paymerang SM

Crush Payment Fraud Risk in 2019

PAYMENT AND CARD EXPERTS

ERIC WALDENMAIER

Vice President at Paymerang

As Vice President at Paymerang, Eric maintains partnerships with various state and national associations to reach audiences through webinars, conferences and referrals. For over 5 years, he has helped clients streamline vendor disbursements, eliminate fraud and earn millions of dollars through their AP departments.

LEIGH MOORE

Sr. Director, B2B Partnerships & Innovation at Visa

Leigh Moore is responsible for the establishment and sustainability of B2B partnerships and new initiatives that accelerate the growth of Visa Business Solutions. In this role, she focuses on developing an ecosystem of key strategic partnerships in the accounts payable segment to extend Visa's reach through collaboration and thought leadership, leveraging talent, relationships and resources across the global Visa enterprise.

JEFF GAINER

Director of Information Security & Risk Management at Paymerang

Jeff leads Paymerang's information security and risk management programs to ensure a trusted payment experience for our clients and their vendors. Jeff has over 20 years of experience in the financial services sector with GE Capital, Genworth Financial and Impact Makers. He's spent the last 10 years focused on managing operational risks in the areas of data security, business continuity, outsourcing and fraud.

ANGELA TISE

Moderator

As a leader in the marketing efforts of The CFO Leadership Council's northeast region, Angela is an experienced manager who strives to improve and insure overall membership quality. In addition, on a national level, she supports our financial executives with our uniquely designed members-only Problem Solving Forums and Ask The Expert calls.

