WHO BEARS THE RISK OF LOSS WHEN HACKED?

Presented by:

Ted Hamilton

and

Lorna Walker

Western Region Meeting 2022

BUSINESS EMAIL COMPROMISE (EMAIL ACCOUNT COMPROMISE)

- Scam that targets both individuals and businesses who perform transfer-of-funds transactions such as wire or automated clearing house transfers; or,
- Scam may seek employees' personally identifiable information ("PII") or wage information such as W-2 forms

BUSINESS EMAIL COMPROMISE

- Cloud-based email services allow users to conduct business via tools such as email, shared calendars, online file storage, and instant messaging
- A cybersecurity criminal will compromise legitimate business or personal email accounts
- Small and mid-sized businesses, or those with limited IT resources, are the most vulnerable

BUSINESS EMAIL COMPROMISE STATISTICS

- Between May 2018 and July 2019, there was a 100% increase in losses due to business email compromise (BEC) claims
- Between 2019 and 2020, there was a 110% increase in complaints
- Between July 2019 and December 2021, there was a 65% in losses from BEC
- Between 2016 and 2021, $43 billion in losses were due to BEC
- In 2021, BEC attacks were the biggest contributor to cybercrime losses, with victims losing $2.4 billion
- Between January 2014 and October 2019, $2.1 billion losses from BEC scams were from two popular cloud-based email services
- Exposed loss for U.S. victims is close to $15 billion
- Fraudulent transfers have been made to 144 countries and has been seen in all 50 states
- Thailand and Hong Kong banks remain primary location for receiving banks, with China in third
- Increasing in United Kingdom, Mexico, Singapore, and Turkey

HOW BEC WORKS

- The scammers typically gain access to a company's email accounts or spoof their email addresses
- The criminals exploit the compromised email accounts for illegal fund transfers to accounts under their control
- The scammer asks the recipient to make a wire transfer, divert payroll, change banking details for future payments etc.
- Targets the inboxes of employees who handle the financial decisions
- Targets wire and ACH transfers
- Target small, medium, and large businesses, although individuals can be targeted if amounts are large enough
- Success rate is very high, given that they impersonate someone who has the target's trust, such as business partners or company executives
- The average Business Email Compromise attack targets no more than six employees

TYPES OF BEC SCAMS

Invoice Scam - Attackers impersonate a company's trusted supplier to request payment be wired to a fraudulent account for a fake invoice.

CEO Scam - Scammers impersonate higher-level executives (CEO's, CFO's, or COO's) of the targeted company who send emails to employees in finance requesting them to transfer money to the account controlled by the scammers. These scams are usually accompanied with an urgent message for funds to be wired immediately.

Account Compromise - An executive or employee's email account is hacked and used to request invoice payments from vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts.

Attorney Impersonation - Attackers pretend to be a lawyer or someone from the law firm supposedly in charge of crucial and confidential matters. Normally, such bogus requests are done through email or phone, and during the end of the business day.

HR/Payroll ("Data") Theft – Employees under HR and bookkeeping are targeted to obtain personally identifiable information (PII) or tax statements of employees and executives. Such data can be used for future attacks such as CEO fraud.

BEC AND MONEY TRANSFERS

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- Scammers compromise business email accounts to redirect payments or to conduct unauthorized transfer of funds to attacker-controlled bank accounts
- The average loss involving wire transfers is $35,000
- The average amount lost per company was $270,000
- Historically, attacks relied on domain impersonation and email spoofing
- Today, scammers are turning to the more sophisticated account takeover methods

BEC AND PAYROLL DIVERSION FUNDS

T. HAMILTON & L. WALKER CLLA
WESTERN REGION 2022

- HR or payroll representatives receive an email appearing to from employee requesting to update their direct deposit information for their pay
  - Some receive phishing emails prior to receiving requests for changes to direct deposit accounts
- Employees receive an email with a spoofed log-in page for an email host, and then enter their usernames and passwords allowing access to their email accounts so scammers' emails are sent legitimately
- BEC and payroll diversion increased 815 percent between January 1, 2018 and June 30, 2019

BEC IS DIFFICULT TO DETECT

BEC attacks rely on impersonation and other social engineering techniques and impersonation to trick people interacting on the attacker's behalf.

