# Anatomy of a Fraud

## Business E-mail Compromise & Computer Intrusion

First Merchants Bank

## What is Business E-Mail Compromise?

- Scam targeting businesses that regularly perform **ACH** and **Wire Transfer** payments.
- **Small** and **Mid Sized** businesses but all are susceptible.

## How is the fraud perpetuated?

- Employees receive an email request to transfer funds.
- Typically from a representative of upper management of their company or a vendor from another company.
- The message is not from the company's management or vendor, it is an impersonation by the fraudster.
- The email received is typically spoofed or compromised.

## Who is the target?

- Multiple Targets – any employee
- Senior Management
- Individuals responsible for handling ACH and Wire transfers and financial payments within the company.

# Business E-Mail Compromise (BEC) – Case Study 1

- A commercial client switched their remittance processing in June 2018 from check to ACH.  Their vendors were contacted in May to provide bank account information.
- A controller of a vendor provided their bank information via e-mail to the commercial client in May.
- In June, the ‘controller’ from the vendor emailed new account information to the commercial client.
- From June – Mid October 2018 the client made 13 ACH Payments to the ‘vendor’s account’ totaling $571,343.86.
- Using the email and telephone information the ‘controller’ provided, the commercial client maintained contact with the ‘controller’ who confirmed they had received and applied the ACH payments.
- Mid-October the vendor’s CFO contacted the commercial client by phone advising they had not received any of the 13 ACH payments into any bank account under their control.
- This is when the commercial client discovered the fraud.


# Case Study 1, continued

- Due to the vendor's email being spoofed, any correspondence the commercial client and vendor were exchanging for 6 months were not actually being exchanged with the controller. The fraudster was intercepting all correspondence and money.
- FMB worked with the receiving bank in an effort to recover funds.
- A portion of the funds were recovered.
- The IT Department of the client and vendor became immediately involved to isolate the intrusion.
- Federal authorities were immediately contacted
- How would this have been caught?
  - Calling a known vendor phone number on file to confirm the payment information change

# Computer Intrusion – Case Study 2

- Subject: Business client using online banking and ACH payroll feature
- Fraud vehicle:  Online Banking compromise via client computer intrusion
- Loss Exposure:  $90,437
- FMB's systems flagged a suspicious newly created ACH Payroll file for $58,684
- Why:
  - Large, even dollar amounts
  - A legitimate payroll file was submitted a day prior
  - A new phone number for the primary user was recently added

# Case Study 2, continued

- FMB responded by:
  - Deactivating OLB
  - Restricting all account debits
  - Attempted to restrict the outgoing ACH file until verified
- During the 4 minutes between fraud flag and getting things shut down another outgoing ACH file was created for $31,753
- Client was contacted via prior phone number and confirmed it to be fraud
- Client also admitted to receiving a verification request of the phone number change but did not act upon it
- The ACH transaction triggered ‘Out of Band Authentication’ – to the fraud number

# Case Study 2, continued

- How did it happen?
  - Client's IT team investigated their systems and scrubbed their emails.
  - Diagnosis: E-Mail Bomb
  - Similar to a DDoS attack and can infect systems with malware/spyware.
  - Ultimately, system/computer intrusion allowed access to OLB
- How to Prevent Computer Intrusion?
  - Ensure systems are secured and protected by regularly scanning & updating virus protection.
  - Designate a specific terminal used for Banking only.
  - Timely response to bank's attempts to verify and authenticate activity or information changes.

# First Merchants Fraud Prevention Efforts

**We continually work to provide an environment in which account information stays secure.**

- We maintain high security standards on our systems and continually research additional controls for protection.
- We continuously monitor our security protocols to keep customers money and information safe.
- We apply a layered approach to security, which helps defeat attempts to compromise our systems.
- We work closely with law enforcement and regulatory agencies to stay current with industry standards for fraud prevention.
- Security alerts are communicated through our website, as well to our online banking customers via secure messaging.

