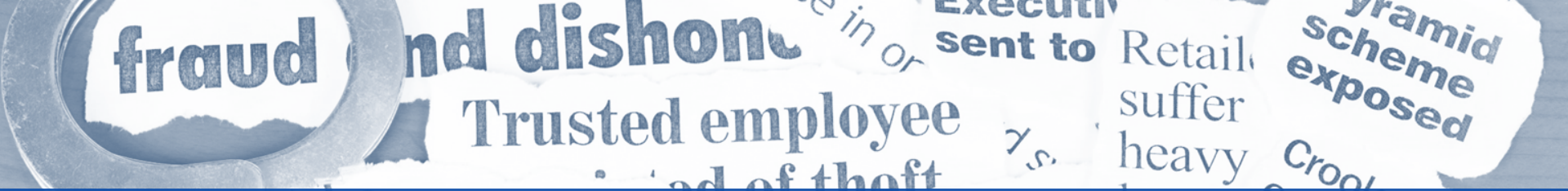
Dannible & McKee, LLP

Certified Public Accountants and Consultants

Delivering **Confidence**



Emerging Fraud & How to Protect Your Assets

Presented by:
Brian W. Johnson, CPA, CFE, Audit Partner and
Kaitlyn A. Hensler, CPA/CFF, CFE, Senior Audit Manager
Dannible & McKee, LLP

Dannible & McKee Fraud Prevention Conference
September 15, 2021

Agenda

- Corporate Credit Card and Reward Points Programs Fraud
- Fraudulent Remittance Losses and Unauthorized Asset Sales and Shipments
- Preparing for a Post-Pandemic Fraud Landscape

Corporate Credit Card and Rewards/Points Program Fraud

Corporate Credit Card Fraud

- Corporate credit cards offer a ton of benefits; however, they can leave businesses vulnerable to employee misuse.
  - Employees may overspend.
  - Make unauthorized transactions.
  - Submit erroneous expense reports.
  - Diversion or use of reward points for personal purchases.

Corporate Credit Card Controls to Consider

- Controls over establishing and approval of new accounts.
- Management review of addition process.
- Management review of activity on corporate card accounts.
- Economic crime insurance.

Corporate Credit Card Master Account With Points Program Fraud Scheme

- Company officer transfers points from corporate master account to his own personal account:
  - Numerous personal extravagant purchases on a continuous basis, remaining undetected for years.
  - Family vacations.
  - Trips for wife to support her personal ventures and activities.
  - College visits with children.
  - Concert tickets.
  - Benefits for parents: travel, hotel, sports tickets.
  - And on and on (use your imagination).

Corporate Credit Card Master Account With Points Program Fraud Scheme

- Events that followed:
  - Company officer retires.
  - New company officer reviews email activity of departing officer.
  - During review, suspicious activities detected, inquiries to CFO provide further sense of a problem afoot.
  - DM engaged, obtains all hard drives from departing officer's computer.
  - DM performs forensic review of hard drive data, includes several years of email activity.
  - Dozens of suspicious emails both indirectly and directly implicating both the departing officer and CFO. Collusion!
  - DM report aids law enforcement in proceeding on toward next steps in recovery.

Corporate Credit Card Master Account With Rewards Points Program Fraud Scheme

- Controls to be considered:
  - Controls outlining usage of corporate credit card program.
  - Policy and procedure as to ownership of and acceptable use of card reward points.
  - Are points Company property or Employee property?
  - Employee compensation?
  - Include points value in employee's W2 earnings?
  - Taxes paid by employee on the value of the compensation represented by points received.

Fraudulent Remittance Losses and Unauthorized Asset Sales and Shipments

Accounts Receivable / IT Systems Fraud How Many Internal Controls Weaknesses Can You Find?

- Company's email server compromised via a phishing attack.
- Fraudsters accessed email account of Accounts Receivable clerk.
- Obtained full access to A/R clerk's Outlook account.
- Fraudsters were able to monitor everything the clerk was doing in Outlook: access to the contacts list, all email addresses relating to customer accounts.

Accounts Receivable / IT Systems Fraud How Many Internal Controls Weaknesses Can You Find?

- Each day, the A/R clerk forwarded Accounts Receivable aging reports by email to upper management for review of status. All customer balances and aging were shown.
- Fraudsters obtained the A/R aging report with client detail and balances owed.
- Fraudsters created a website with same exact same web address as the company, with one character off (one “T” instead of the normal two “T”’s).
- Fraudsters generated an email to all customers informing them the company was no longer accepting check payments. Payment now only possible through the new website.

