

Fraud Overview and Mitigation Strategies



SUNTRUST TEAM:

DOUG HICKMAN
SENIOR VICE PRESIDENT
FOUNDATIONS AND ENDOWMENTS SPECIALTY PRACTICE

JAMES BERNAL
ASSISTANT VICE PRESIDENT
FOUNDATIONS AND ENDOWMENTS SPECIALTY PRACTICE

CHARLENE CRAIG
SENIOR VICE PRESIDENT
NOT-FOR-PROFIT & GOVERNMENT BANKING



Paper vs. Electronic



Protecting from Fraud

Moving from Paper to Electronic

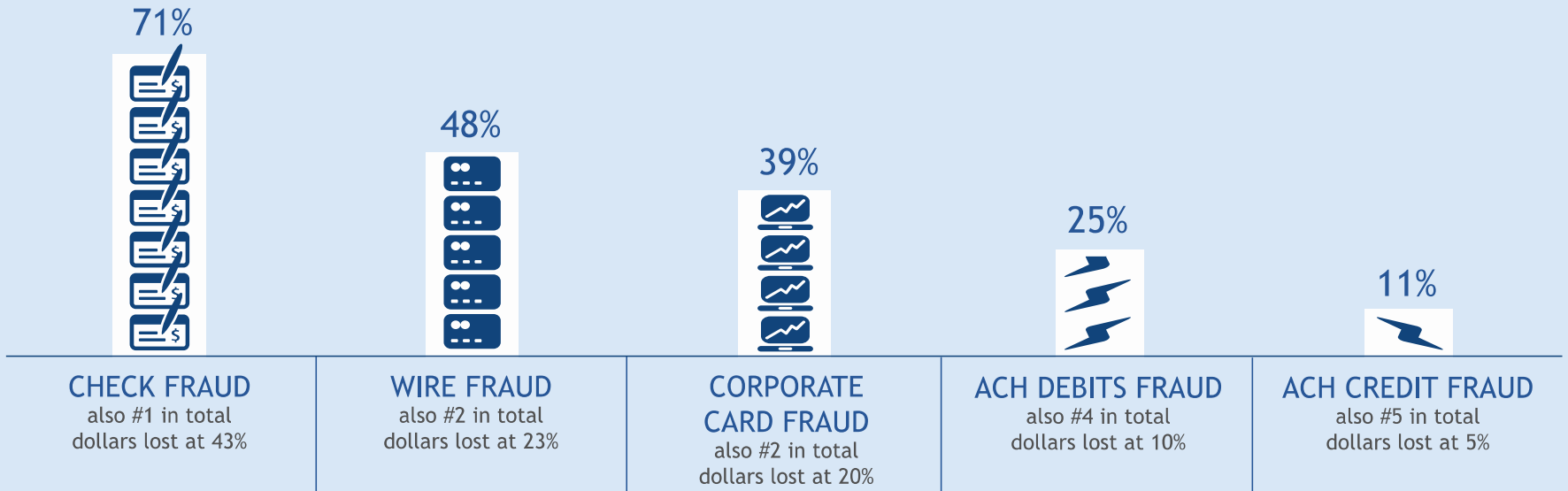
73% of businesses experience fraud, with paper-driven processes and checks as the number one source