AGENDA

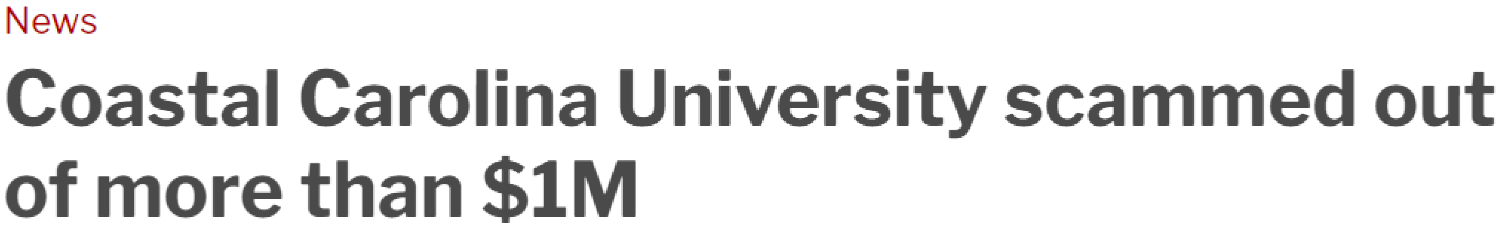
1

The key threats of payment fraud

Four layers of protection available

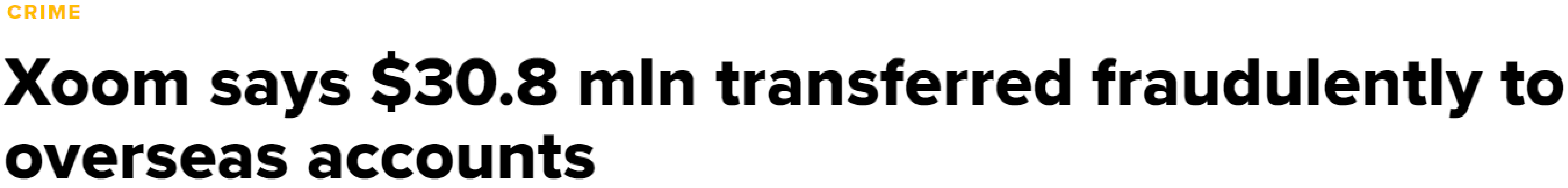
Practical steps you can take

FRAUD IS GROWING


News

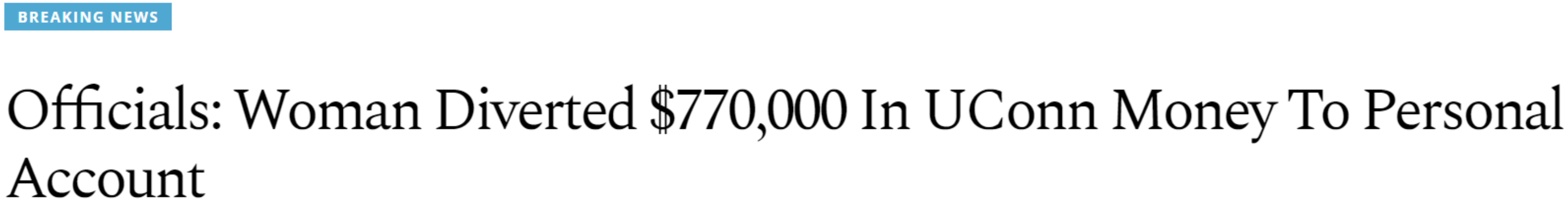
Coastal Carolina University scammed out of more than $1M

Source: Association of College and University Auditors


CRIME

Xoom says $30.8 mln transferred fraudulently to overseas accounts

Source: Consumer News and Business Channel

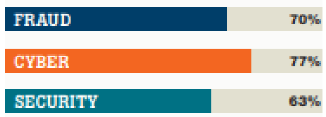

BREAKING NEWS

Officials: Woman Diverted $770,000 In UConn Money To Personal Account

Source: Hartford Courant

…ACROSS ALL INDUSTRIES

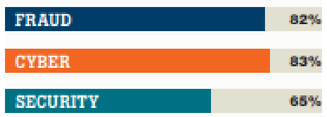
CONSTRUCTION, ENGINEERING AND INFRASTRUCTURE



High staff turnover is the top driver of increased fraud risk (named by 40% of respondents)

86%
Believe exposure to fraud has increased

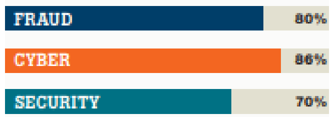
CONSUMER GOODS



Entry to new, riskier markets is the top driver of increased fraud risk (named by 40% of respondents)

92%
Believe exposure to fraud has increased

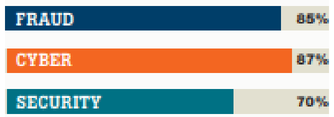
NATURAL RESOURCES



High staff turnover is the top driver of increased fraud risk (named by 40% of respondents)

92%
Believe exposure to fraud has increased

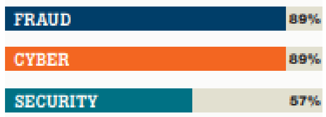
TRANSPORATION, LEISURE AND TOURISM



High staff turnover is the top driver of increased fraud risk (named by 43% of respondents)

96%
Believe exposure to fraud has increased

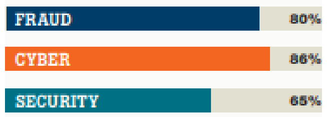
FINANCIAL SERVICES



Entry to new, riskier markets is the top driver of increased fraud risk (named by 34% of respondents)

91%
Believe exposure to fraud has increased

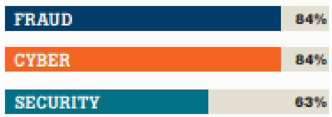
HEALTHCARE, PHARMACEUTICALS AND BIOTECHNOLOGY



High staff turnover is the top driver of increased fraud risk (named by 41% of respondents)

88%
Believe exposure to fraud has increased

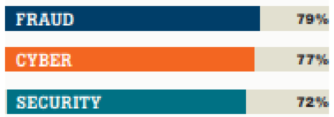
PROFESSIONAL SERVICES



High staff turnover is the top driver of increased fraud risk (named by 47% of respondents)

96%
Believe exposure to fraud has increased

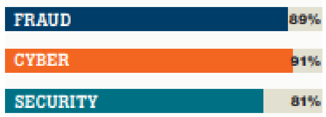
TECHNOLOGY, MEDIA AND TELECOMS



Complexity of IT infrastructure is the top driver of increased fraud risk (named by 39% of respondents)

86%
Believe exposure to fraud has increased

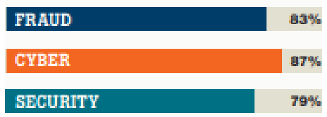
MANUFACTURING



Entry to new, riskier markets is the top driver of increased fraud risk (named by 51% of respondents)

96%
Believe exposure to fraud has increased

RETAIL, WHOLESALE AND DISTRIBUTION



Increasing exposure to public digital touch-points is the top driver of increased fraud risk (named by 33% of respondents)

87%
Believe exposure to fraud has increased

Percentage of participants from each industry whose companies experienced fraud, cyber or security incidents in the last 12 months.

