



TRENDS IN BANKING FRAUD
WHAT YOUR MUNICIPALITY NEEDS TO KNOW

 River Valley
BANK



River Valley Bank

- \$1 billion + community bank
- Headquartered in Wausau, WI
- 15 locations throughout Wisconsin, Upper Michigan
- Business and municipality focus
- Concierge delivery of our Incredible Customer Experience (I.C.E.)

 River Valley
BANK





Pay with Peace of Mind

- Electronic payment systems
 - Primarily ACH and Wire
 - Offer convenience and ease of use
 - Risk if not used properly
- Fraud shift to smaller business
 - Perceived lack of controls
 - AFP Payments Fraud and Control Study—74% of companies experienced either actual or attempted electronic payment fraud
- Education and layered approach to security is key

 River Valley
BANK

Paper is Not Safer


- Legitimate check data is stolen via mail, other
- Routing/account number/signature used to create
 - fraudulent checks or
 - fraudulent ACH (electronic) debits



Businesses have only
24 HOURS
to dispute a fraudulent check or ACH
debit on their account



Businesses have only
24 HOURS
to dispute a fraudulent check or ACH
debit on their account




Good Ole' Fashioned Check Fraud

- Most popular, despite less checks being written
- Technology makes the process easier for the fraudster
- Check data stolen, mail other
- Checks reproduced, presented against your account
- Check looks the same, even the signature is the same
- Realized during monthly reconciliation—too late




Considerations for Prevention

- Reduce the number of checks written—consider using Bill Pay or ACH to make payments, direct deposit
- Review transaction history DAILY, in the AM
- Notify your Bank of suspicious transactions by 10:00 AM
- Discuss use of Positive Pay, Reverse Positive Pay systems to monitor the 24 hour clock for you
- Consider cyber crime insurance as an additional layer




The Lazy Fraudster—ACH Debit Fraud

- Using the same stolen check data, fraudsters can utilize the ACH system to create an ACH debit to your account without your authorization
- Typically smaller, inconspicuous dollar amounts at first
- When items clear easily, larger transactions post
- Same 24 hour dispute window




Considerations for Prevention

- Same as Check Fraud
 - Reduce the number of checks written—consider using Bill Pay or ACH to make payments, direct deposit
 - Review transaction history DAILY, in the AM
 - Notify your Bank of suspicious transactions by 10:00 AM
 - Discuss use of ACH Block & Filter or ACH Positive Pay systems to monitor the 24 hour clock for you
 - Consider cyber crime insurance as an additional layer



Payroll Processing Precautions

Definition: Corporate Account Takeover (CAT) is a form of financial fraud where cyber criminals gain access to business online banking accounts and initiate unauthorized fund transfers—via **ACH and Wire Transfer**—to accounts that are under the cyber criminal’s control. These funds are often then transferred overseas and out of U.S. jurisdiction.




How CAT Happens

STEP 1: Use of social engineering techniques trick users into clicking on malicious links or attachments to emails.


STEP 2: Victims unknowingly download malware on computer, typically allowing keylogging and screenshot capability.

STEP 3: Info is used to login to online banking and authorize fraudulent funds transfer requests.




Symptoms of CAT

- Slow login and screen movement within online banking
- Screens that look different—logos, colors, pages
- Strange ordering of information, i.e. passwords before user names
- Hourglass after entering credentials
- Repeated requests for token information



Considerations for Prevention

- Education of processing personnel is key
- Do not save financial websites as Favorites
- Pay attention to login access times
- Restrict internet and email access
- Use a dedicated computer for financial transactions
- Use dual control, other approval processes
- Use Token authentication
- Set alerts for ACH debit, ACH origination transactions
- Limit IP addresses
- Use fax transmittals to confirm file submissions



Shared Responsibility

- Payment fraud prevention is a shared responsibility
- Develop a security plan for your municipality, focused on understanding the challenges and using the tools and best practices available
- Work with your financial institution and understand the safeguards available to you



QUESTIONS?

For more information~
Lisa Woerpel
Vice President, Cash Management Solutions
River Valley Bank
608-203-9818
608-332-1912 cell
lwoerpel@rivervalleybank.com