Traditional threat detection solutions that analyze email headers, links, and metadata often miss BEC attack strategies.

BEC attacks don't use malware or malicious URLs that can be analyzed with standard cyber defenses.

BEC and EAC are difficult to detect and prevent even with legacy tools, point products and native cloud platform defenses.

IMPERSONATION TECHNIQUES

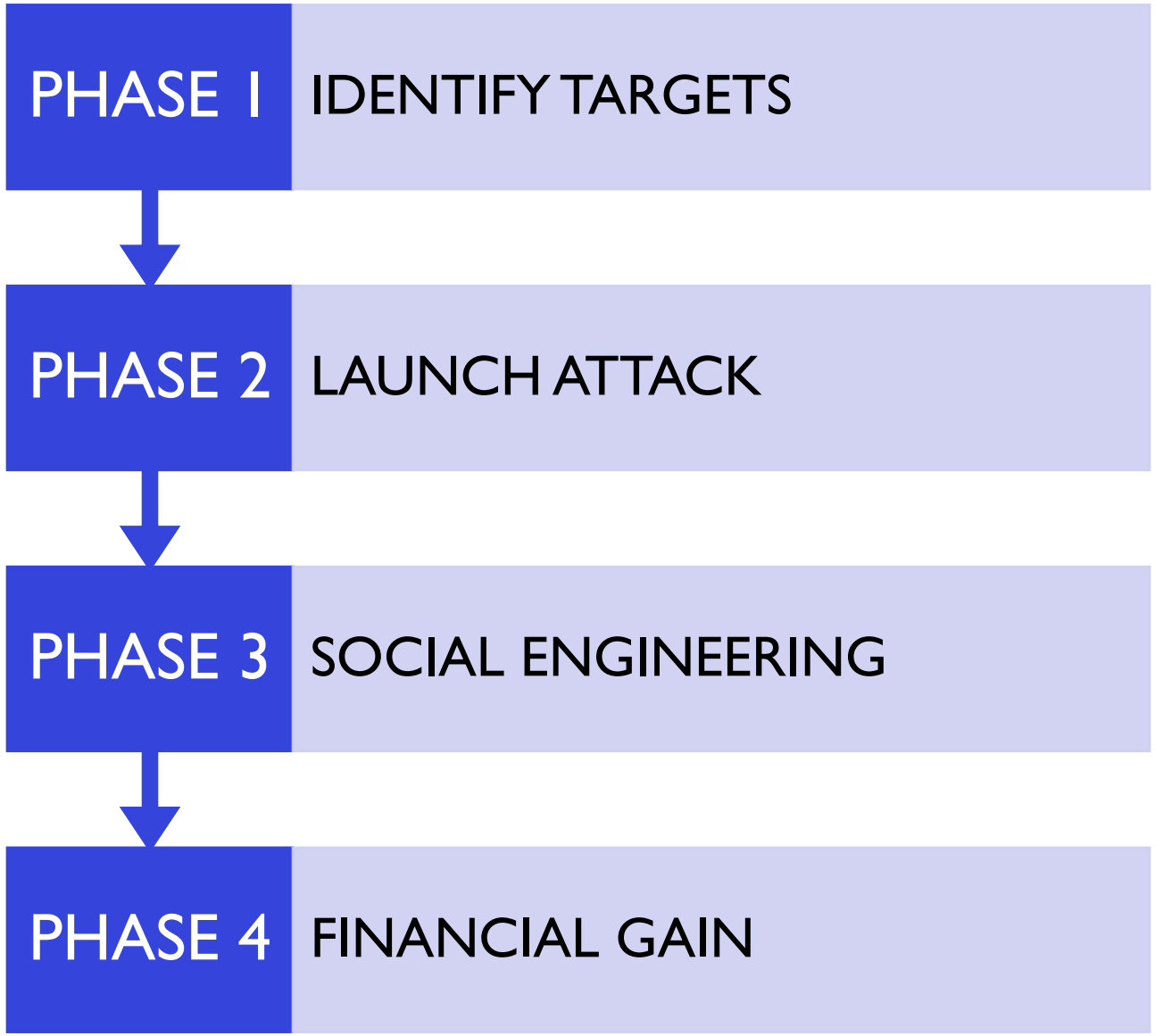
Domain spoofing or lookalike domains

- These attacks are effective because domain misuse is a complex problem. Stopping domain spoofing is difficult, especially when every domain of an outside partner could be used in a BEC attack to exploit users' trust.

Gain control of a legitimate email account

- Allows perpetrator to launch similar BEC-style. In these cases, the attacker isn't just posing as someone, but essentially *is* that person.

BEC PROCESS



T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

PHASE 1: IDENTIFY TARGETS

- BEC attacks are usually focused on executives or employees authorized to make payments on behalf of their organizations.
- Attackers perform reconnaissance over days or weeks, mining contact data from websites, social media, and the dark web. They build a profile of their target organization and then zero in on their victims. Common BEC targets include CEOs, lawyers, and accounts payable personnel.
- The attackers begin by building a targeted list of emails. Common tactics include mining LinkedIn profiles, sifting through business email databases, or even going through various websites in search of contact information.

PHASE 2: LAUNCH ATTACK

- Attackers begin rolling out their BEC attacks by sending out mass emails. It's difficult to identify malicious intent at this stage since attackers will utilize tactics such as spoofing, look-alike domains, and fake email names.
- Unlike mass phishing emails that follow a "spray and pray" approach, BEC attacks come across as believable and legitimate.
- Scammers prepare for the attack by performing activities such as spoofing email addresses or creating lookalike domains, impersonating trusted vendors, or taking over a legitimate email account of the victim's manager or colleague.

PHASE 3: SOCIAL ENGINEERING

- At this stage attackers will impersonate individuals within a company such as CEOs or other individuals within finance departments. It's common to see emails that request urgent responses.
