Defending yourself against the Fraud Epidemic

AMERIS BANK

Member FDIC

EQUAL HOUSING LENDER

Association for Financial Professionals Fraud and Control Survey Statistics

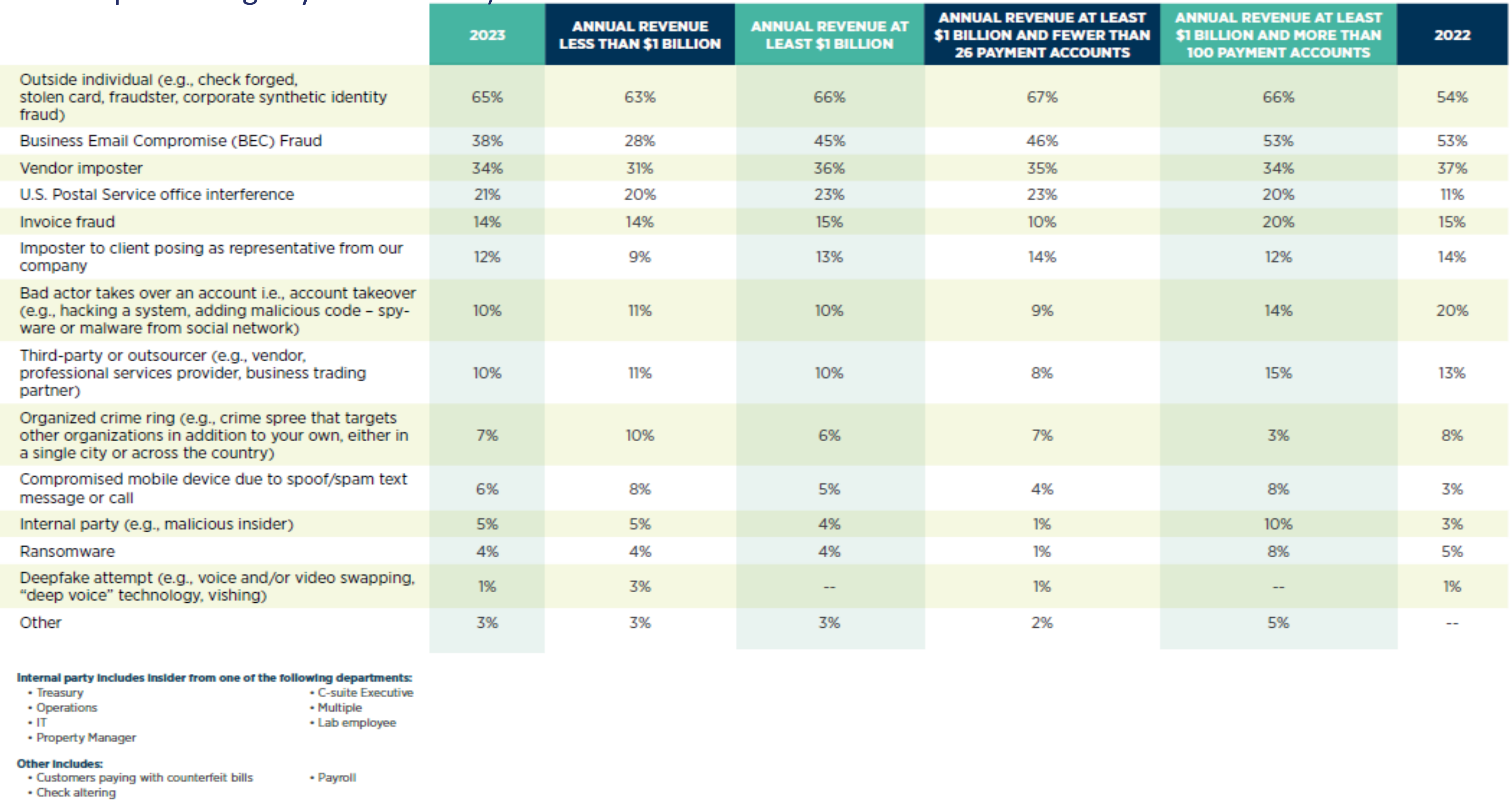
2024 AFP Payments Fraud and Control Survey Report-Comprehensive Report

