

The Invisible Enemy: Fighting Fraud in AP Automation





presenters



SIERRE LINDGREN

Senior Fraud Analyst

Sierre Lindgren is a Senior Fraud Analyst at Paymerang. In addition to overseeing Paymerang's fraud team, Sierre helps create new fraud mitigation tools, policies and procedures, and analyzes recent fraud trends and schemes. She also spends time educating business offices nationwide on how to protect themselves from fraud during thought leadership. Before Paymerang, she spent 11 years in the banking industry, with the last five of those years focusing on fraud and investigating ACH, wire, and debit card fraud disputes from customers. Lindgren holds degrees in Psychology and Criminal Justice from Virginia Commonwealth University. When she's not fighting fraud, she enjoys spending time with her two children and rescue dogs on the Rappahannock River.



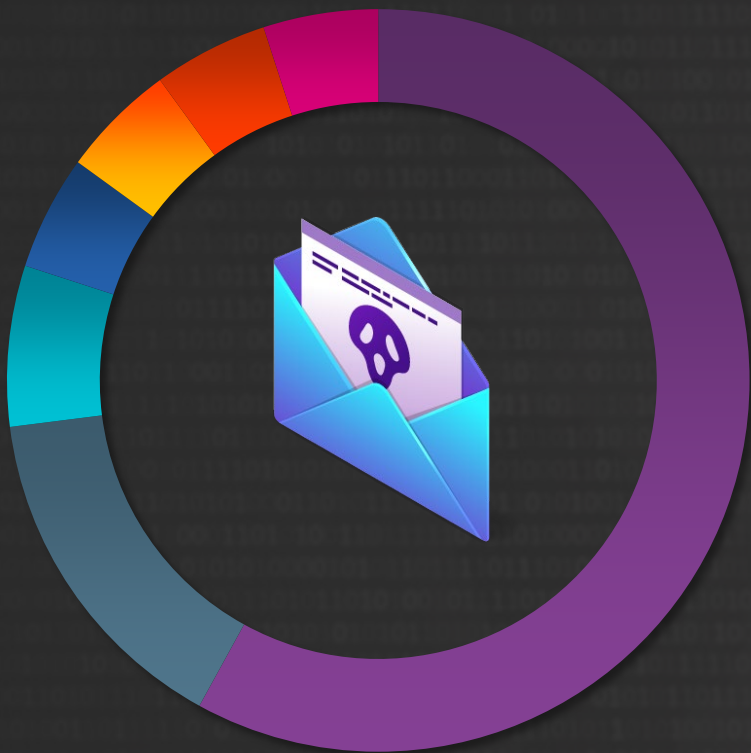
TIFFANY ALLEN

Channel Program Director

As a Channel Program Director at KwikTag by Paymerang, Tiffany is focused on the management and execution of partner programs with KwikTag. With more than 15 years in the Microsoft Dynamics scope, Tiffany channels her extensive marketing experience to generate new partnerships for KwikTag. Tiffany enjoys spending time with family at the pool or beach, soaking up the sun! Tiffany is a University of North Texas alum, Go Eagles!



a matter of when, not if



Departments Most Vulnerable to Being Targeted by BEC Fraud

(Percentage Distribution of Organizations)

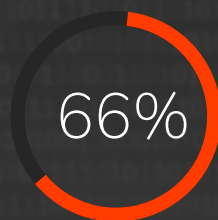
- 58% - Accounts Payable
- 15% - Treasury
- 7% - CEO, COO, CFO or other C-Suite Executive
- 5% - Procurement/Sourcing
- 5% - Human Resources/Payroll Dept.
- 5% Accounts Receivable
- 5% - Other

Source: 2021 AFP Payments Fraud and Control Survey Report

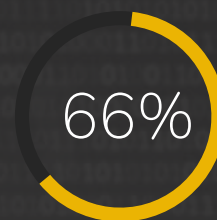
➤ | payment methods impacted by fraud

Payment Methods Subject to Attempted or Actual Fraud (Percent of Organizations)