# Best Practices for Companies

**General**

- Never provide personal or confidential information – always protect
- Do not respond to or click on links from e-mails; do not open attachments on suspicious e-mails
- Reconcile all accounts and statements quickly
- Tighten internal security controls, including employee training
- Maintain up-to-date anti-virus/anti-spyware with regular scans
- Implement firewall configured correctly
- Restrict employee PC hardware such as CD burners and USB ports
- Implement strict policies for confidential information storage and destruction
- Use cross-cut shredders on all documents with sensitive or confidential data
- Investigate purchasing insurance to reduce the risk of loss, should fraud occur

# Best Practices for Companies, continued

**Online Banking**

- Always protect online banking login credentials
- Use a dedicated PC for conducting financial transactions
- Monitor all account activity daily via online banking
- Use dual authorization for online banking transactions
- Enforce the use of robust passwords
- Enable idle PC “timeouts”

# Payment Fraud & Prevention Tools

First Merchants Bank

# Current Fraud Stats

**As of 2019*:**

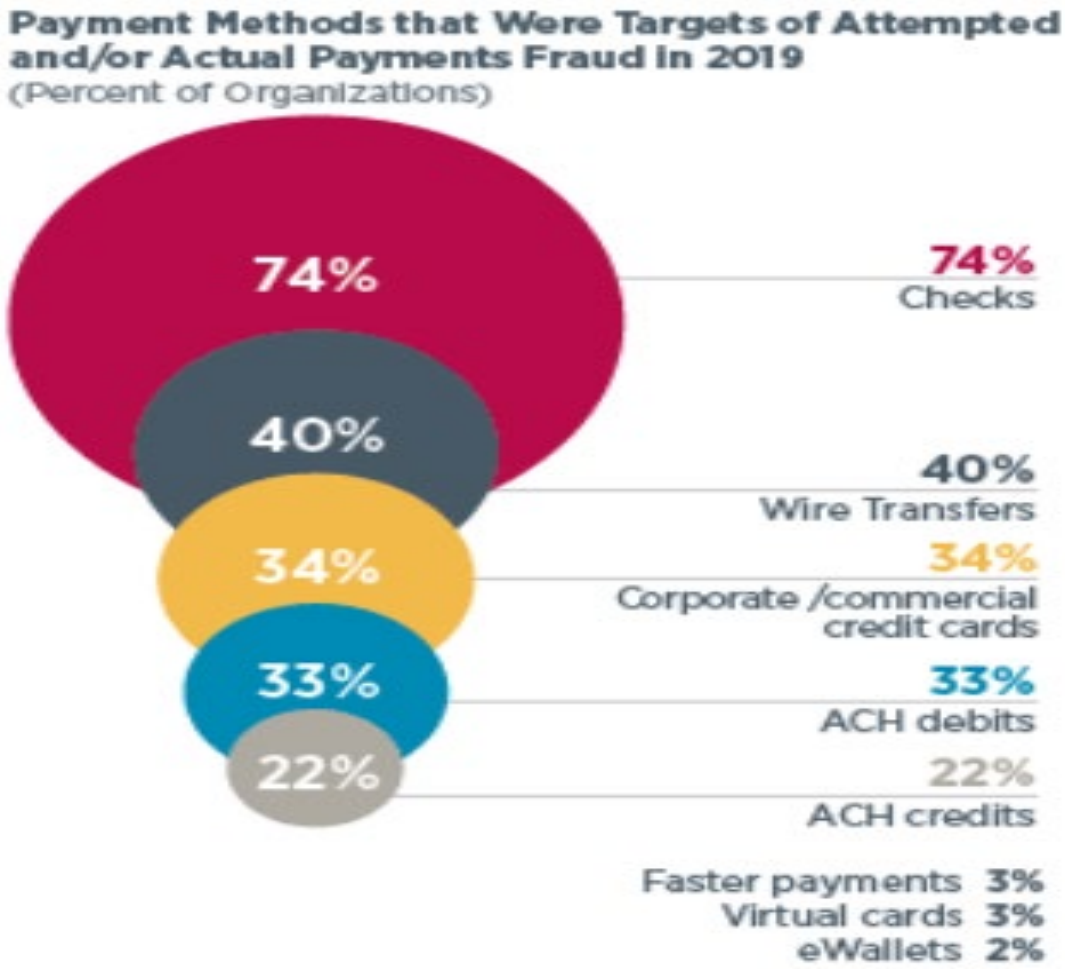
- 81% of companies were targets of payment fraud last year
- 75% of organizations experienced Business Email Compromise (BEC)
- 54% of organizations reported financial losses as a result of BEC
- 42% of BEC scams targeted wires, followed by ACH credits at 37%
- 74% of organizations experienced check fraud,
- 33% were subject to ACH debit fraud & 22% were subject to ACH credit fraud