AFP PAYMENTS FRAUD AND CONTROL SURVEY

Sources of Fraud by Payment Method

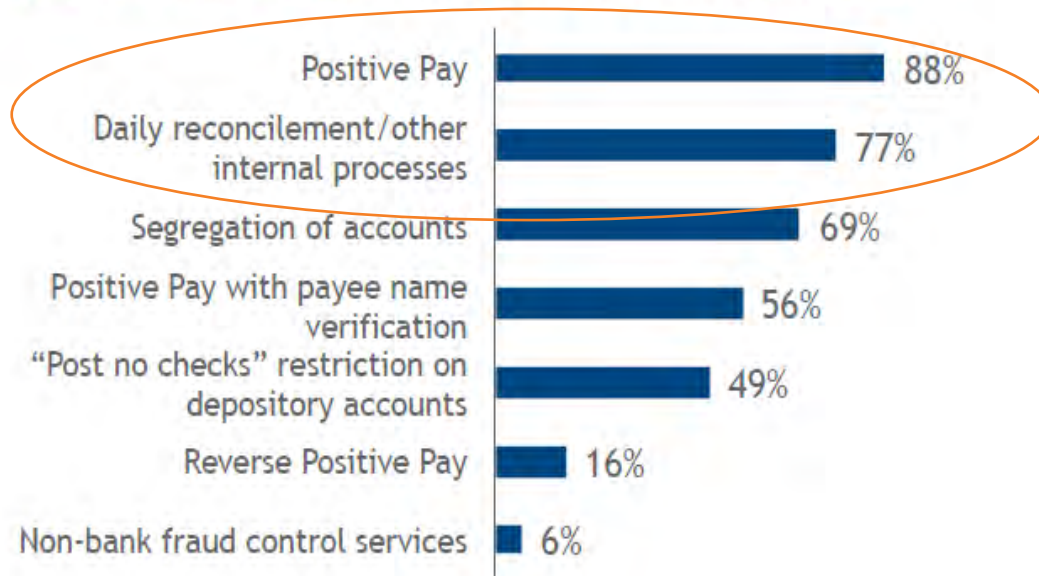
(% of organizations that experienced attempted or actual payments fraud)



Source: AFP Payments Fraud and Control Survey, 2016

Check Fraud Prevention Measures

(% of organizations that experienced at least one attempted check fraud)

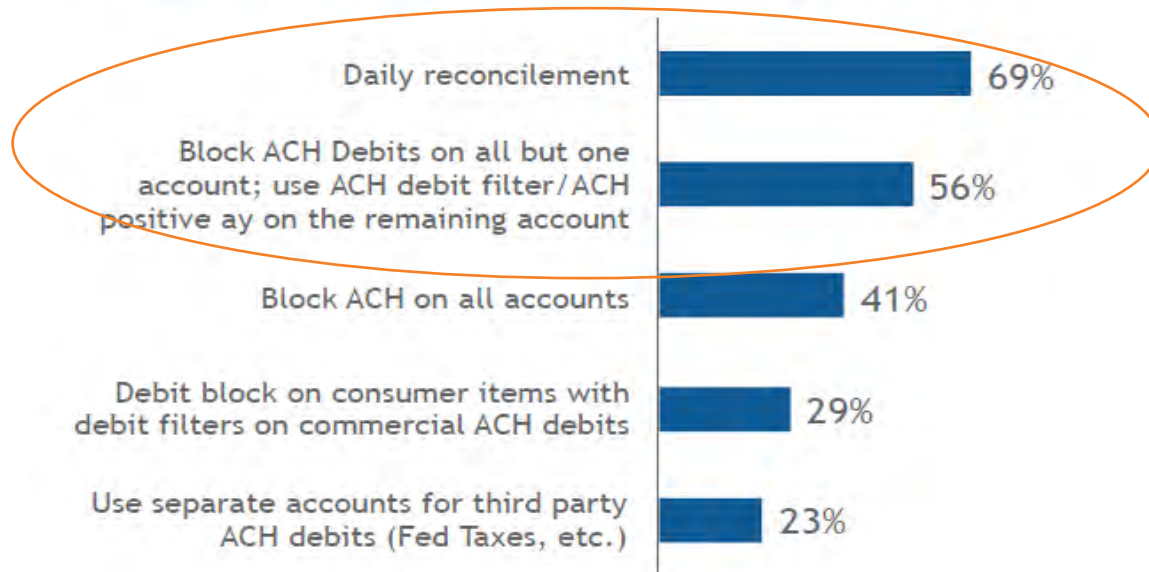


Source: AFP Payments Fraud and Control Survey, 2016

FRAUD PREVENTION BEST PRACTICES - ACH

ACH Fraud Prevention Measures

(% of organizations that experienced at least one attempted check fraud)



Source: AFP Payments Fraud and Control Survey, 2016

WHO'S BEING TARGETED

Risk assess to effectively position your defense to these threat actor groups. Get informed.