● 2021 ● 2020

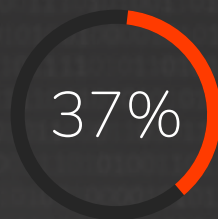


66%

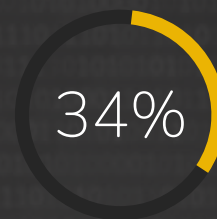


66%

Checks



37%

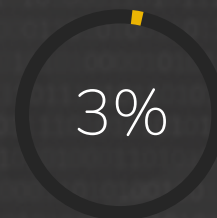


34%

ACH Debits



3%



3%

ACH Credits

Source: 2022 AFP Payments Fraud and Control Survey Report



virtual cards are a safe option

66%

**IN 2021, 66% OF COMPANIES
PAYING BY CHECK EXPERIENCED REAL OR
ATTEMPTED FRAUD, COMPARED TO ONLY**

3%

**3% WHEN PAYING WITH
SINGLE-USE VIRTUAL CARDS**





payments fraud

71%

OF ORGANIZATIONS

**WERE VICTIMS OF PAYMENTS FRAUD
ATTACKS AND ATTEMPTS IN 2021**

(The Association for Financial Professionals Payments Fraud and Control Survey)





three types of fraud



BUSINESS EMAIL
COMPROMISE



VENDOR IMPERSONATION



PHISHING

What is Business Email Compromise?

Scam artists use emails to dupe accounting departments into transferring funds to illegitimate accounts.

Fraudsters spoof URLs and send emails pretending to be vendors or company senior management requesting either a change in bank account information or a transfer of funds to a fraudulent account.





BEC statistics

62% OF PRACTITIONERS
INDICATE BEC THE PRIMARY
SOURCE OF **FRAUD ATTACKS**
AT THEIR ORGANIZATION

2021 AFP Payments Fraud And Control Report



34% OF ORGANIZATIONS
REPORT **FRAUDSTERS**
ACCESSED ACH CREDITS
USING BEC IN 2020

34% OF COMPANIES
EXPERIENCED A FINANCIAL
LOSS AS A RESULT OF THESE
EMAIL SCAMS OR THE FBI
REPORTED THAT BEC SCHEMES
RESULTED IN APPROXIMATELY
\$1.8 BILLION LOSSES

76% OF ORGANIZATIONS
WERE **TARGETED** BY BEC IN
2020-2021 AFP PAYMENTS
FRAUD AND CONTROL REPORT

----- Forwarded message -----

From: Martie Sherlock <Msherlock@5thstreetcatering.com>

Date: Thu, Sep 2, 2021 at 1:04 PM

Subject: Invoice for 5th St. Catering 8/30/2021 : E62693

Please do not process CHECK payments, We are having some error issues with our check systems which has made us loose count on payment records. we cannot cash checks at the moment till further notice, We want all payment sent to us via Ach Transfer only.

Please see attached for our ACH bank account information for payment, kindly have it updated on your system for future reference.

Await your response

Thank you,

Martie Sherlock

5th Street Catering

3506 Davis Street

New Kelton, PA 40835

215.290.7594 ext. 13

Send



business email compromise
example

What is Vendor Impersonation?

Fraudsters send fake emails to companies asking for payment



vendor impersonator persona



ABCD

AGGRESSIVE **B**OUNCING **C**LUELESS **D**ESPERATELY HASTY



sign of a fraudster

A FRAUDSTER

MIGHT USE **JOHN.KELLY@COMPONY.COM**
(AN EXTRA “O” IN COMPANY) INSTEAD OF
JOHN.KELLY@COMPANY.COM TO TRICK
VICTIMS INTO THINKING THEIR EMAIL
IS LEGITIMATE.



New message



From: Shirille Jackson <s.jackson@pharmakinexx.com>
Sent: Thursday, November 11, 2021 10:03 AM
To: Invoice AP <IAccountsPayable@vistapharm.com>; Noel Greenberger
<Noel.Greenberger@verticepharma.com>
Subject: [External] Invoice 3076 from [Pharmakinexx](#), Inc. PO#01-2006 Q4 Expan. Ext.

Goodmorning,

We would like you to pay this outstanding invoice and our future invoices to our new banking details via ACH Payment. Please let me know if you have an ACH form for us to fill out or should I just email you our banking information.

Thank you,


Shirille

Shirille Jackson

PharmaKinexx
330 Milltown Road
East Brunswick, NJ 08816
732-613-4422 ext. 114
s.jackson@pharmakinexx.com

Life isn't about waiting for the storm to pass....
It's about learning to dance in the rain!

This e-mail transmission may contain confidentiality or legally privileged information that is intended only for the individual or entity named in the e-mail address. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or reliance upon the contents of this e-mail is strictly prohibited. If you have received this e-mail transmission in error, please reply to the sender and then please delete the message from your inbox.