- 80% of organizations were victims of attempted or actual fraud in 2023, on the rise since dropping below 80% in 2020 and at 65% in 2022.
- Payment methods impacted by Fraud:
  - 65% Checks
  - 24% Wires
  - 35% ACH Debits, 20% Credit cards, 19% ACH Credits
- 63% of organizations have been subject to attempted or actual Business Email Compromise (BEC)
  - Increased vigilance has reduced this from a high of 80% in 2018
  - 34% of organizations reported financial losses as a result of Business Email Compromise
- 77% of BEC Fraud is from spoof emails, 52% from Domain lookalike emails and 43% from a legitimate email taken over by a fraudster
- 60% of payments fraud is discovered by treasury staff
- 40% of organizations discovered fraud less than two weeks after the incident occurred

Sources of Attempted Fraud

2024 AFP Payments Fraud and Control Survey Report-Comprehensive Report

Sources of Attempted/Actual Payments Fraud Attempts (Percentage of Organizations Experiencing Payments Fraud)



	2023	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS	2022
Outside individual (e.g., check forged, stolen card, fraudster, corporate synthetic identity fraud)	65%	63%	66%	67%	66%	54%
Business Email Compromise (BEC) Fraud	38%	28%	45%	46%	53%	53%
Vendor imposter	34%	31%	36%	35%	34%	37%
U.S. Postal Service office interference	21%	20%	23%	23%	20%	11%
Invoice fraud	14%	14%	15%	10%	20%	15%
Imposter to client posing as representative from our company	12%	9%	13%	14%	12%	14%
Bad actor takes over an account i.e., account takeover (e.g., hacking a system, adding malicious code – spy-ware or malware from social network)	10%	11%	10%	9%	14%	20%
Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	10%	11%	10%	8%	15%	13%
Organized crime ring (e.g., crime spree that targets other organizations in addition to your own, either in a single city or across the country)	7%	10%	6%	7%	3%	8%
Compromised mobile device due to spoof/spam text message or call	6%	8%	5%	4%	8%	3%
Internal party (e.g., malicious insider)	5%	5%	4%	1%	10%	3%
Ransomware	4%	4%	4%	1%	8%	5%
Deepfake attempt (e.g., voice and/or video swapping, "deep voice" technology, vishing)	1%	3%	--	1%	--	1%
Other	3%	3%	3%	2%	5%	--

Internal party includes insider from one of the following departments:

- Treasury
- Operations
- IT
- Property Manager
- C-suite Executive
- Multiple
- Lab employee

