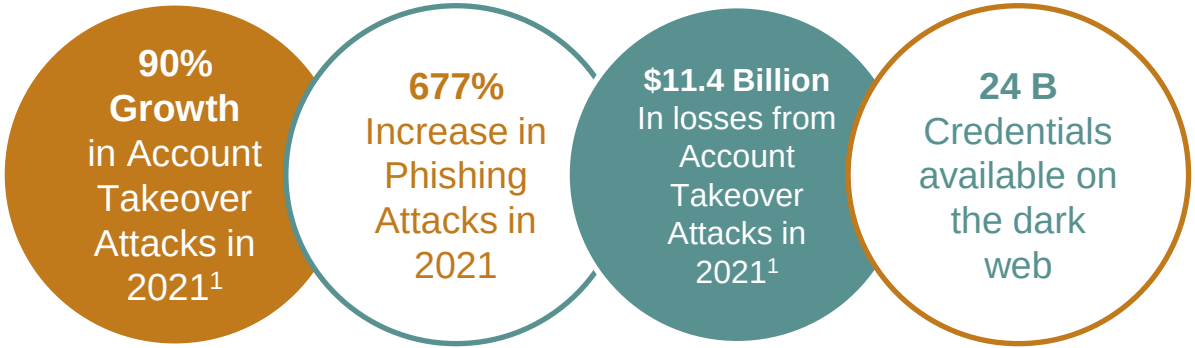
- Vendor fraud/conflict of interest
- Collusive merchants
- Data breaches

Source: Mastercard Cards 101

Credit Card Fraud Landscape

Account Takeover has become the #1 Security Concern for Organizations (surpassing Malware).

Login credential success rate jumped to ***9.9%***, up from an average of 1.9% in 2020. [2]



Source: Mastercard Card Cyber & Intelligence Latest Industry Trends: Identity, Scams, Crypto

1. Javelin Research “Identity Fraud Study: The Virtual Background”
2. NuData Credential Stuffing Report 2022

Credit Card Fraud Prevention

Fraud can be detected by parents,teachers and you!

Credit card fraud that occurs in school districts usually happens because districts trust their employees' decisions or because the districts do not fully understand the purchase.

Credit Card Fraud Prevention

Thankfully, there are many precautionary steps that schools can take to minimize the risk of credit card fraud and to identify suspicious activity promptly.

- **Prevention is the best means of protection- and it starts at the time you issue cards.**
- **Monitor to ensure that cards are only used for school purposes**
- **Implement strong controls**
- **Have rules on which types of purchases are allowable for a credit card to prevent purchasing policies from being circumvented**
- **Train employees on best practices for card use and management and how not to fall for scams**

Credit Card Fraud Prevention

When it comes to business credit card fraud, prevention is the best means of protection.

- Only issue business credit cards to trusted employees that have a legitmate business need and for reasonable limits.
- Implement an approval process to issue new cards and change limits.
- When setting up cards, consider providing an alternative piece of information to SSN to be used for validation. Do not setup employee cards with generic or public information (ex. All 1's for the SSN, company TIN).
- Ask your card provider if you can add a verbal passcode to the account for Program Administrators to provide before account information is provided. Change regularly!
- Keep card information secure- don't save it to your computer, write it down, or leave physical cards out in the open.
- Encourage employees to only carry their card when nessecary, leaving it in a secure location when not.
- Take advantage of of controls offered by the credit card company such as limits, pins (no generic PINs!) or merchant codes etc.
- Register for available account alerts.

Credit Card Fraud Prevention

Ensure credit card use is only for school purposes.

- Have employees sign credit card use agreements.
- Closely examine supporting documentations for all expenditures- monitor for altered or fabricated documents
- Always require itemized receipts. Question items and have reimbursements made immediately for personal items, if any are noted
- Do not allow disorganization
- Segregation of Duties is key in preventing fraud. Make sure no one has the ability initiate, approve, and complete any one transaction.
- Timely reconciliation of credit card transactions and routine monitoring by multiple levels

made and entering a purcha GUIDELINES SAMPLE r the funds accordingly. Below are the ns.

