BUSINESS FUNDAMENTALS BOOTCAMP

Tactical Skills
for the Growing Business

Defending yourself against the Fraud Epidemic

Nick Ferrer
VP, Senior Treasury Management Officer
TD Bank

Nick.Ferrer@td.com
www.td.com

BUSINESS FUNDAMENTALS BOOTCAMP

Tactical Skills for the Growing Business

Nick Ferrer, VP Senior Treasury Management Officer

Nick Ferrer has over 15 years of treasury management experience and currently serves as Vice President of Treasury Services for TD Bank, Florida. He handles all of the Treasury Management needs for the region, which includes middle market, government and not for profit banking.

Ferrer began his banking career in Miami with Wachovia/Wells Fargo. He was recently the Treasury Officer for SunTrust Bank specializing in Commercial, Government and Not for Profit segments. Through his financial career, Nick has given seminars as a subject matter expert for multiple associations.

Association for Financial Professionals Fraud and Control Survey Statistics

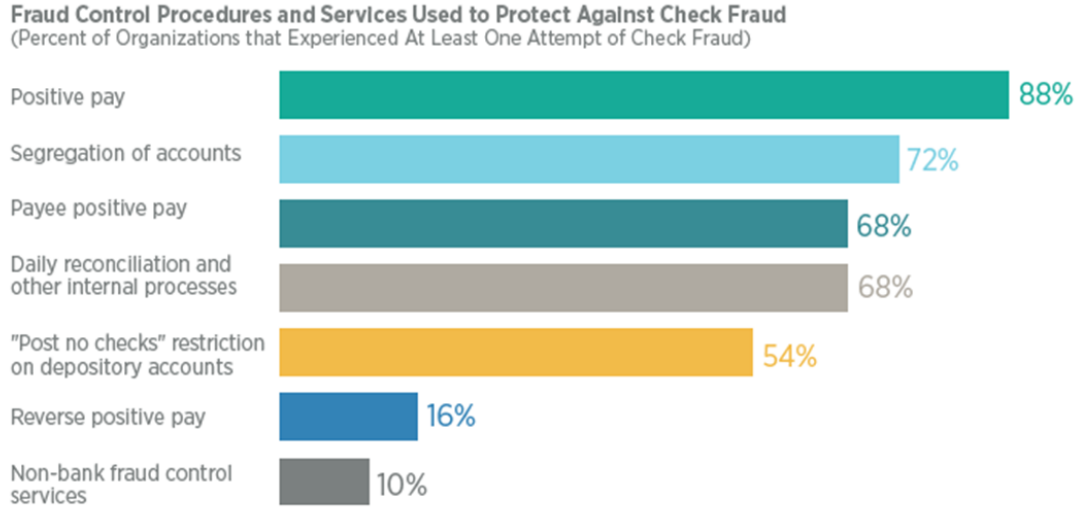
2019 AFP Payments Fraud and Control Survey Report-Comprehensive Report

Protecting from Fraud

- 82% of organizations were victims of attempted or actual fraud in 2018
  - 70% Checks
  - 45% Wires
  - 33% ACH Debits, 29% Credit cards, 20% ACH Credits
- 80% of organizations have been subject to attempted or actual Business Email Compromise (BEC)
  - Up from 64% in 2016
  - 54% of organizations reported financial losses as a result of Business Email Compromise
- 65% of payments fraud is committed by individuals outside the organization
- 67% of payments fraud is discovered by treasury staff
- 47% of organizations discovered fraud less than two weeks after the incident occurred

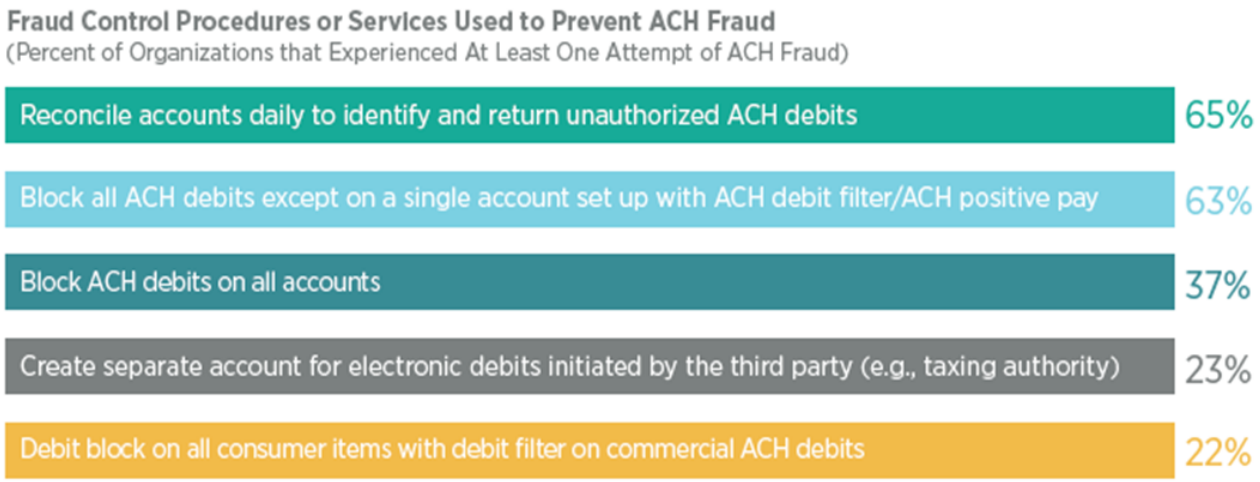
Protect Against Check Fraud

2019 AFP Payments Fraud and Control Survey Report-Comprehensive Report



Controlling ACH Fraud

2019 AFP Payments Fraud and Control Survey Report-Comprehensive Report



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 FUNDAMENTALS BOOTCAMP
Tactical Skills for the Growing Business