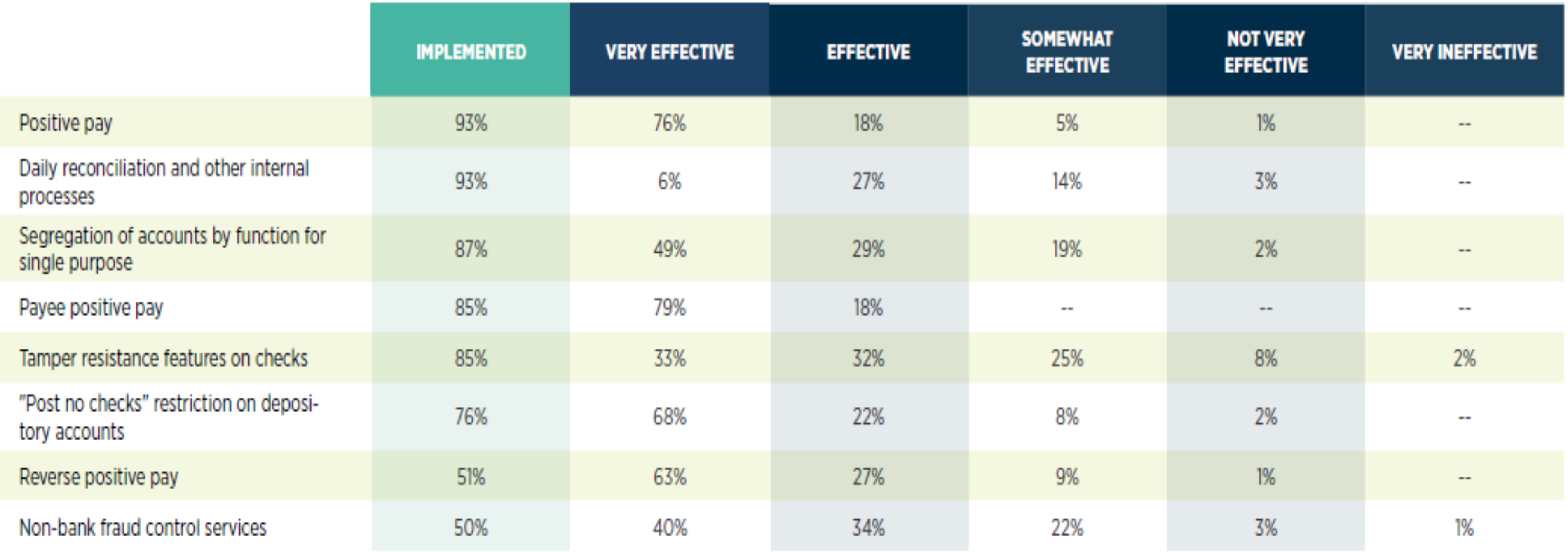
Other includes:

- Customers paying with counterfeit bills
- Check altering
- Payroll

Controlling Check Fraud

2024 AFP Payments Fraud and Control Survey Report-Comprehensive Report

Effectiveness of Fraud Control Procedures and Services used to Protect Against Check Fraud

