ALTAMAHA Bank & Trust

Michaela McCoy
INFORMATION SECURITY OFFICER
michaela.mccoy@altamaha.bank

FRAUD AWARENESS AND PREVENTION FORUM RECAP

Tuesday, August 16th

Our goal is to help the community stay informed of current fraud & scam tactics used by criminals. We want to help prevent you, your business, your loved ones, from suffering financial losses. Please talk to your young adult children and elderly loved ones to help educate them on ways to avoid scams.

Altamaha Bank is Committed to Fight Fraud.

Banks have a responsibility and are deeply committed to protecting customer information. At Altamaha Bank we:

- Invest heavily in **Cyber Security** protections like Firewalls, Anti-virus, regular software updates, Audits
- **Require employees to have secure passwords** and multifactor authentication when accessing bank computers
- Regularly **Train** employees on fraud trends & verification procedures
- We can't look at every transaction or every check clearing, but we have software that enables us to see **large dollar checks** clearing. We also manually **compare** your signatures on large checks to your signature card.
- If check numbers are way out of sequence, as this is an indication that fraudulent checks are possibly trying to clear, your account is also **flagged** for our review.
- **Terri Sands, Managing Director of Secura Risk Management at Stout,** recently conducted an Onsite Employee Fraud Training for Altamaha Bank. She and her company have partnered with community banks for fraud training and mitigation for many years.

SECURA STOUT

FRAUD AWARENESS AND PREVENTION FORUM RECAP CONTINUED

Practical Tips:

- Remember, your bank will NEVER contact you to ask for account #, passwords, pins, social security number, or security codes. Don't let someone trick you into giving up personal information and don't trust the caller ID. Hang up and call your banker to verify.
- Fraudsters have ways of making text messages, phone calls, emails APPEAR as if coming from your bank. This is called spoofing. Fraudsters also pretend to be people within your own organization, someone you know, Amazon, your electric company, etc.
- Stay in the know by:
  - Reviewing your bank account transactions regularly using your Mobile App
  - Enabling debit card text alerts
  - Enabling activity alerts
- People 2 People Payment Options(CashApp, Venmo, PayPal, and Zelle) are convenient but, remember:
  - Never send money to people you don't know.
  - These payment apps are intended for sending money to people you know and trust personally. Not to purchase items from people you don't know or to purchase items online.

Ways that Small Business Owners can Mitigate Risks

Remember, there's not a one size fits all approach. Every business is different so each will need to evaluate their own risks and determine what works best for you.

- Look into Cybersecurity Insurance.
- Train your employees on Email Phishing Scams and other Cyber Risks.
- **Business Email Compromise (BEC)**
  - A common BEC Scam Scenario: The email address of someone you do business with has been hacked. The fraudster sends the employee in your business who handles accounts payable an email or regular invoice indicating their payment terms have changed. The employee pays the invoice not realizing the payment has been sent to the fraudster's account. Unfortunately, the money is now sent and you're unable to get it back.
  - Implement procedures at your business to require verification of emailed payment term changes. Calling an existing telephone number is a simple procedure to get started with.
- **Check Fraud:**
  - Payables checking accounts are the most susceptible to fraud. **Therefore, payables checking accounts should only have funds needed to cover checks you've issued.**
  - We recommend that you place the rest of your money in a reserve account. This account can be at the same bank.
  - Be sure to block ACH debits on the reserve account and to not have checks ordered at any time.
  - Simply use Online Banking to transfer funds from the reserve account to your payables account with each check run.
  - Designate someone in your office to review transactions clearing every day first thing in the morning.
  - Try to get in the practice of reviewing account activity prior to 10 am each business day. If you see a fraudulent check or transaction, notify your bank immediately.

FRAUD AWARENESS AND PREVENTION FORUM RECAP CONTINUED

Positive Pay: An Automated Tool to Help Small Businesses

- Banks have offered Positive Pay to business customers for many years, but recent technology has made it much more automated.
- Positive Pay is truly a Fraud Deterrent **tool** for businesses who regularly issue checks payments and to help business owners protect themselves against fraudulent checks written on their account.
- It truly **saves you time** in manually reviewing checks clearing.

Here's how it works:

- You simply upload your electronic check register into online banking.
- Positive Pay **AUTOMATICALLY** verifies checks clearing against your check register and shows you any exceptions.
  - Exception Examples would be checks not in your check register due to the dollar amount being different or a check # doesn't match.
- A designated person in your office will review transactions clearing every day first thing in the morning.
- If you see a fraudulent check or transaction while reviewing the images of the exceptions, you will have the opportunity to **return it by 10 am.**
  - A check exception will remain in a Paid status unless you select to return it.
- Please talk to your personal banker to see if Positive Pay is a good fit for your business.

Helpful Links for Businesses and Consumers:

Educational Handouts are available on our website: https://altamaha.bank. Type Fraud in the search bar, or navigate to Manage > Fraud Awareness and Prevention.

The PowerPoint presentation from our guest speaker Todd Renner will be emailed to participants that registered in advance. If you did not register in advance, simply email valerie.mclendon@altamaha.bank and she will put you on the mailing list.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

https://www.ftc.gov/business-guidance/small-businesses
https://www.ftc.gov/business-guidance/resources/scams-your-small-business-guide-business
https://consumer.ftc.gov/scams
https://consumer.ftc.gov/consumer-alerts/2022/04/how-do-you-spot-scam-listen-how-someone-tells-you-pay

Internet Crime Compliant Center
https://www.ic3.gov/
https://www.ic3.gov/Media/Y2022/PSA220504