Source: A commissioned study conducted by Forester Consulting on behalf of Kroll, August 2016

POLLING QUESTION 1

How are you paying vendors today?

A) All Checks

B) Check and some ACH

C) Check, ACH and Card

POLLING QUESTION 2

If you are processing E Payments (ACH or Card), How are you doing it?

A) All in house

B) Bank or Card provider disburses some payments

C) Third party does it all for me

THE FACTS ABOUT CHECKS

> “On that check is my name, address, phone number, my bank’s name and address, my bank account number, routing number, and my signature.”

Frank Abagnale (Catch Me If You Can)

CHECK FACTS & BENEFITS

- #1 risk of fraud. 75% of businesses in 2017
- Your bank cannot stop a fraud from happening
- Checks are the most time consuming and expensive way to pay vendors
- Most payment problems are check related
- Simple (always done it this way)

KEY THREATS:

- Duplicate a check
- Electronically process it for a different amount
- Pay fraudulently (internal)
- Bank account data right on the document

PRACTICAL SOLUTIONS

- Positive Pay with your bank
- Stop paying vendors by check, use electronic payments
- Engage a third party to process payments

IS ACH THE SOLUTION?

ACH FACTS & BENEFITS

- More secure than checks
- Payments process like clockwork
- Cost effective
- Control delivery

DOWNSIDE & RISK

- Months to set up
- Acquire, manage and secure vendor banking data
- Remittance information to vendor
- Intricate scams
- Phishing and hacking

PRACTICAL SOLUTIONS

- Process ACH over check whenever you can
- Read, understand, implement and train NACHA compliance
- Encrypt vendor banking data
- Engage a third party to process payments

IS CARD THE ANSWER?

CARD BENEFITS

- Liability is limited for unauthorized payments
- Set controls around use of the card account
  - Establish authorization limits
  - Block Merchant Category Codes (MCCs)
- Opt for single-use virtual card accounts vs. physical plastic
- Commercial rails can assist with payment traceability and reconciliation

KEY CONSIDERATIONS

- Management of credit lines at company or account level
- Tying payment and vendor management strategies
- Determine card issuance strategy to mitigate misuse
- Balancing prevention and employee experience

PRACTICAL SOLUTIONS

- Use card whenever possible, which often includes rebates
- Incorporate single use virtual cards accounts in addition to traditional plastic
- Determine the best payment strategies to optimize working capital and mitigate risk