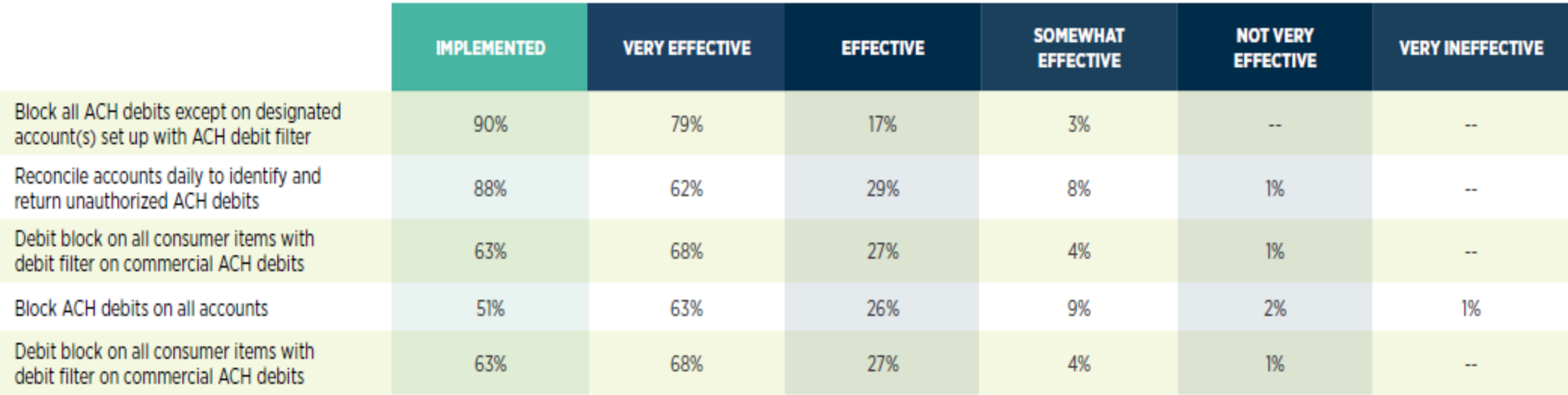


	IMPLEMENTED	VERY EFFECTIVE	EFFECTIVE	SOMEWHAT EFFECTIVE	NOT VERY EFFECTIVE	VERY INEFFECTIVE
Positive pay	93%	76%	18%	5%	1%	--
Daily reconciliation and other internal processes	93%	6%	27%	14%	3%	--
Segregation of accounts by function for single purpose	87%	49%	29%	19%	2%	--
Payee positive pay	85%	79%	18%	--	--	--
Tamper resistance features on checks	85%	33%	32%	25%	8%	2%
"Post no checks" restriction on depository accounts	76%	68%	22%	8%	2%	--
Reverse positive pay	51%	63%	27%	9%	1%	--
Non-bank fraud control services	50%	40%	34%	22%	3%	1%

Controlling ACH Fraud

2024 AFP Payments Fraud and Control Survey Report-Comprehensive Report

Effectiveness of Controls in Mitigating ACH Debit Fraud (Percent of Organizations)



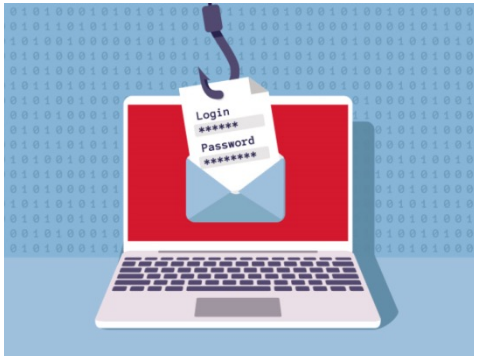
	IMPLEMENTED	VERY EFFECTIVE	EFFECTIVE	SOMEWHAT EFFECTIVE	NOT VERY EFFECTIVE	VERY INEFFECTIVE
Block all ACH debits except on designated account(s) set up with ACH debit filter	90%	79%	17%	3%	--	--
Reconcile accounts daily to identify and return unauthorized ACH debits	88%	62%	29%	8%	1%	--
Debit block on all consumer items with debit filter on commercial ACH debits	63%	68%	27%	4%	1%	--
Block ACH debits on all accounts	51%	63%	26%	9%	2%	1%
Debit block on all consumer items with debit filter on commercial ACH debits	63%	68%	27%	4%	1%	--

The Threat Landscape:

Business Email Compromise

Business Email Compromise

- Posing as Senior Executives in emails
- Impersonating Vendors
- Pretending to be other third parties



Other Types of email used in attacks are:

- Faxes requesting revisions to bank accounts
- Emails from fraudsters who hacked Senior Executives
- Emails impersonating HR Departments
- Emails requesting change in payroll info

Business Email Compromise:

Mitigation Best Practices- WIRES

Wire transfers are Once Again Prime Target for BEC Scams

- Educate your staff about the fraud risks inherent in their daily processes. Training, training and more training!
- Create a culture that empowers employees to ask questions.
- Develop a process for wire validation that includes access to key executives for approval.
- Employ dual approval for funds movement.
- Verify important or large transactions through an alternate method.
- Limit the amount of public information available about your company's internal operations.
- Conduct all banking on a dedicated machine used for no other task.
- FOLLOW YOUR OWN PROCEDURES!!!!!!

Business Email Compromise:

Mitigation Best Practices - Payables

- Train associates on all vendor management policies.
- Empower employees to ask questions when in doubt.
- Know your vendor.
- Plan how your vendor will connect with you.
- Validate changes to vendor master file.
- Require verbal confirmations.
- Vendor lists should be kept in a hard copy file.
- New vendor system.
- FOLLOW YOUR OWN PROCEDURES!!!!!!