Accounts Receivable / IT Systems Fraud How Many Internal Controls Weaknesses Can You Find?

- The scheme was discovered when the collections department made collection calls to ask customers why payment was not being made on their accounts.
- Scheme operated approximately three weeks before detection.
- Company is still in the process of trying to recover receivables payments, issues abound.
- Customer payments have all been lost to fraudsters.

Accounts Receivable / IT Systems Fraud How Many Internal Controls Weaknesses Can You Find?

- **Unclear at Present**:
  - Who is responsible for the loss: the Customer or the Company?
  - Does Company risk angering the customer by asserting the Company was never actually paid: the Customer should have been diligent enough to notice they were sending payment to a fraudulent site?
  - Does the Company absorb the loss as a cost of maintaining good customer relations?
  - Did the Company have economic crime/fraud insurance in place to reimburse this loss?

Accounts Receivable / IT Systems Fraud

Control Weaknesses:

- **The Customer**
  - Missed detection of payment website as fraudulent (perhaps understandable but under the circumstances the instructions to change payment process should be reviewed with management).

Accounts Receivable / IT Systems Fraud

Control Weaknesses:

- **The Company**
  - IT: Failure to properly secure the internal IT environment.
  - Finance group: emailing documents with customer information (hard to avoid in practice).
  - Insurance policy coverage deficient.

Accounts Receivable / IT Systems Fraud

- All A/R reports now centrally-located on private Company intranet. Emailing has been discontinued!
- IT: Employee education, anti phishing security tests, policy/procedure/software updates and improvements.

Shipment Address Fraud Relating to Online Sales

- Fraudsters established fraudulent PayPal accounts.
- Ordered multiple inventory items on the client's website.
- Once the inventory was delivered, fraudsters did not pay PayPal. (Presumption is that merchandise acquired was resold for cash).
- PayPal identifies that address and payment information are fake following their investigation: PayPal does not absorb the loss. Company was forced to record a loss on the sales and inventory.
- Client loss: approximately $35,000 expensed in 2020 due to fraudulent PayPal sale transactions.

Shipment Address Fraud Relating to Online Sales

- Company caught onto the scheme after a few months as it investigated aging receivables originating through PayPal transactions; implemented policies and procedures to prevent further instances. Overall, the loss was immaterial to the financial statements.
- **But that's not the point!** The instance highlighted a defect in internal controls.
- Management implemented an effective fraud mitigation regime to preclude reoccurrence of this particular manner of fraudulent sales in the future.
- A **robust body of policy and procedures were implemented** to target the weaknesses that were identified which attributed to the fraud.

Identifying Fraud – Customer Controls

- **Overall:** Customer online orders will automatically be flagged by the website with the “Hold CC-Fraud” product type once imported into software revenue module. Then review!
- Manual equivalent is to identify and download daily orders and review before shipment…catch the problems up-front!

Identifying Fraud – Customer Controls

- Review Considerations:
  - A customer is requesting overnight shipping for an expensive order.
  - How to handle credit checking for online purchases for amounts exceeding specified levels? Customer Service interaction with customer on a live basis?
  - Is the Shipping Address Suspicious?
  - The shipping address is a high-risk location (vacant property, hotel, etc.)
  - The billing and shipping addresses are substantially different (same state, different zip codes).
  - The IP address of the customer is very far from (in another state) from the shipping address.
  - Multiple orders are being shipped to the same address within a short period of time.
  - A customer asks you to change the shipping address after the order is invoiced.

Identifying Fraud – Customer Controls

Does the Order Seem Unusual or Suspicious?

- The main item on the order has an unusual quantity (more than 2 of Product 1, more than one 6-pack of Product 2, based upon customary or expected sales quantities to traditional customers.)
- The same customer (same name, email, phone, or computer IP) places a large quantity of orders within a short time.
- A customer offers to let you use their shipping service to receive a discount (i.e., customer controls where orders are shipped).
- An abnormally large number of orders is placed during an unusual time of day.

Identifying Fraud – Customer Controls

Is Your Customer Exhibiting Suspicious Behavior?

