

Eastern Bank Business Confidence Survey – Q2 Results

Results from the Eastern Bank Commercial Banking division survey conducted in collaboration with AIM:

- Business Confidence Index - positive gains compared to Q1'26
- Company Confidence Index – multi-quarter increases as clients are confident in their own firms.
- Current / Future Confidence Index – measures sentiment at time of survey and in six-months. Both showed positive signs in Q2. Future sentiment was higher for Eastern Bank clients than that of Statewide participants.

Q2 perspectives:

- Investor sentiment remains optimistic but sensitive to inflation data. The 24% increase in diesel fuel prices in August create headwinds and consumer pressure. Long term rates remain volatile with recent inflation and employment reports. The market is at 90% odds of a 25bps rate hike this week, further tightening into 2027.

Current Loan Covenants - A&E Firms

- Your Bank should recognize the unique nature of your business where “your assets go home each night”. Loan structures should acknowledge goals and objectives of professional services firms.
- Performance can be measured on pre-distribution profit recognizing discretionary nature of compensation plans.
- Cash flow available for Debt Service (Debt Coverage Ratio) and Balance Sheet leverage (Total Liabilities / Tangible Capital Base) are common measurements.

Fraud and Risk Awareness



Threat Landscapes: Social Engineering

Motive: Capture financial, personal or business information for fraudulent use or direct the recipient to act (e.g. wire funds, change account information)



Spoofing

Impersonate someone familiar to target (imposter fraud) or spoof a website



Spear Phishing

Specific population, targeted individual (e.g., specific company)



Whaling

High profile/ranking individual (CFO or Finance department)



Vishing

Via phone or voice message (IRS calls, tech support, elder abuse) *This is an ever-growing threat.*



Phishing

General population, email sent to induce a person to reveal personal info

TOP Current Events/Threats for Businesses

- ✓ **ACH Credit Micro Entry Fraud:** Fraudster initiates small micro credit, waits, then debits the account.
- ✓ **Check Fraud:** Still popular, increased during the pandemic and now stolen mail has increased.
- ✓ **Business Email Compromise (BEC):** BEC is a scam targeting businesses working with domestic and foreign suppliers and/or businesses regularly performing wire transfer payments. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds. Vendors are increasingly getting their email compromised and targeting their customers in addition to lawyers and title companies.
 - ✓ Accounts Payables (AP) Teams often targets
- ✓ **ACH Payment Fraud:** Occurs during BEC or as spoofing. This is why it is so critical that customers verify any payments or payment change information VERBALLY on the phone.
- ✓ **Ransomware:** A type of malicious software designed to block access to a computer system until money is paid.

Get the full report at FBI Internet Crime Complaint Center (IC3) www.ic3.gov

Best Practices & Value-Added Resources

- ✓ ***The Reality: Accounts Payable Departments overwhelmingly targeted by fraudsters***
- ✓ **Being proactive rather than reactive means being prepared:** Reconciling and utilizing services such as ACH and Check Positive Pay are always recommended. The daily practice of reconciliation and the utilizing PP services are the very best ways to manage fraud at the account level. Utilize the Eastern Treasury platform for account information and **setup transaction alerts** to help monitor ACH fraud. In light of recent uptick in ACH micro entry fraud, the alerts are more important than ever.
- ✓ **Fraud Awareness Education:** Fraud awareness education at a minimum on an annual basis. Stay informed with up-to-date fraud information and keep the discussion open for conversation.
- ✓ **Ransomware attacks:** Be prepared to back up data early and often, this helps mitigate exposure during a ransomware attack.
- ✓ **Understanding responsibility.** This is important around sharing Personally Identifiable Information (PII), such as payroll data and login/passwords to secure sites.