 Please consider the environment before printing this e-mail.

Send

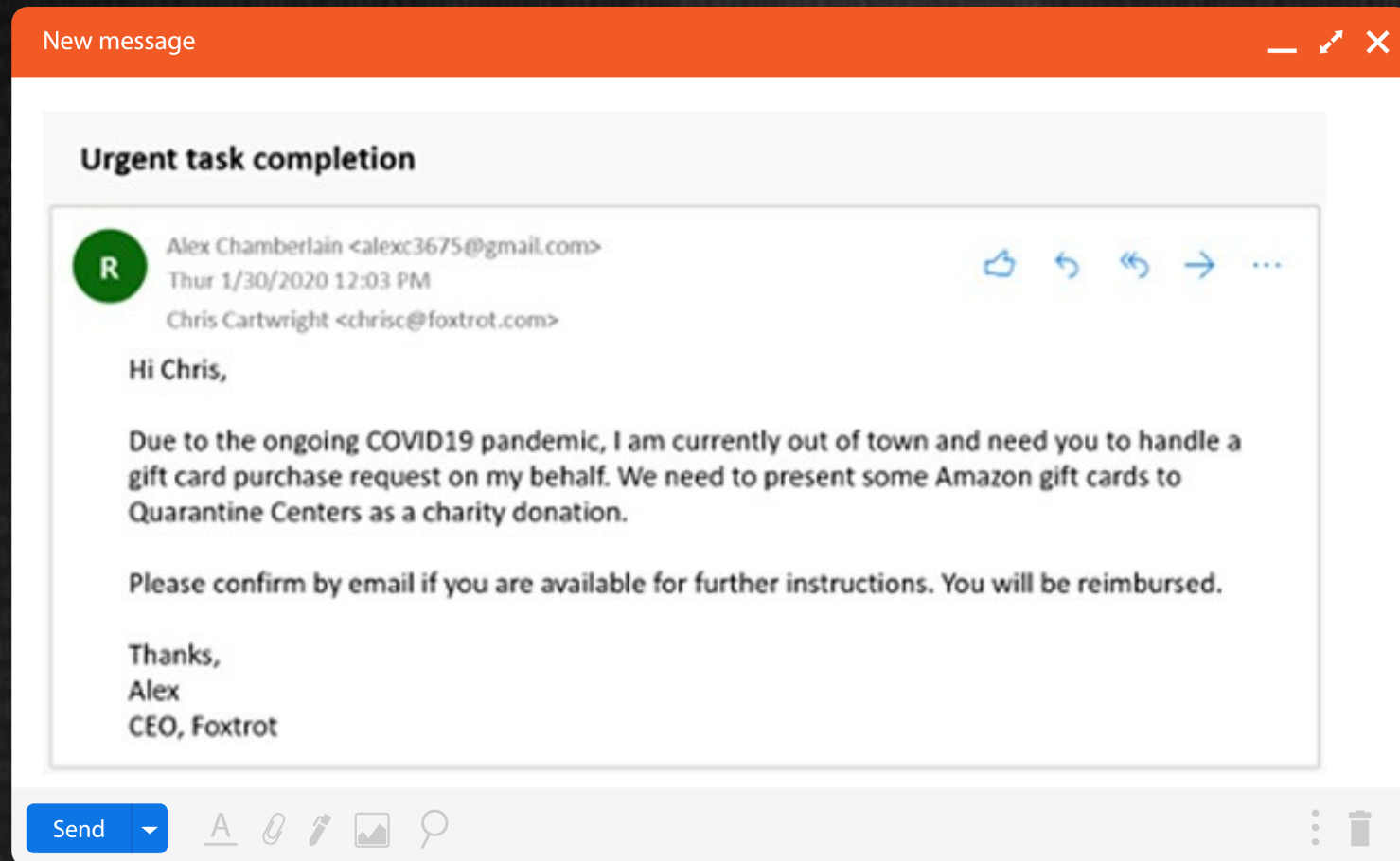


What is Phishing?

Fraudsters send a fake message designed to trick a victim into revealing sensitive information so the attacker can expose the victim's device to malicious software, get their credit card information and passwords.



phishing examples





practical steps

AS LONG AS THERE IS MONEY AND VALUABLE DATA, THERE WILL BE FRAUD ATTEMPTS AND THREATS TO SECURITY



PAYMENT

- Positive 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