- The customer's email address is using a temporary or "bogus" website (@email.test, @protonmail.com, @mail.com, test@test.com, etc.).
- The customer email address looks like a name, but it's very different than the customer's name given (Name: Jimmy John, Email: nickytony@yahoo.com).
- The customer's email address is very generic (firstnamelastname##@yahoo.com).
- Recent claims or chargebacks from this customer.

Identifying Fraud – Customer Controls

Reviewing Orders

- During each online order import, the importer should review the open online orders to find any that are marked as *Suspicious*.

Identifying Fraud – Customer Controls

Was the Order Correctly Flagged?

- For each order, review it using the Identifying Fraud criteria to see if it needs further verification or it was flagged by mistake. Here are some examples of a false positive:
    1. The order has **multiple quantities of a Product**, but it's clearly for an established vendor or a large organization that would have need of it. This could be evident by their company name, email domain, etc.
    2. The **bill-to and ship-to zip codes are different**, but both addresses match with the customer's company name after a quick search online.
    3. The **customer has a good standing relationship with the Company**: they are an established customer with no record of fraud.
- In the case of a false positive, at the rep's discretion, the order can be unmarked prior to import. Change the entries under the Suspicious column in the order import sheet to No – make sure to do this for every row of the order. Changing this to No will prevent it from being put on hold in the revenue system.

Identifying Fraud – Customer Controls

Verify of Orders and Policy Education/Instructions to Customer Service Team

- If an order is still suspicious after the initial review for false positives, two tactics further combat fraud: **Verify** and **Delay**.

  1. If an online order is imported to the revenue system with the "*Hold CC-Fraud*" product type, leave it alone for at least 7 calendar days. **Do not contact the customer or change the order product type / status.**

     a) This waiting period is to give the cardholder time to dispute the claim if it is fraudulent and to make sure that Production doesn't ship out the order.

Identifying Fraud – Customer Controls

Verify of Orders and Policy Education/Instructions to Customer Service Team

2. After the suspicious order has been on hold for 7 calendar days, send an email to the customer:

Hello <CUSTOMER NAME>,

Your recent order is temporarily on hold while your payment is reviewed. At your earliest convenience, please contact us from the phone number listed on the original order confirmation to verify your purchase.

If we do not hear from you within 7 days, your order will be cancelled.

Identifying Fraud – Customer Controls

Verify of Orders and Policy Education/Instructions to Customer Service Team

a) If you are contacted by the customer prior to this initial 7-day period, tell them that the order is on hold while the payment is verified.

b) If you are asked to explain the delay, tell them that it's so the bank can confirm the buyer's identity before allowing the sale.

c) If they press on you for more information or demand it be expedited, respectfully refuse and explain that our process is put in place to protect our customers identities.

d) If you are contacted regarding an order from an email address different from the one on the original order (and it's not an obvious typo or another individual from the same company email address), tell them that they need to contact you from the original email.

e) Do not provide any details of the original order to the customer. The exception being the order number itself (in case they had multiple orders that were flagged).

Identifying Fraud – Customer Controls

Verify of Orders and Policy Education/Instructions to Customer Service Team

3. When you are called by the customer's original phone number, ask them to verify the following details:
    a) Full Name
    b) Full Billing and Shipping Addresses
    c) Explanation of Mismatched Name & Email Address (if applicable)
    d) Explanation of Different Billing/Shipping Address (if applicable)
    e) Explanation of the Address' Risky Location (if applicable)
    f) Explanation of Odd Item Quantities (if applicable)

Identifying Fraud – Customer Controls

Verify of Orders and Policy Education/Instructions to Customer Service Team

4. When they are finished, read full name, billing and shipping address back to them to confirm.
5. If all the details are correct and you feel that the order is no longer suspicious, proceed to the Approving Orders section below.
6. **If any of these are wrong and/or do not match the original order, do not tell them which details are incorrect. Simply thank them for their response and tell them you will unfortunately need to cancel the order.**
    a) They are free to resubmit it at their discretion or place the order via Amazon/another reseller.
    b) Recommend to them to resubmit using a PayPal account on our website to have the smoothest ordering process and quickest validation.

Preventing Fraud Risks - Online Payment Processing

Use of Online Payment Processors (e.g., PayPal)

- Online should be treated exactly the same as bank accounts.
- Management should review a “bank reconciliation” of all online accounts monthly.
- User ID and password combinations should be changed frequently.
- Credentials should be assigned only to the minimum number of people required, based upon job duties and the principle of least privilege.
- Upper-level management should always be in possession of the current access credentials and confirm the ability to access the accounts.