- The actual BEC attack can take place in one email or an entire thread, depending on the adversary's thoroughness.
- The communication often uses persuasion, urgency, and authority to gain the victim's trust.
- The perpetrator then provides wire instructions to the victim to facilitate making payments to a fraudulent account.

PHASE 4: FINANCIAL GAIN

- If attackers can successfully build trust with an individual, this is typically the phase where financial gain or data breach is made.
- Once the money is wired to the attacker, it is quickly collected and disseminated across multiple accounts to reduce traceability and retrieval chances.
- Rapid response times are critical for most cybersecurity incidents, and the same holds true for BEC attacks.
- If organizations are slow to identify a BEC attack that has been executed successfully, it's unlikely that the money will be recovered.

DETECTION OPTIONS FOR BEC

	Vector and Delivery	Techniques	Payload	Legacy Email Controls
Spam	Mass email	N/A	Known malicious link or executable	✓
Mass phishing	Mass email	Mass-produced phishing kits	Known malicious link or executable	✓
VIP Impersonation	Gmail/Yahoo, lookalike domains	Social engineering	"Soft" payload as an ask/request, fake attachments	✗
Payroll fraud	Gmail/Yahoo, lookalike domains	Impersonation, social engineering	"Soft" payload as an ask/request	✗
Vendor fraud	Email from compromised account	Impersonation, social engineering	"Soft" payload as an ask/request, fake attachments	✗
Credential phishing	Email from compromised account, Gmail/Yahoo	Redirects, brand impersonation for login pages, 0-day domains	0-day links, fake attachments	✗
Account takeover	Credential phishing attack	Auto-forwarding rules, lateral movement	0-day links, fake attachments	✗

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

MOST COMMON WAYS TO COMPROMISE BUSINESS EMAIL

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

SPOOFING

HACKING

PHISHING

SPOOFING

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

EMAIL ACCOUNT

- Variations on a legitimate email
  - Lorna.Walker@sweetwalker.com v. Lorma.Walker@sweetwalker.com

WEBSITE

- Create website to trick victims into thinking website is real

HACKING

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- Social engineering
  - Makes it possible for cybercriminals to impersonate one of the people involved in those money transfers to make the victim send the money to a cybercriminal-owned banking account.