A purchase order shall be created for each charge in Skyward. The vendor to be used on the Skyward purchase order is Mastercard BMO. The staff that is using the card and/or the person responsible for checking the card in or out will need to take the responsibility for creating the purchase order no later than 24 hours after the charge has been made. The purchase order will be used to verify approval for the purchase, availability of budgeted funds and adequate supporting documentation before the payment is made.

Receipts, Sales Tax and Procurement Card Statements

Receipts

The District requires an itemized receipt for each purchase. If a receipt is lost, you should contact the vendor to obtain a duplicate receipt. If the vendor is unable or unwilling to help you, the following options apply:
1. Call our procurement card provider at (800)361-3361 and ask for a duplicate receipt. If you are only provided a charge card slip receipt (receipt that does not itemize your purchase), you will also have to fill out the Missing/Lost Receipt/Detail Form.
2. You may use a Missing/Lost Receipt Form. Please complete the form with as much detail as possible and have your supervisor sign it. This form may only be used twice in one school year. If use of this form occurs more than twice in one school year, your card privileges will be suspended until the end of the school year (June 30th).
3. Pay the entire bill personally by attaching a check made out to the School District of Denmark with a copy of the receipt that was paid by the District procurement card in error.

An Itemized Original Receipt and the missing/lost receipt form in lieu of that receipt must, at the least, have the following items on the receipt:

Name of Merchant.
Address/Phone # (at least one way to contact the merchant)
Description of each item purchased.
Price for each item purchased.
Tax for the taxable items, if it was charged as we would need a credit.
Grand Total.
Date of Purchase.
Method of payment.

Sales Tax

All Denmark School District purchases are tax exempt; therefore, tax should not be charged to District purchases. If you were charged tax on your procurement card there are two options:

School District of Denmark Business Department Aug 2, 2021

1. Contact the vendor to ask for the tax to be reimbursed to your procurement card. If you are obtaining a credit back from the vendor for the tax and the credit is not obtained in the same billing cycle as the original purchase, you will either need a copy of the original receipt showing the tax amount or a receipt showing the tax that was refunded to your statement where the credit appears. Put a copy with the statement where the original charge appears also.

2. Pay for the sales tax personally by attaching a check made out to the School District of Denmark with a copy of the receipt that sales tax was charged on the District procurement card.

CEIS Number 008-0000182414-04 Issued 12/27/2020
Sales Tax Exempt Certificate

Please contact Alli at Ext. 4012 or hardya@denmark.k12.wi.us for a copy of a S211 form if needed.

Card Holder Reconciliation
Procurement card transactions will be uploaded into the Skyward system on the 20th of each month. Transactions brought into the system will require the cardholder to enter a purchase order.

Please follow these steps to reconcile your procurement card transactions.
1. Go into Skyward and verify you have entered a purchase order for each card transaction.
2. Attach all procurement card receipts in Skyward to the related transaction's purchase order if not already attached. If receipts are not scanned into Skyward the purchase order will be denied until the documentation is attached. Once completed re-submit for approval.
3. After you submit your transaction for approval, your supervisor will also need to approve the purchases similar to any other purchase order, expense reimbursement etc.

Approval of Purchases
Before the end of the day of the 20th of each month, the supervisor shall have reviewed all purchases for the billing cycle in Skyward by approving individual purchase orders for each transaction. If changes need to be made, the supervisor has the ability to change the description and/or the account number on the purchase order in Skyward or deny the transaction and ask their staff to correct the transaction details and/or account number. The supervisor's purchase order approval indicates that the cardholder was authorized to make those purchases and that those purchases were made in accordance with the applicable procedures. It is the supervisor's responsibility to report any discrepancies found to

Credit Card Fraud Prevention

Ensure credit card use is only for school purposes.

- All new vendors should be subject to approval
- Purchasing procedures should be divided among several employees(for example, the person ordering services or supplies should not be responsible for approving payments).
- Have a robust credit card policy or manual that defines allowable and unallowable purchases. Provide periodic training for personnel reviewing expense reports focused on policies and procedures.
- Implement deadlines for submission of receipts and revoke credit card access for non-compliant cardholders. Review and approve all purchases before making payments to the credit card company.