Preventing Fraud Risks - Online Payment Processing

Use of Online Payment Processors (e.g., PayPal)

- Monitor accounts for unusual or unexpected activity: shipments to unknown addresses, unusual quantities, foreign transactions.
- Enable fraud alerts available to account owners and route delivery to the appropriate addresses.
- Unusual activity should be followed up on immediately to ensure the company's ability to recover lost funds should a fraud occur.
- Take care to avoid interaction with phishing emails designed to fraudulently obtain access credentials.

Preparing for a Post-Pandemic Fraud Landscape

Preparing for a Post-Pandemic Fraud Landscape

- Shifts in business operations, economic impacts, and changes in consumer behavior due to the pandemic will likely remain significant factors affecting entities going forward.
- In turn - fraud risks have also been affected and anti-fraud programs must evolve with them.
- To assess how organizations are preparing for the “next” normal, the Association of Certified Fraud Examiners (ACFE), in collaboration with Grant Thornton, surveyed anti-fraud professionals around the globe regarding the current and expected effects of COVID-19 on the fraud landscape.

Changes to the Levels of Fraud and Fraud Awareness Post-Pandemic

51% of organizations have **uncovered more fraud** since the onset of the pandemic

71% expect the **level of fraud** impacting their organizations to **increase** over the next year

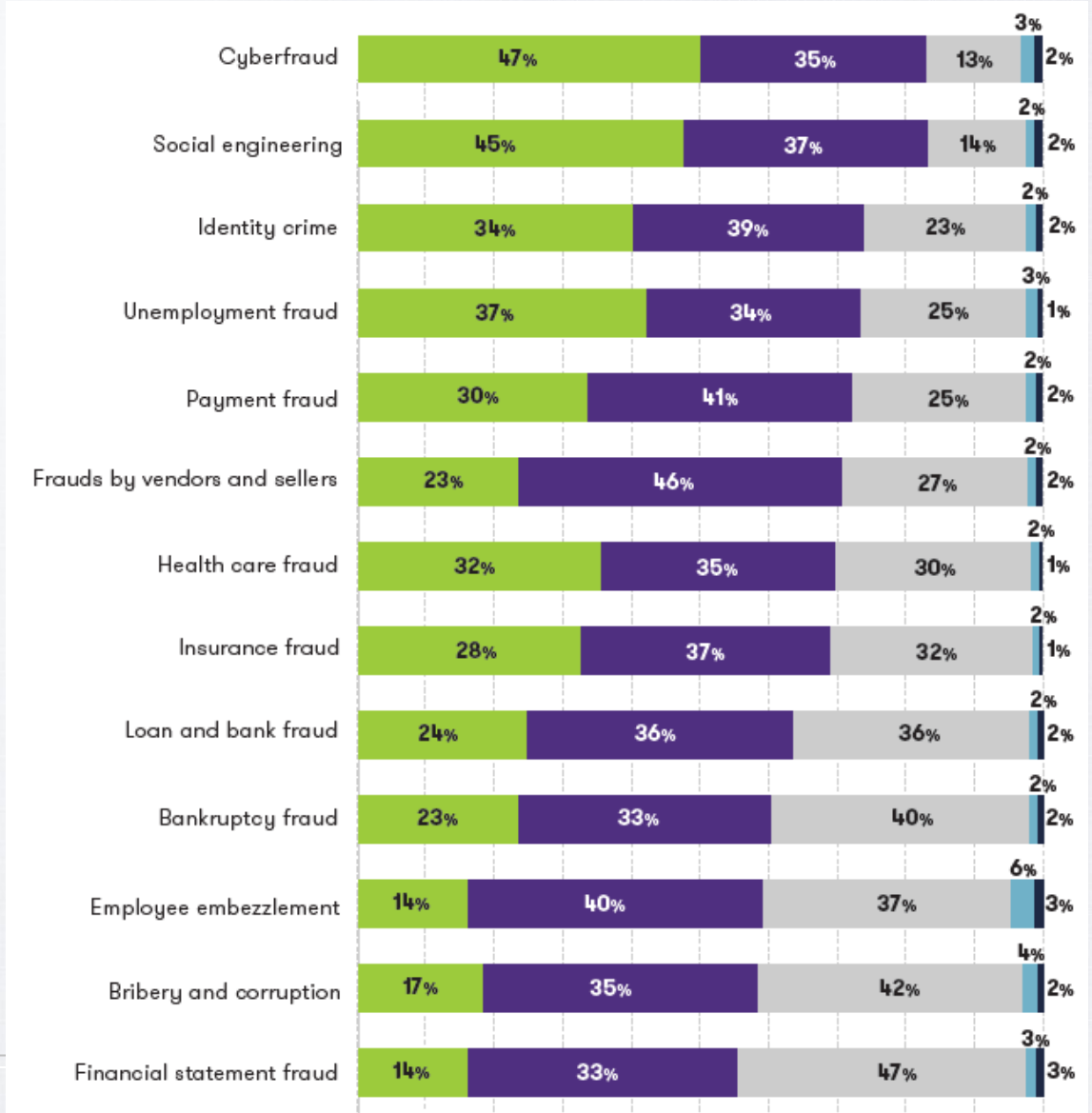
More than **80%** of organizations have already implemented **one or more changes** to their **anti-fraud programs** in response to the pandemic