HACKING TRICKS

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- **Exploiting Trusted Relationships**
  - To urge victims to take quick action on email requests, attackers make a concerted effort to exploit an existing trusted relationship. Exploitation can take many forms, such as a vendor requesting invoice payments, an executive requesting iTunes gift cards, or an employee sharing new payroll direct deposit details.

HACKING TRICKS

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- **Replicating Common Workflows**
  - An organization and its employees execute an endless number of business workflows each day, many of which rely on automation, and many of which are conducted over email. The more times employees are exposed to these workflows, the quicker they execute tasks from muscle memory. BEC attacks try to replicate these day-to-day workflows to get victims to act before they think.
  - Compromised workflows include:
    - Emails requesting a password reset
    - Emails pretending to share files and spreadsheets
    - Emails from commonly used apps asking users to grant them access
- **Suspicious Attachments**
  - Suspicious attachments in email attacks are often associated with malware. However, attachments used in BEC attacks forego malware in exchange for fake invoices and other social engineering tactics that add to the conversation's legitimacy. These attachments are lures designed to ensnare targets further.

HACKING TRICKS

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- **Socially Engineered Content and Subject Lines**
  - BEC emails often rely on subject lines that convey urgency or familiarity and aim to induce quick action.
  - Common terms used in subject lines include:
    - Request
    - Overdue
    - Hello “First Name”
    - Payments
    - Immediate Action
  - Email content often follows along the same vein, with manipulative language that make specific, seemingly innocent requests. Instead of using phishing links, BEC attackers use language as the payload.

HACKING TRICKS

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- **Leveraging Free Software**
- Attackers make use of freely available software to lend BEC scams an air of legitimacy and help emails sneak past security technologies that block known bad links and domains.
- For example, attackers can use :
  - SendGrid to create spoofed email addresses
  - Google Sites to put up phishing pages
  - Google Forms
  - Google Docs
- These software platforms can be used to:
  - Extract sensitive data from victims
  - Host phishing links and fake invoices in Box and Google Drive

PHISHING

- Cyber criminals use phishing kits that impersonate popular cloud-based email services
- Target victims using cloud-based services
- Cyber criminals analyze the content of compromised email accounts for evidence of financial transactions
- Configure mailbox rules of the compromised account to delete key messages
- May also enable automatic forwarding to an outside email account

PHISHING TRICKS

- Impersonate email communications between businesses and third parties, such as vendors and customers, to request payments be redirected to a fraudulent bank account
- Cyber criminals often access the address books of compromised accounts to identify new targets to send phishing emails
- Can lead to multiple victims from one compromised account

LAW DETERMINING LIABILITY

- There is no specific code dealing with these types of transactions
- Courts have looked to:
  - UCC Article 3 (Negotiable Instruments)
  - UCC Article 4A
  - Breach of contract rules, including:
    - UCC Article 2
    - Agency principles
  - Common law

ARTICLE 3: NEGOTIABLE INSTRUMENTS

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- Sections:
  - 3404 - imposters; fictitious payees
  - 3403 - unauthorized signatures
  - 3406 - negligence contributing to forged signature or alteration of instrument
- The party who is in the best position to prevent the fraud bears the burden of loss
  - *E.g.*, Who had the "last chance" to prevent the loss?
  - Fact specific