Credit Card Fraud Prevention

Implement strong operational controls.

- Avoiding issuing no name/departmental cards. Best practice is to always issue the card in the name of an individual.
- Regularly monitor transactions and card limits to make adjustments/take action as needed.
- Utilize soft blocks (i.e. Card On/Off) if available.
- Partner with HR teams for regular reporting of terminated employees to ensure cards issued to those employees get closed ASAP.
- Similar to annual access reviews, implement regular card reviews.
- Keep contact information up to date.
- Ask about your card issuers requirements for online account access- do they require strong enough credentials?

Credit Card Fraud Prevention

Continuously Train

- Train employees on internal policies and procedures. Hold regular refresher training.
- Make sure employees know who to contact and when if suspicious activity is detected or their card is lost/stolen.
- Share best practices.
- ATO, Phishing, and Business Email scams- do your employees know what they are, how to identify, and who to report them to?
- Teach employees how keep credit card information safe online:
  - Check to make sure the website is secure by looking for the lock icon or https in the address bar.
  - Logout of websites and online account applications when finished with them.
  - Keep browsers and devised up to date.
- Teach employees not to disclose personal or credit card information over the phone unless they can verify they are a trusted source.

Credit Card Fraud Prevention

How credit cards are used can also help prevent fraud.

- Ensure merchants are dipping vs swiping. Chip transactions are more secure.
- Do not allow websites to remember card or password information.
- Check the terminal- can you spot a skimming device?

- If supported, use your card for a contactless (tap) payment to avoid exposure from skimming devices.

Credit Card Fraud Prevention

Look into implementing virtual cards, especially for vendor payments or one-time use scenarios.

- Virtual cards (VCs) are one-time use cards generated for a specific payment and delivered to the recipient via secure email, portal, or application.

- VCs are one of the most secure payment methods because of the controls they have including:
  - **Unique 16-digit card** number is generated each time a VC payment is requested. No more card on file or providing static card numbers over the phone or online.
  - VCs are **only issued for the amount request**ed. Transactions attempted for a different amount are declined.
  - VCs are **only valid for a limited time** (usually 30 days).
  - **MCC restrictions** can be placed on each individual payment preventing unauthorized use from getting through.

- VCs can also be integrated into AP automation tools or submitted to your card issuer via files to help streamline payment processes

Steps to identify credit card fraud

Recommended best practices to identify credit card fraud

Regularly review statements

- Make sure to regularly review statements so that you can detect any unfamiliar charges. Consider conducting weekly reviews using online banking tools to keep the task manageable. Ensure that issues are reported to the credit card company as soon as possible.

Compromised Cards ie Lost/Stolen Cards

- Ensure that issues are reported to the credit card company as soon as possible. Add a temporary block immediately if needed and/or add a new card.
- Update security details if you believe they have been compromised

Recommended best practices to identify credit card fraud

Regularly review bills and invoices

- Reviewing bills and invoices to ensure you are not receiving correspondence and collection notices for unfamiliar accounts.
    - Fictitious vendors, could be a kickback scheme for example

Anyone can commit fraud

- Only 3.3% of fraud is found in an external audit.
- Fraud is more likely to be detected by a tip than any other method. Almost half of all fraud is reported by a tip from an employee or hotline..
    - Fraud hotline or other reporting mechanism should be provided

Contact Information:

Marylou Schirpke, Senior Vice President
Municipal Government Banking at Town Bank
140 S. 1st Street
Milwaukee, WI 53204
mschirpke@townbank.us
414-255-1007

Courtney Broderick, Vice President
Wintrust Treasury Management
731 N. Jackson Street
Milwaukee, WI 53202
cbroderick@wintrust.com
414-255-1013

Janelle Marotz, CPA, SFO, CSRM
Director of Business Services
School District of Denmark
450 North Wall Street
Denmark, WI 54208
https://www.Denmark.k12.wi.us/
marotzj@Denmark.k12.wi.us
920-863-4006

Sarah Eberly
Vice President, Commercial Products
Wintrust Financial Corporation
9700 W. Higgins Road, 5th Floor
Rosemont, IL 60018
seberly@wintrust.com
847-939-9757

Questions?