ACFE and Grant Thornton: Preparing for a Post-Pandemic Fraud Landscape Survey 2021

How Are Fraud Risks Expected To Change Post-Pandemic?

- Most respondents expect increases in all types of fraud risks.
- More than half of respondents expect to see increases in every category except one (financial statement fraud).

ACFE and Grant Thornton: Preparing for a Post-Pandemic Fraud Landscape Survey 2021



ACFE and Grant Thornton: Preparing for a Post-Pandemic Fraud Landscape Survey 2021

How Are Anti-Fraud Budgets Changing?

- Budgetary and staffing support can be especially critical in times when organizations are experiencing or expect to experience increases in fraud.
- For fiscal year 2021, 86% of most respondents' organizations increased or maintained the overall budget for their anti-fraud programs.

ACFE and Grant Thornton: Preparing for a Post-Pandemic Fraud Landscape Survey 2021

What Factors Are Impacting Fraud Risk During and Post-Pandemic?

- More that two-thirds of respondents indicated that the following risk factors have had a significant or moderate influence on their organization's fraud risk landscape and/or fraud risk management program during the pandemic:
  - Shifts in business operations (e.g., the shift to remote work)
  - Changing consumer behavior (e.g., virtual retail/online transactions).
- They also remain the top two risk factors expected to affect respondents' organizations in the coming year, highlighting the lasting repercussions of these changes.