Business Email Compromise Mitigation Best Practices -**Wires**

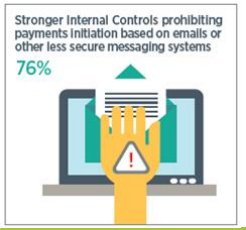
Wire transfers are Once Again Prime Target for BEC Scams

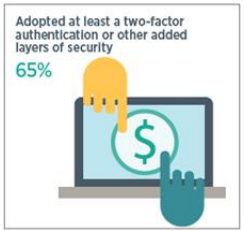
- Educate your staff about the fraud risks inherent in their daily processes. Training, training and more training!
- Create a culture that empowers employees to ask questions.
- Develop a process for wire validation that includes access to key executives for approval.
- Employ dual approval for funds 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 FUNDAMENTALS BOOTCAMP
Tactical Skills for the Growing Business

Business Email Compromise
Mitigation Best Practices –**Supplier/Invoice**

- 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!!!!!!





The Threat Landscape: **Ransomware**

BUSINESS FUNDAMENTALS BOOTCAMP
Tactical Skills for the Growing Business

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.

Mobile Ransomware Threat Grows

Handheld Electronics are the next battlefield for domination of personal information. In an increasingly mobile work environment, all businesses and their employees must be extra vigilant.

- Mobile malware, banking malware, and ransomware are the primary threats to expect in 2019. (Source: Fortinet)
- More than 18 million mobile malware instances were detected by Symantec in 2018. (source: Symantec)
- Kaspersky Labs found that the majority of the malware in 2018 was targeting phones on the Android operating system.
- Cybersecurity giant Symantec identified mobile use as a significant point of vulnerability for businesses and private users in 2018. In their annual Internet Security Threat Report (ISTR) they state “Threats in the mobile space continue to grow year-over-year, including the number of new mobile malware variants which increased by 54 %”.
- Less than 20% of mobile malware is delivered via a browser — the remainder of the payloads come through an app. (Source: RSA Current State of Cybercrime)

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.

[1] For additional information on Avoiding Social Engineering and Phishing Attacks, please see US-CERT Security Tip (ST04-014), available at: https://www.us-cert.gov/ncas/tips/ST04-014

The Threat Landscape:
Beware of Online Risks

BUSINESS FUNDAMENTALS BOOTCAMP
Tactical Skills for the Growing Business

Phishing Top Traps

Top Social Media Email Subjects

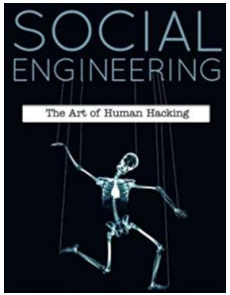
- LinkedIn: "Add me" "Join Network" "New Message"
- Login Alerts
- Tagged Photo
- Free Pizza
- New Voice Message
- Unread Message

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
- Email Account Updates

The Threat Landscape

- Phishing (Email)
- Smishing (text Message)
- Vishing (Voice/Phone)
- Twishing (Twitter)
- 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!!!!!!!!!!




AVOID FRAUD

Recommendations

10 Risk Mitigates Every Business Should Perform

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

ANY FINAL QUESTIONS ?

Nick Ferrer

VP, Senior Treasury Management Officer

TD Bank

Nick.Ferrer@td.com

www.td.com

Remember to Complete the Speaker Survey

Supportingstrategies.com/bootcamp

‘click’ event name

scroll to agenda

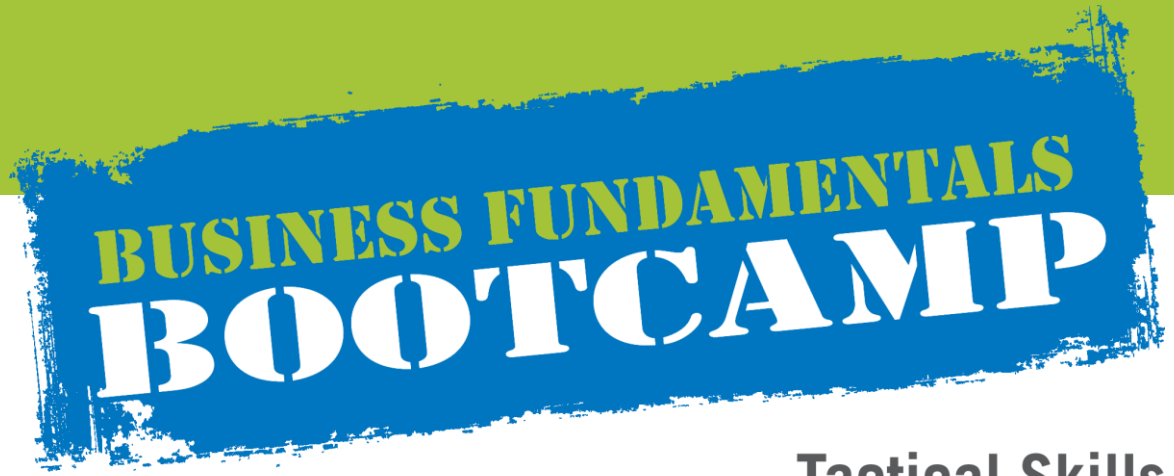
select your speaker

BUSINESS FUNDAMENTALS BOOTCAMP

Tactical Skills for the Growing Business

Thank You!


BUSINESS FUNDAMENTALS
BOOTCAMP
Tactical Skills
for the Growing Business



Tactical Skills for the Growing Business