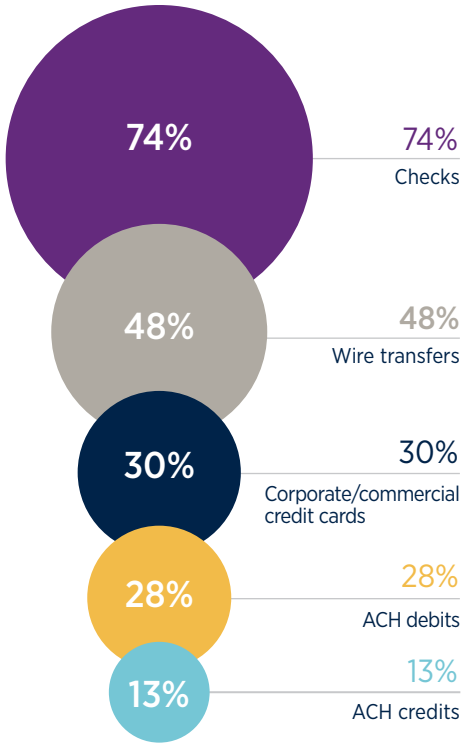
ASSOCIATION FOR FINANCIAL PROFESSIONALS

AFP MINI-COURSE
PAYMENTS FRAUD
Tip Sheet

Payment Methods Subject to Fraud



Source: 2018 AFP Payments Fraud & Control Survey

Payments fraud is big business. In a recent study, the Federal Reserve Bank has estimated that annual third party payments fraud losses in the U.S. are in excess of $6 billion. But that's only the tip of the iceberg. Global card fraud losses are estimated to exceed $16 billion a year and that number is growing quickly. Throw in other types of fraud, such as account takeover and internal payments fraud, and the number should be big enough to get anyone's attention.

1. BEST PRACTICES TO COMBAT CHECK FRAUD

- Payee Positive Pay
- Set default for exceptions to "do not pay"
- Reconcilement – daily is almost essential
- Use secure check stock
- Secure your check stock
- Use secure number fonts
- Eliminate manual checks
- Use check blocks
- Move paper payments to EFT
- Participate in anti-fraud groups

2. BEST PRACTICES TO COMBAT ACH FRAUD

As payments move to electronic rails, fraud migrates with it. The volume may be smaller but losses can be large. ACH fraud can be hard to recover from since payments are real or near real time. Proper vendor management is essential.

- Dual control
- Same day reporting and alerts
- Daily reconcilement
- Use special purpose accounts for EFT payments
- Debit blocks and filters (ACH Positive Pay)
- Use templates for wires
- Verify all payment requests
- Run all transactions through A/P
- Use Universal Payment Identification Code (UPIC technology)

4520 East-West Highway | Suite 800 | Bethesda, MD 20814 | USA | T: +1 301.907.2862 | F: +1 301.907.2864 | www.AFPonline.org

AFP MINI-COURSE

PAYMENTS FRAUD

Tip Sheet

3. BEST PRACTICES TO COMBAT CARD FRAUD

Card fraud is a growing part of payment fraud, partly due to the growing use of the corporate card. If you have not done so already, document policies and procedures regarding use of the corporate card. Retail card fraud and online card fraud are an even bigger problem for anyone who accepts card payment.

- Always verify signature on card transactions
- Use address verification services (AVS)
- Use CVC2 and CVV2
- Be wary of international orders
- Send confirmations separately from transactions
- Require signed proof of delivery for shipments not to billing address
- Tokenization
- Balance and reconcile your terminals every night
- Lock terminals when not in use
- Process refunds only to the original card number

4. HOW TO SPOT INTERNAL FRAUD

Look for these signs:

- Accounting exceptions/anomalies
- Internal control weaknesses
- Analytical symptoms
- Behavior changes
- Lifestyle changes
- Tips and complaints

The internal Fraud Triangle

These 3 elements need to be present for Internal Fraud:

5. CYBERCRIME

Fraudsters are after cash assets and much much more. Types of cybercrime are:

Malware

Malware is any software that tries to infect a digital device. Most commonly, it is done with the intent to inflict damage on the organization or system.

Ransomware

Malware that takes over your computer or system and demand a type of payment to restore control.

Phishing

The creation and use of e-mails and websites designed to look like e-mails and websites of well-known legitimate businesses to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords.

Pharming

Pharming uses DNS server and IP addresses to create look-alike websites that you may not know you are accessing.

Smishing and Vishing

Similar to phishing but via text or voice mail.

6. CREATE A CYBER RISK MANAGEMENT PLAN

Incident Response Plan Types of cybercrime are:

- Specify the response team
- Notification channels - define
- Escalation Procedures
- Identify regulatory requirements
- Don't forget PR
- Test at least annually

4520 East-West Highway | Suite 800 | Bethesda, MD 20814 | USA | T: +1 301.907.2862 | F: +1 301.907.2864 | www.AFPonline.org