**2020 AFP (Association for Financial Professionals) Survey Report*

# Payments Fraud – 2019*

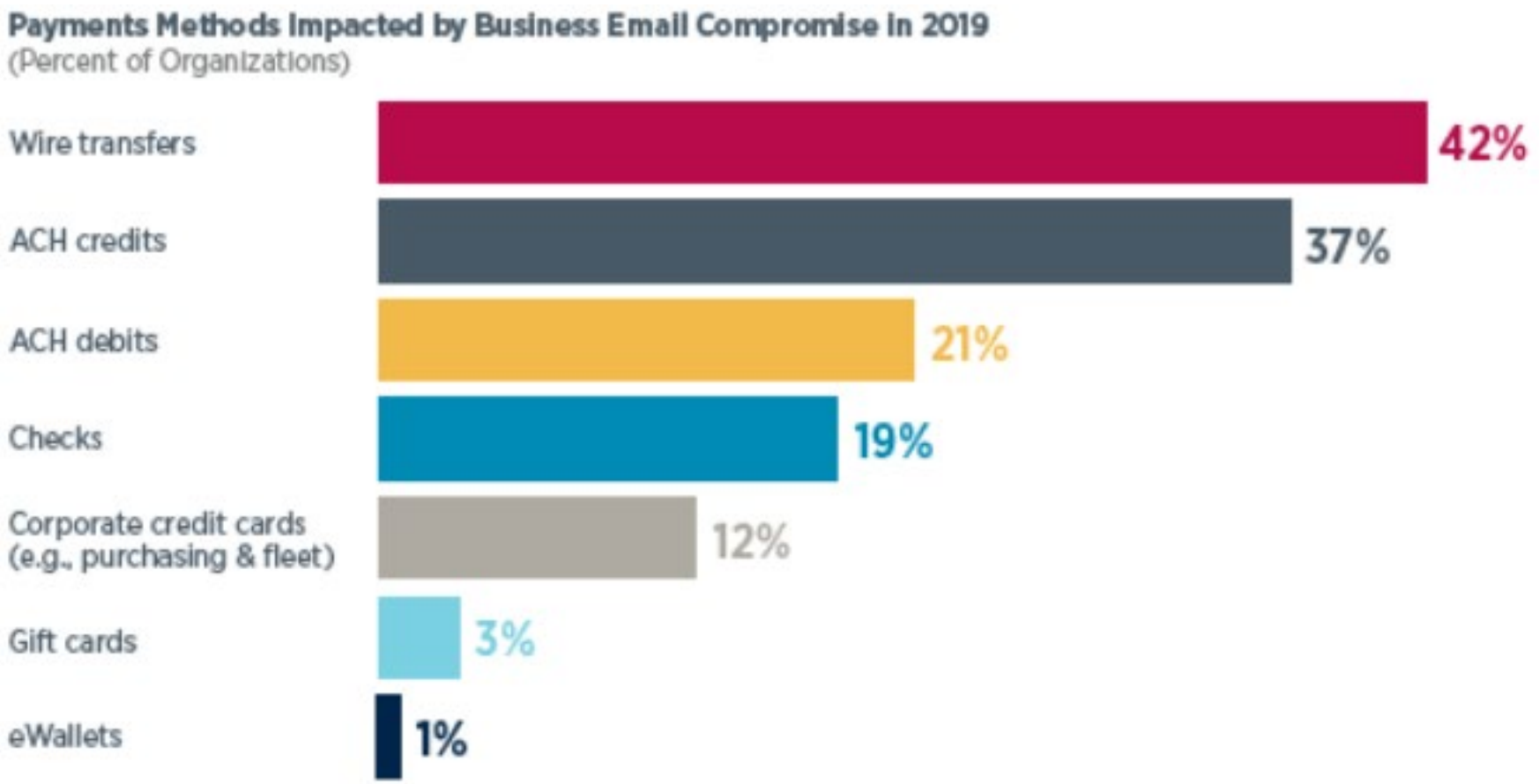

*2020 AFP (Association for Financial Professionals) Survey Report

# Sources of Payments Fraud in 2019*




*2020 AFP (Association for Financial Professionals) Survey Report

# Payments Fraud – Methods 2019*




*2020 AFP (Association for Financial Professionals) Survey Report

# Fraud Remediation

- Immediate actions once fraud is discovered
  - Contact your local Banking Center, Treasury Solutions, or Treasury Management Officer
  - Complete a Fraud report
  - File a police report
- Compile a list of legitimate items (ACH & Checks)
  - Amounts, Payee, Dates, Check number
- Monitor daily to ensure items get paid (no response from client may result in items being returned)
- Options to remediate once fraud occurs
  - New account (notify all vendors/customers with new account information) OR
  - Enroll in Positive Pay Services
- NACHA Rules: Business must dispute Unauthorized ACHs within 1 business day of posting to your account.
- Fraud disputes could take up to 90 business days before funds may be returned to the Client. FMB will do everything in our power to recoup the funds, but there is not a guarantee of credit and may ultimately result in a loss to the Client.

# ACH Positive Pay

**Allows businesses to decide who can debit their account via ACH.**

- ACH debit transactions that are presented for payment from your account(s) are displayed through Business Online Banking as Exceptions
- Individuals responsible for handling ACH and Wire transfers and financial payments within the company.
- You can review and decision Exceptions 8:00am-3:00pm EST
- If no decision is made on an Exception item by 3:00pm, the ACH debit transaction will be returned
- Alerts can be sent to notify users when there is an Exception item to review
- During the review period, payment rules can be set around the Originator to pay with a maximum dollar threshold, if desired

**69% of organizations reconcile daily to identify and return unauthorized ACH debits; 60% block all ACH debit transactions except for a single account that is set up with ACH debit filter or ACH Positive Pay.***

**2020 AFP (Association for Financial Professionals) Survey Report*

# Check Positive Pay

**Helps protect business accounts from counterfeit, duplicate, and altered checks.**

## Payee Positive Pay

- A check “Issue File” is submitted through Business Online Banking, which includes: issue date, payee, check number, and the dollar amount for each check.
- Presented items that do not match will be considered an Exception.
- Exceptions must be decisioned by 1:00pm EST, otherwise the default decision will be followed.
- Alerts can be set to notify Users when there is an Exception item(s) to review.

## Reverse Positive Pay

- Each check is presented as an Exception
- Exceptions must be decisioned by 1:00pm EST, otherwise the default decision will be followed.