Stronger Internal Controls prohibiting payments initiation based on emails or other less secure messaging systems

76%

Education and training on the BEC threat and how to identify phishing attempts

76%

Implementing company policies for providing appropriate verification

68%

Adopted at least a two-factor authentication or other added layers of security

65%

The Threat Landscape:

Ransomware

Ransomware Statistics and Facts

Rate of Ransomware Attacks

- A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021 (source: Cyber Security Ventures)
- 1.5 million new phishing sites are created every month. (Source: webroot.com)
- Ransomware attacks have increased over 97 percent in the past two years. (Source: Phishme)

Statistics on Ransomware Demands

- An IBM study suggested that over a quarter of all companies would pay more than $20,000 to hackers to retrieve data that had been stolen.
- Ransomware generates over $25 million in revenue for hackers each year. (Source: Business Insider)
- More than half of ransoms were paid bitcoin.

FBI Tips and Preventative Measures

(www.FBI.gov)

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP Addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set and anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrators accounts should only use them when necessary.

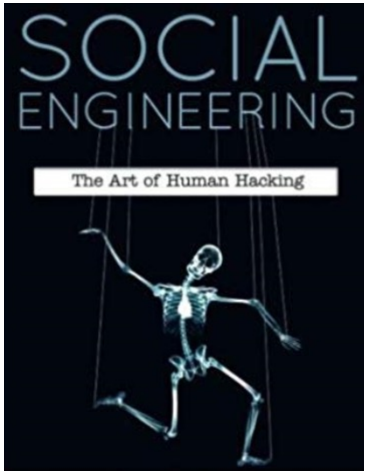
The Threat Landscape:

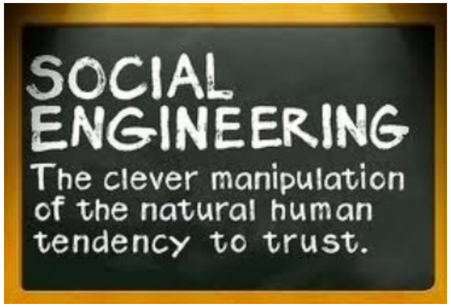
Beware of Online Risks

Social Engineering

Social engineering attacks are a type of cybercrime wherein the attacker fools the target through impersonation. They might pretend to be your boss, your supplier, someone from our IT team, or your delivery company. Regardless of who they're impersonating, their motivation is always the same — extracting money or data

- Phishing (Email)
- Smishing (text Message)
- Vishing (Voice/Phone)
- Twishing (Twitter - X)
- Search Engine Poisoning (Malicious Websites)
- Trusted Site Compromise
- Malvertising (the use of online advertising to spread malware)
- Scareware (scaring individuals into buying dangerous software)
- Fake Mobile Apps
- Email Account Updates
- Social Engineering!!!!!!!!!!




SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

Phishing Top Traps

Top Social Media Email Subjects

- LinkedIn: "Add me" "Join Network" "New Message"
- Login Alerts
- Tagged Photo
- Free Pizza
- New Voice Message
- Unread Message

Top Social Media Email Subjects

- Official Data Breach Notification
- UPS Delivery
- IT Reminder: Password Expiration
- Change Password Required Immediately
- Please Read- Important from Human Resources
- All Employees- Update your Healthcare Information
- Revised Vacation & Sick Time Policy
- Company Survey

AVOID FRAUD

Recommendations

12 Risk Mitigates Every Business Should Perform

1. **Initiate Background Checks** on **ALL** employees and contractors
2. **Have a Fraud Plan** and test it routinely, run simulations and drills
3. **Conduct an Assessment** to know how money leaves your business
4. **Leverage Bank Account Design Structure** to increase risk controls
5. **Mandate Process Controls** including dual control and segregation of duties
6. **Manage Employee Access** based on necessary job functions
7. **Isolate a Computer** for banking and payment initiation
8. **Inspect Bank Accounts Daily** and reconcile "frequently"
9. **Use Fraud Prevention Services** like Positive Pay, Payee PPay, ACH Blocks & Filters, etc.
10. **Pick up the Phone** to authenticate ALL requests
11. **Notify the Bank and Law Enforcement** if you are under attack (see IC3.gov)
12. **Cultivate a Risk Management Culture** to further ensure controls

Stay in touch!

Seanne Holliday CTP, CAMS
912.433.1734
Seanne.holliday@amerisbank.com