Some examples:

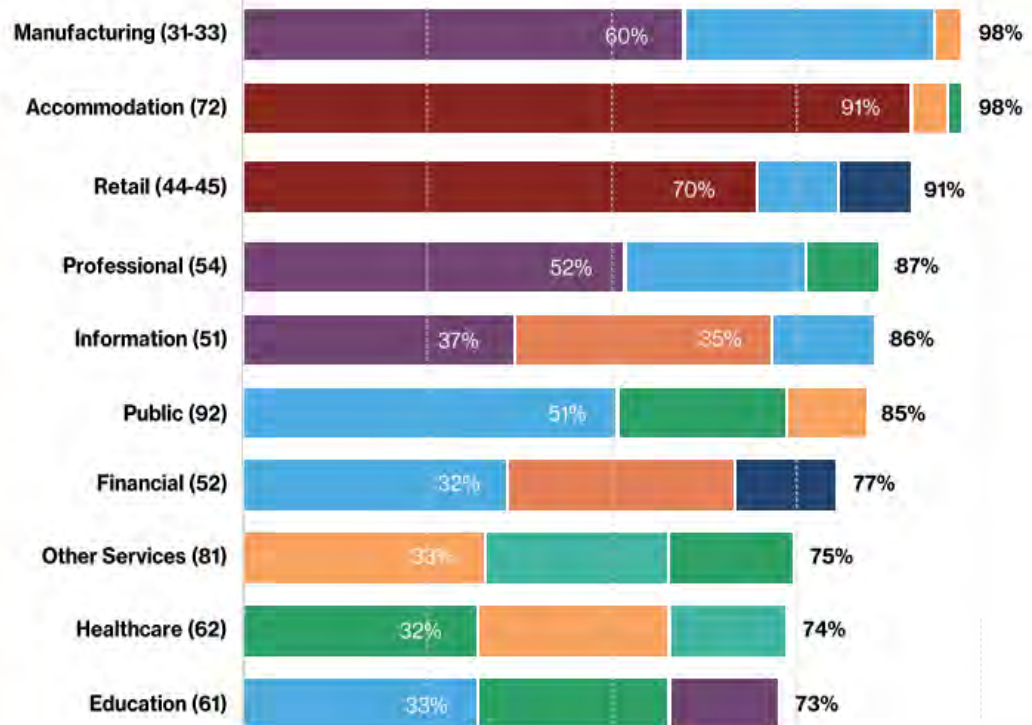
- Money
- Intellectual Property
- Customer Data
- Classified Data

VERIS incident pattern view.

2014 top targets, filtered by breaches.

- Point-of-sale intrusions
- Web application attacks
- Insider and privilege misuse
- Physical theft and loss
- Miscellaneous errors
- Crimeware
- Payment card skimmers
- Denial of service attacks
- Cyber-espionage

Incident patterns, by Industry (2015)




Other Services = Entertainment, Technology, Transportation

Source: 2015 Verizon Data Breach Investigations Report Data


THE THREAT LANDSCAPE - BUSINESS EMAIL COMPROMISE



BUSINESS EMAIL COMPROMISE




After checks, **wire transfers** were the second most popular vehicle for **payments fraud**, with 48% of organizations exposed.



A majority of organizations were exposed to **Business Email Compromise (BEC) scams** in 2015.

9 out of 10 finance professionals strongly believe **EMV cards** will successfully alleviate point-of-sale fraud.



EMV Card

BUSINESS EMAIL COMPROMISE

- Business Executive Fraud - Email accounts of high-level business executives (CFO, CTO, etc.) are spoofed/hacked and a fraudulent wire transfer request is made
- Bogus Supplier Invoices - After a vendor has been hacked, a company is asked to change payment instructions or pay an invoice to an alternative, fraudulent account.
- Attorney Impersonation- Scammers convince targets that wire transfers are needed for legal matter settlement, indicating the need for confidentiality and urgency.
- Data Theft - The goal isn't direct funds transfer. Scammers are looking for sensitive corporate financial information.





BUSINESS EMAIL COMPROMISE

Best Practices - Wire Transfer

- Educate your staff about the fraud risks inherent in their daily processes.
- Create a culture that empowers employees to ask questions
- Develop processes for wire validation that include access to key executives for approval.
- Require two people to approve large sums or to make changes to any information that impacts the movement of funds.
- Verify important or large transactions through an alternate method including phone call or in-person.
- Limit information available to the general public about your company's internal operations.
- Conduct all banking on a dedicated machine used for no other task.