AGENDA

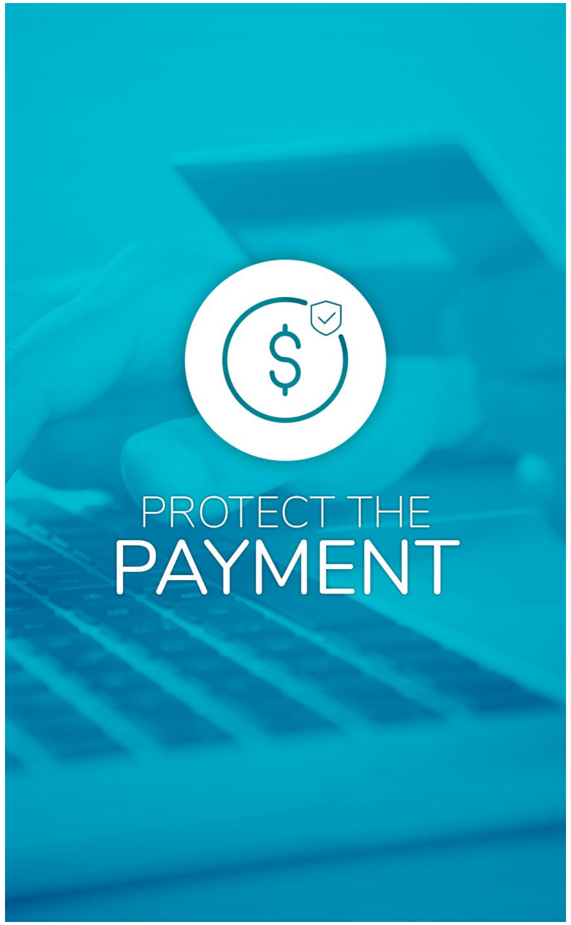
The key threats of payment fraud

2

Four layers of protection available

Practical steps you can take

FOUR LAYERS OF PROTECTION AVAILABLE



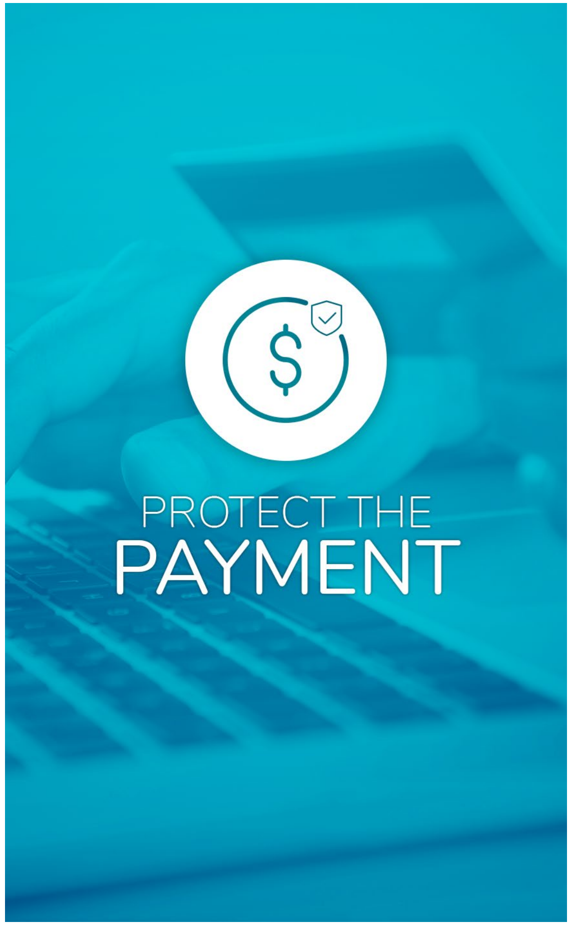
PROTECT THE
PAYMENT

SECURE THE
OPERATIONS

FORTIFY THE
NETWORK

LOCK DOWN
COMPLIANCE

PROTECT THE PAYMENT



POSITIVE PAY

WHY: To ensure only the authorized party on a check is allowed to cash that check and reduce the likelihood of payment to a fraudulent entity.

HOW: Enroll in the Positive Pay service at the financial institution where check payments are sourced.

VIRTUAL CARDS

WHY: To limit the exposure of open, higher limit credit lines that are in use for payments.

HOW: Transact using VISA virtual debit cards (vCards) to limit payments to a one-time use, preloaded payment amount.

ACH PAYMENT

WHY: Use of electronic payments that can be trusted through an established network, where the likelihood of fraud is reduced.

HOW: Register to use ACH payments with the bank account where payments are sourced and take additional steps to protect the payment information (i.e. encrypt sensitive data).

PROCEDURES

WHY: Procedures need to be in place to validate payment relationship information before action is taken to modify accounts or payments.

HOW: Before engaging with vendors or making any changes to information, the identity of the other party must be verified. Limit the information your employees can see and do not allow them to change sensitive data without approvals.

SECURE THE OPERATIONS

SECURE ENVIRONMENT

WHY: All payment data needs be protected in the operating environment where processed.

HOW: Use a combination of a clean desk policy, removal of all payment information from open office view, and a certified shredding service.

TRAINING

WHY: The payment team members are an important line of defense for ensuring a secure operation.

HOW: Conduct security awareness training by qualified staff on a regular basis to ensure team is aware of threats and how to detect suspicious links or fraudulent email addresses. Provide ongoing payment threat awareness information so the team knows what is considered suspicious and are ready to respond to it.

FRAUD DETECTION

WHY: To detect fraudulent payments and ensure that only legitimate payments are made.

HOW: Verify any anomalous changes made to vendor account information before processing payments. Assign fraud scores based on recent account changes.

PROCEDURES

WHY: To ensure operational controls are present throughout the payment process.