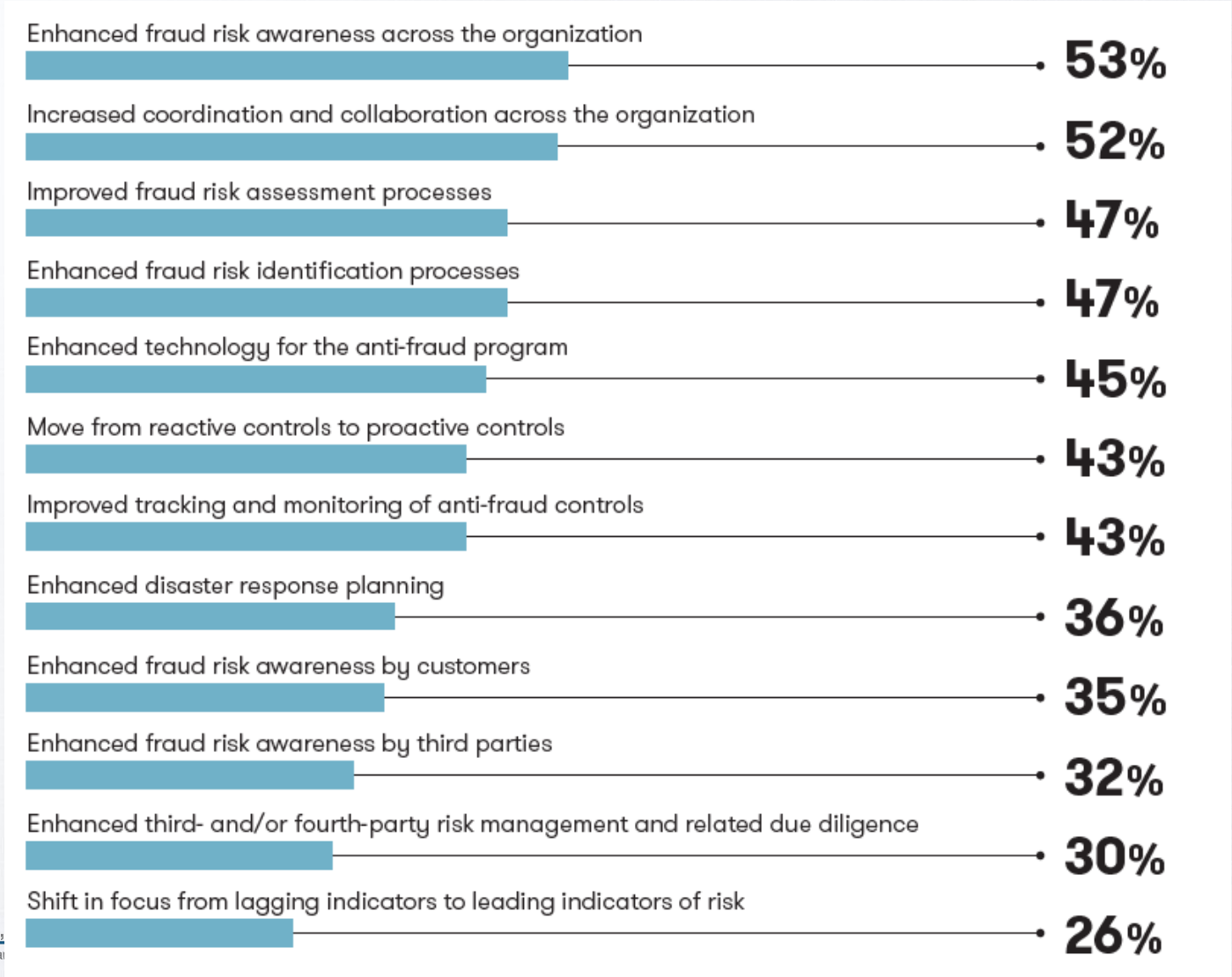
ACFE and Grant Thornton: Preparing for a Post-Pandemic Fraud Landscape Survey 2021

Lessons Learned to Move Anti-Fraud Programs Forward Post-Pandemic

- Pandemic revealed that there are strong opportunities for improvement in anti-fraud programs across organizations.
- There are common areas of many organizations' anti-fraud programs that require improvement to be more effective in the post-pandemic fraud landscape.

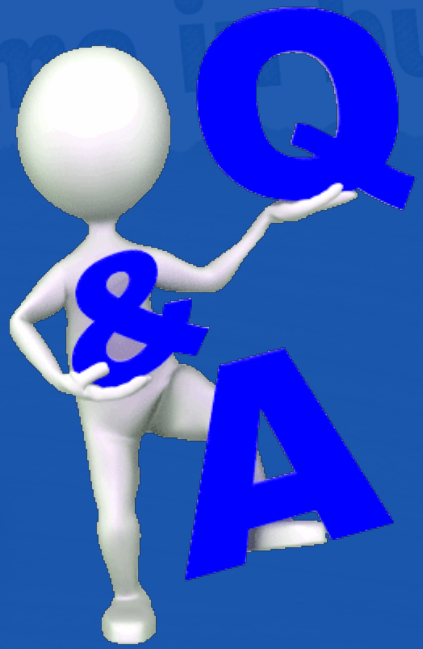
ACFE and Grant Thornton: Preparing for a Post-Pandemic Fraud Landscape Survey 2021

Changes needed to make anti-fraud programs more effective going forward.



ACFE and Grant Thornton: Preparing for a Post-Pandemic Fraud Landscape Survey 2021

Questions



Brian W. Johnson, CPA, CFE
Audit Partner
bjohnson@dmcpas.com

Kaitlyn A. Hensler, CPA/CFF, CFE
Senior Audit Manager
khensler@dmcpas.com

Copyright / Disclaimer

This presentation and any related materials are designed to provide accurate information in regard to the subject matter covered, and are provided solely as a teaching tool, with the understanding that neither the instructor, author, publisher, nor any other individual involved in its distribution is engaged in rendering legal, accounting, or other professional advice and assumes no liability in connection with its use. Because regulations, laws, and other professional guidance are constantly changing, a professional should be consulted if you require legal or other expert advice.