Banking Relationship

Stacy Childers
Managing Director, Municipal Solutions
Bremer Bank

The Banking Relationship

Security

Transparency

Communication
Security

- Safety of deposits
  - Full collateralization of public funds to reduce a local government's exposure to any bank credit risk
- Availability of deposits
  - Access and availability of funds
- Creditworthiness of the bank
  - Analysis of the bank's core ratios of financial strength
  - How dynamic is the bank's balance sheet
  - Access to recent financial statements
  - Does the bank have a rating by a third-party rating agency

Communication

- At a minimum, annual review meetings
  - What's new? What's still working, what isn't
  - Are your goals still the same?
  - Short, medium and long-term cash management and investment strategies
  - An identified and responsive service team
  - Introduction of new products and services as they occur

Transparency

- Contract that specifies services and fees
- Account analysis statements that contain specifics
- How are deposit and loan rates calculated and applied
- Consistency of delivery throughout the marketplace
Collateralization of Public Deposits

• Collateralization of public funds ensures the funds are safeguarded in the event of a bank failure
• State and federal laws, including FDIC regulations, are in place to provide guidance on appropriate collateral, both for methods and margins
• In Minnesota, 118A sets the rules

MN State Statutes – 118A

• Requirements
  - Designate authorization of one or more financial institutions as depository of funds
  - Methods and margins for collateralization
• Approved pledging instruments
  - FDIC: $250,000
  - US Govt Treasury Bills, Treasury Notes, Treasury Bonds
  - US Govt Agencies
  - General Obligation securities from state or local governments rated “A” or better
  - Revenue Obligation securities from state or local governments rated “AA” or better
  - Irrevocable Standby Letter of Credit issued by FHLB rated “AA”
• Total collateral requirement amount computed at market value shall be 110% of deposits
• Exception for FHLB Letter of Credit – Requirement is 100% of deposits
Bank Due Diligence

- Implement evaluation procedures for creditworthiness of financial institutions
  - Bank Credit Rating – Standard & Poor’s, Moody’s, Fitch & Kroll
  - Audited Annual Financial Statements
  - Call Reports - https://cdr.ffiec.gov/public
  - Business Continuity & Disaster Recovery
  - 3rd Party Vendors

Current trends in payments fraud

Deb West, CTP
VP, Treasury Solutions Consultant
Bremer Bank

Payments fraud continues to be prevalent.
Check fraud is on the decline yet remains the largest exposure in payments fraud. 

While check fraud attempts decline, we still see a troublesome increase in Wire and ACH attempts over time.

Perpetrators of payments fraud are varied:

- 64% Outside Individual (e.g., forged check, stolen card)
- 58% Business Email Compromise
- 22% Third-party or outsource (e.g., vendor)
- 21% Account takeover
Combating payments fraud

Daily monitoring
Secure check stock
Online payment solutions
Internal controls
Shred documents

A look at fraud practices and scams

Sara Larsen
VP, Treasury Solutions Consultant
Bremer Bank

What kinds of fraud attempts are businesses facing today?
- Business email compromise
- Email account compromise
- Check fraud
**Business email compromise (BEC)**

Targets businesses who perform a lot of wire transfers, especially to foreign suppliers

Uses social engineering or computer intrusion techniques

Lucrative (for the fraudsters): FBI states that over $26 billion stolen from over 166,000 victims in 3 years

---

**A common hallmark of BEC: It looks real**

- Target the “money movers”
- “Kindly,” “Urgent,” “Secret,” “Confidential”
- Closely mimic legitimate email addresses
- Well-written
- Positioning around executives

---

**Payroll diversion**

HR representative receives email requesting update to employee’s direct deposit

Typically, the new direct deposit is directed to a prepaid card account

This approach has resulted in over $8.3 million in losses in just 18 months

---

19

20

21
How can you prevent BEC from happening to you?

Simple steps:

- Leak clearly
- Protect privacy
- Click with caution
- Triple check

Some even better steps:

- Educate your employees
- Protect and monitor your networks
- Periodically review email rules
- Establish dual controls

Check fraud

- Check forgeries: unauthorized issuance or stolen checks
- Check alterations: changes to payee or amount made by hand or chemical
- Counterfeit checks: closely mirror check stock of business
What if your business is a victim of fraud?

Act immediately:
- Contact your financial institution
- You may need to close your account - OR - enroll in fraud prevention tools
- File a police report
- File a report on ic3.gov

FBI Internet Crime Complaint Center
https://www.ic3.gov

Mitigating payments risk

Deb West, CTP
VP, Treasury Solutions Consultant
Bremer Bank

Why is fraud prevention so important on business accounts?
- UCC allows shorter return windows on business accounts than consumer accounts
- Businesses are increasingly targeted for BEC attacks and more
- Check fraud is an ongoing risk
- An attack puts your operation at risk – and diverts your resources
Many fraud prevention tools are just a click away

Our Positive Pay lineup:

**Positive Pay**
- Protect against check fraud

**ACH Positive Pay**
- Protect against “check washing” alteration schemes

**Payee Verification**
- Safeguard against ACH fraud by reviewing payee information

**Debit-Block**
- The ultimate in control, with all debits/payments blocked until further review

---

How it works:

**Positive Pay**

Save your check data to a file

Upload file to Online Banking

You review the “exceptions” – items presented for payment that don’t match your original file

You submit decisions to pay or deny each exception item

---

How it works:

**Positive Pay + Payee Verification**

Even stronger protection against check fraud

Additional check verification measures, ensuring payee match

Particularly valuable for guarding against “check washing” and other chemical alterations of checks

---

28

29

30
You can take extra steps to boost your safeguards

- Dual controls
- Internal controls
- Mobile access
- Non-response settings
- Daily reviews
- Secure check stock
- Timely shredding of materials
- Integrated Payables

<table>
<thead>
<tr>
<th>How it works:</th>
<th>ACH Positive Pay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online files of approved debits that you upload to Online Banking</td>
<td></td>
</tr>
<tr>
<td>Ability to create “approved lists” of vendors and associated limits</td>
<td></td>
</tr>
<tr>
<td>User entitlement limits and dual controls</td>
<td></td>
</tr>
<tr>
<td>Exceptions can be reviewed and decisioned in Online or Mobile Banking</td>
<td></td>
</tr>
</tbody>
</table>

How it works: Debit Block

Ability to prohibit specific debit transactions
Available on ACH debits and check debits