BUSINESS EMAIL COMPROMISE

Best Practices – Supplier/Invoice

- Train associates on all vendor management policies and empower them to ask questions when in doubt.
- Know Your Vendor - perform due diligence on the company's background and existence
- Dual approvals for new vendors
- Email requests for new vendor set-up not accepted
- Plan How Your Vendor Will Connect to You
- EDI, secure FTP, Web portal, Phone
- Test, document, and validate
- Segregate Responsibility of Vendor Authentication and Purchasing Functions
- Changes to Vendor Master File : Requests must be validated by trusted source at vendor
- Verbal Confirmation - Vendors should be required to verbally approve changes using phone numbers that are known and listed for vendors
- Vendor list, including contact information of individuals authorized to make payment changes, should be kept in a hard copy file
- New Vendor system flags (systemic red flags of change of normalcy)

Fraud Prevention:

- Prevent compromised email accounts
 - Password discipline, consider two-factor authentication
- Be alert to fake email addresses and websites
 - “0” vs “o”, “1” vs “l”
- Even the telephone may not be trusted!
 - Verify caller’s identity (fraudsters can “spoof” telephone numbers)
- Dual control / approvals on payroll, payment, and wire systems
 - Separate user ID for initiation and approval

THE THREAT LANDSCAPE - BEWARE OF ONLINE RISKS



THREAT LANDSCAPE...

- Phishing (Email)
- Smishing (Text Message)
- Vishing (Voice/Phone)
- Twishing (Twitter)
- Search Engine Poisoning
- Trusted Site Compromise
- Malvertising
- Software Vulnerabilities
- Scareware
- Fake Mobile Apps



Avoid Getting Hooked By a Phish...



CYBERSECURITY PROGRAM

- Have an Information Security policy
- Strong password requirements
 - Length, complexity, and lock outs
- Keep up-to-date on security patches
 - Operating systems
 - Software
 - Don't forget about your browsers!





CYBERSECURITY PROGRAM

- Malware / antivirus protection
- Firewalls and other security tools
 - Keep your data on your network or under your control
 - Access restrictions and use of company assets
 - Remote access
 - Third-party hosted sites/apps



SECURITY AWARENESS

- General user awareness
 - How to spot a phishing email
 - Fake “help desk” scam
 - Good password security
- Don't forget about your IT staff





FOCAL POINTS

Top 5 Security Program Focal Points

1. Have Information Security Policy

Executive level approval, updated regularly

2. Have relevant and up-to-date technical security standards

3. Vulnerability & patch management

“99% of the exploited vulnerabilities were compromised more than a year after the CVE was published” (Verizon DBIR)

4. Have an effective security awareness program

User, technical staff, clients

5. Identify and assess your risks

Technology, business processes, third-parties

Effective, risk-based assessment process

PASSWORD SECURITY

Don't

- use the “remember password”
- re-use the same password across multiple sites
- write down or share your password

Do

- use a different password for each account and change them often.
- use a combination of upper/lower case, numbers, and special characters
- use long (12 characters or greater), random multi-word passwords
- leverage multi-factor authentication

- *Substitute numbers for letters and vice versa*
- *Use multiple random words*
- *Use capitalization in random places, intentionally misspell words, or spell them backwards*
- *Use words then remove letters and add relevant numbers: First Car – 1992 Ford Mustang = FdMstg92*
- *Use phrases substituting letters with numbers: The party is at 7 o'clock = prtyszat7*
- *Experiment with your favorite song, album, or movie titles by adding numbers: Michael Jackson's Thriller = MJAXtHri13r*

Top 25 Most Common Passwords of 2016

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321
11.	qwertyuiop
12.	myn00b
13.	123321
14.	666666
15.	1@tcskd2w
16.	777777
17.	1q2w3e4r
18.	654321
19.	555555
20.	3rjs1la7qe
21.	google
22.	1q2w3e4r5t
23.	123qwe
24.	zxcvbnm
25.	1q2w3e

Better Safe Than Sorry...

- Only download or buy apps from legitimate app stores.
- Know the reputation of apps and particularly the app publisher.
- Understand requests the app are asking to do with your device.
- Only enter credit card info on secure shopping portals.
- Be alert for poisoned search results when using search engines to find products.
- Don't use free public Wi-Fi to make purchases or do online banking.
- Be suspicious of great deals and don't click the links.
- Make sure the connection to e-commerce sites is secured (HTTPS).

SOURCE: Network World 11/22/16

QUESTIONS / COMMENTS?