# Card Fraud & Best Practices

First Merchants Bank

# Card Fraud Defined

- Card fraud is a form of identify theft that involves an unauthorized use of another's credit card information for the purpose of charging purchases to an account or removing funds from it.
- Types:
  - Card-Present
    - Retail
    - Face-to-Face
  - Card-Not-Present
    - Mail
    - Telephone Orders
    - E-Commerce

# Card Fraud Defined

- Industry Statistics
- Advances in Technology
- Small Business

# Card Present (CP) Fraud

**Retail**

- Counterfeit, fake, doctored cards
- Lost or stolen cards
- Point of Sale Terminals

# Card Not Present (CNP) Fraud

**Mail, Telephone Orders, E-Commerce**

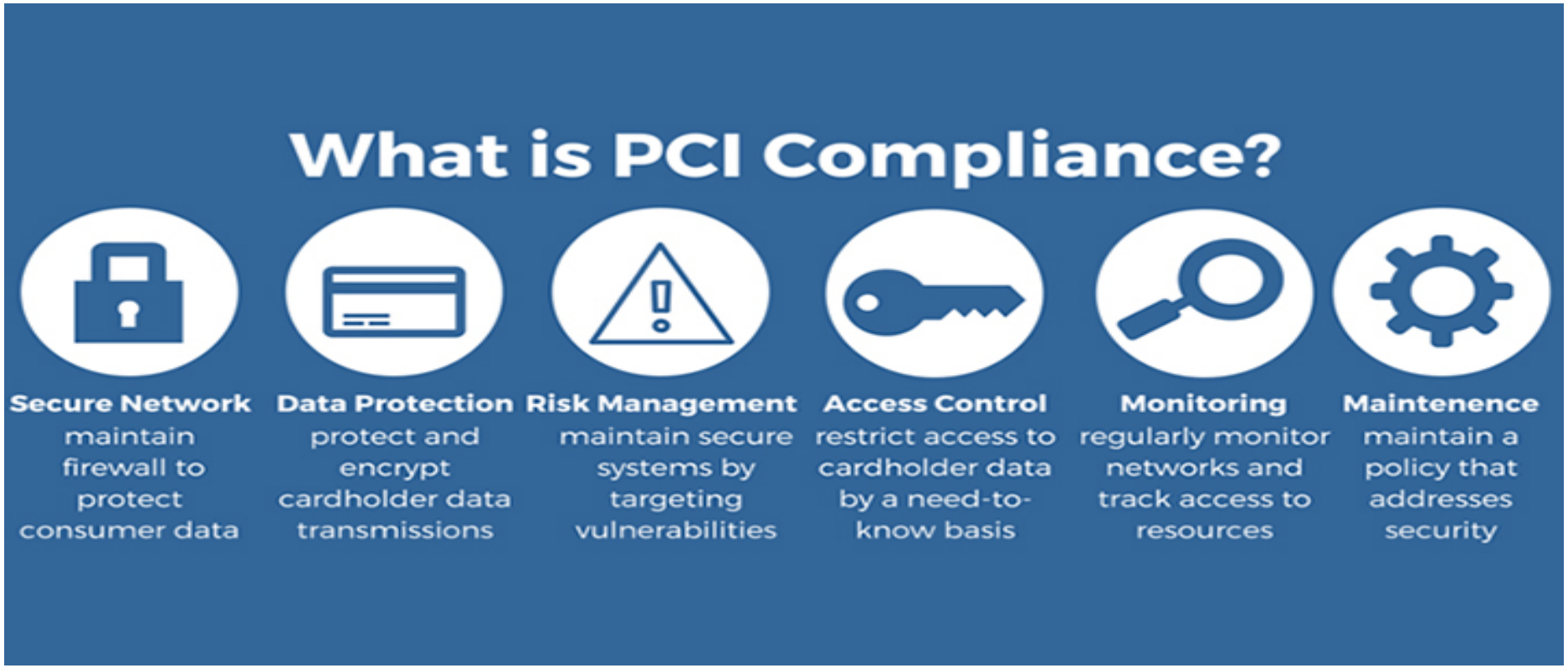
- Unable to Verify Cardholder
- Identity Theft
- Web-based Data Breaches
- Online Shopping and Mobile Payments