HOW: Set up all payment processes with multiple approvals, single payment limits and segregation of duties. Implement job rotation and cross-training for payment team members. Appropriate access controls.

FORTIFY THE NETWORK

END POINT PROTECTION

WHY: To ensure that only safe and trusted software run on computers that process payments.

HOW: Provide protection with the use of anti-virus software coupled with best in class application whitelisting technology to protect against forms of malware.

EMAIL DEFENSES

WHY: To reduce the amount of unsafe email into the payment process and protect sensitive information sent in payment email.

HOW: Deploy layers of spam/phishing defenses, including spear phishing detection, along with email encryption and rights management to protect sensitive email content.

VULNERABILITY MANAGEMENT

WHY: To identify exploitable software and security weaknesses in the payment system in order to reduce exposure to possible system compromise.

HOW: Enable a vulnerability management program with regular security posture scanning, software patching, and expert penetration testing.

THREAT PROTECTION

WHY: To determine when suspicious actions are being attempted or carried out against the payment system.

HOW: Enact intrusion and anomalous behavior detection capabilities with multi-factor authentication and full logging in the appropriate layers of the payment system.

LOCK DOWN COMPLIANCE

NACHA

WHY: To ensure automated payments are processed in a trusted and controlled environment.

HOW: Process payments using the ACH Network which maintains the highest level of safety and security for its participants through governance oversight by NACHA.

SOC-2

WHY: To verify the operating effectiveness of a service provider's Availability, Integrity and Confidentiality (AIC) security controls, by an audit expert, for companies wanting to use the service.

HOW: If you are a service provider, then contract an audit service to conduct a SOC-2 assessment, in accordance with AICPA Trust Service Criteria.
If you are a consumer of a supplied service, then request the SOC-2 Report from the supplier and confirm any gaps in expected controls.

PCI

WHY: If payment cards are processed or stored there is a security standard mandated by the Payment Card Industry (PCI) that must be attested.

HOW: Implement the PCI Data Security Standard (PCI-DSS) to ensure that cardholder data is maintained in a secure environment accordingly.

OFAC LIST

WHY: To reduce the likelihood of payments being sent to individuals or organizations determined to be threats to US national interests.

HOW: Compare the US Treasury Office of Foreign Assets Control (OFAC) Sanctions List against pending payments and stored supplier data to identify possible threats.

AGENDA

The key threats of payment fraud

Four layers of protection available

3

Practical steps you can take

PRACTICAL STEPS

As long as there is money and valuable data, there will be fraud attempts and threats to security.

PAYMENT

- Positive pay
- E Pay
- Use one-time use, preloaded virtual cards
- Encrypt account information
- Verify vendors before making changes
- Limit employee access
- Require approval for changes

OPERATIONS

- Clean desk and secure documents
- Utilize certified shredding service
- Verify anomalous changes
- Assign fraud scores
- Suspicious links and fraudulent email detection training
- Multiple approvals
- Single payment limits
- Segregation of duties
- Job rotation and cross training
- Defined access controls

NETWORK

- Antivirus Software and whitelisting technology
- Vulnerability management program
- Security posture scanning
- Software patching
- Expert penetration testing
- Spam and phishing defenses
- Email encryption
- Multi-factor authentication

COMPLIANCE

- NACHA - read it, learn it, train it
- Do not store banking data if you can avoid it
- PCI- Secure cardholder data
- SOC 2- Security controls for integrity and confidentiality
- OFAC- Know your vendor and where your money is going

GET HELP TODAY

paymerang℠

Since 2010. Paymerang has helped hundreds of companies, secure and shield their payments and bank accounts from fraud and has relieved the burden of vendor payments, reconciliation, data retrieval, management, storage and compliance.

- IN 30 DAYS A COMPLIANT AND COMPREHENSIVE PAYMENT SOLUTION CAN BE IMPLEMENTED
- NO CAPITAL EXPENDITURE AND, ON AVERAGE, LESS THAN 10 STAFF HOURS INVESTED
- ASK FOR A FREE PAYABLE ANALYSIS A FINANCIAL BENEFIT REVIEW
- EFFICIENCY, SECURITY AND PROFITABILITY

CONTACT US

Questions / Comments

Please send any questions, comments or feedback to:

Eric Waldenmaier
Vice President

(804) 334-5775
ewaldenmaier@paymerang.com