# Merchant Loss & Liabilities

- Chargebacks and Refunds
- Fines and Penalties
- Higher costs of Compliance
- Termination of ability to accept card payments
- Diminished sales
- Negative publicity and press resulting in a damaged reputation
- Loss of customers
- Going out of business

# Payment Card Industry Data Security Standards (PCI DSS)

**If you accept or process payment cards, the PCI Data Security Standards apply to you.**



# Best Practices to Mitigate Card Fraud

- Maintain awareness of latest fraud trends
- Use a verified payment processor
- Ensure equipment & software are current
- Security of sensitive cardholder data
- Network and PC firewalls
- Password-protected secured internet
- Strong Passwords
- Check for skimming devices
- Educate employees
- Add insurance, breach protection
- Follow the PCI Data Security Standard

# Your First Merchants Team

| Contacts | | | | |
|---|---|---|---|---|
| Adam Maze | Treasury Management Officer | amaze@firstmerchants.com | 317-566-7689 | Indianapolis, IN |
| Aimee Gilliland | Treasury Management Officer | agillilland@firstmerchants.com | 614-583-2047 | Columbus, OH |
| Angel Gibson | Treasury Management Officer | agibson@firstmerchants.com | 734-374-9302 | Wyandotte, MI |
| Angela Bomia | Treasury Management Officer | abomia@firstmerchants.com | 734-240-2335 | Monroe, MI |
| Casey Spencer | Treasury Management Officer | cspencer@firstmerchants.com | 765-423-7246 | Lafayette, IN |
| Deborah Milne | Treasury Management Officer | dmilne@firstmerchants.com | 219-513-5107 | Munster, IN |

# Your First Merchants Team

| Contacts | | | | |
|---|---|---|---|---|
| Heather Gigliotti | Treasury Management Officer | hgigliotti@firstmerchants.com | 317-762-2223 | Muncie, IN |
| Jon Schiesser | Treasury Management Officer | jschiesser@firstmerchants.com | 219-513-5109 | Merrillville, IN |
| MaKayla Thurman | Treasury Management Officer | mthurman@firstmerchants.com | 317-566-7638 | Indianapolis, IN |
| Michelle Martin | Treasury Management Officer | mdmartin@firstmerchants.com | 317-844-2302 | Indianapolis, IN |
| Susan Cobello | Treasury Management Officer | scobello@firstmerchants.com | 734-242-1936 | Plymouth, MI |
| Valerie Lloyd | Treasury Management Officer | vlloyd@firstmerchants.com | 260-207-6708 | Ft. Wayne, IN |

# Your First Merchants Team

| Contacts | | | | |
|---|---|---|---|---|
| Dale Buffin | Merchant Card Sales Officer | dbuffin@firstmerchants.com | 765-751-1841 | Muncie, IN |
| Dave Mongan | Merchant Card Sales Officer, Team Lead | dmongan@firstmerchants.com | 317-566-7676 | Greenwood, IN |
| Gretchen Schilb | Merchant Card Sales Officer | gschilb@firstmerchants.com | 260-414-9885 | Indianapolis, IN |
| Heather Burkhart | Merchant Card Sales Officer | hburkhart@firstmerchants.com | 734-240-5062 | Monroe, MI |
| Jim August | Merchant Card Sales Officer | jaugust@firstmerchants.com | 219-670-2474 | Merrillville, IN |
| Kristin Rayburn | Merchant Card Sales Officer | krayburn@firstmerchants.com | 765-423-7235 | Lafayette, IN |
| Nicole Kauffman | Merchant Card Sales Officer | nkauffman@firstmerchants.com | 614-583-2130 | Columbus, OH |
| Rachael Anspach | Merchant Card Sales Officer | ranspach@firstmerchants.com | 260-207-6724 | Ft. Wayne, IN |