ARTICLE 3: COMMON FACTORS

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- Did each party exercise ordinary care?
  - *i.e.*, Did a party ignore red flags?
- Did the seller have safety protocols in place to protect their email system?
- Did the seller previously have its email system hacked?
  - If so, did the seller notify its customers?
- Did the buyer receive conflicting emails with different payment instructions over a short period of time?
- What were the nature of the wire instructions?
  - *e.g.*, wire to a foreign bank account, to a bank outside the seller's region, or to an unknown beneficiary
- What was the nature of the fraudulent email?
  - Was the email address identical to the seller's email?
  - Was the email address similar to the seller's email?
  - Did the email use the correct name, spelling, phrasing, and jargon?
  - Were there changes or inaccuracies that would raise suspicions?
- Were protocols followed?

ARTICLE 4A: FUNDS TRANSFERS BY ELECTRONIC MEANS

- Adopted in all 50 states
  - Check for variations
- Establishes uniform and predictable rights, duties, and liabilities regarding funds transfers
- Imposes on banks the obligation to refund unauthorized funds transfers for a one-year period after the bank gives the customer notice
- The bank can limit its liability in two ways:
  - The payment order initiating an electronic transfer if the sender authorized it with actual or apparent authority; or,
  - If the account holder and the bank have agreed that authorization for the payment order will be verified by a security procedure (such as a PIN)
    - Then, the payment order is reasonable if compliance with this procedure is reasonable and such compliance occurred

ARTICLE 4A: LIABILITY PRINCIPLES

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- Banks will routinely enter into agreements specifying the security procedures the bank will use.
  - A review of whether these procedures were followed may result in bank liability.
- A review after the fact is helpful, but one should review these procedures in advance.
  - What does your bank require to initiate a wire transfer?
  - Is it reasonable?
  - What are the potential vulnerabilities?
  - Are you following it?

BREACH OF CONTRACT & ARTICLE 2

- Assigns liability to the party who failed to comply with the contractual obligation
  - Typically, this is the party who wired the funds to a fraudulent account
- Does not address who acted reasonably
- Only looks at the fact that buyer agreed to pay seller for goods/services and must comply with that obligation
- Minority rule

AGENCY PRINCIPLES

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- Apparent or Ostensible Authority
  - Hacked seller intentionally or inadvertently induced an innocent buyer into believing that the person emailing was its agent
  - Fraudsters conduct is irrelevant
  - Critical Factor is whether the seller's actions or omissions gave rise to the buyer's reasonable belief the fraudster was the seller's agent
- Most courts have declined to apply this principle

ATTORNEY DUTIES

- Attorneys have an ethical obligation to take reasonable efforts to prevent the inadvertent or unauthorized disclosure of information relating to the representation of a client
- Attorneys must safeguard confidential information including, but not limited to:
  - Electronic transmissions
  - Communications

CASE LAW ADDRESSING BEC

ARTICLE 3

ARROW TRUCK SALES, INC. V. TOP QUALITY TRUCK & EQUIP., INC.
(CASE NO. 8:14-CV-2052-T-30TGW, 2015 WL 4936272 (M.D. FLA. AUG. 18, 2015))

- Arrow paid a hacker after receiving one invoice from the hacker and one from the seller
- Fraudsters hacked into both buyer's and seller's email accounts
  - Created new email accounts that were almost identical and also sent emails from the legitimate accounts
  - Sent "updated" wire instructions from both legitimate and fraudulent emails
- Creditor sent invoice with valid wire instructions and identical to prior invoices
- Arrow did not inquire before sending the payment even though account information was different from original invoice and prior transactions
- Court applied UCC Article 3 imposter rule finding:
  - The buyer (Arrow) was in the best position to prevent the fraud given conflicting accounts
  - The buyer "should have exercised reasonable care after receiving conflicting e-mails containing conflicting wire instructions by calling [the seller] to confirm or verify the correct wire instructions."
- Court found that the failure to pay was a breach of contract
- Court found seller was not negligent in handling its email account

BILE V. RREMC, LLC,

(2016 U.S. DIST. LEXIS 113874 (E.D. VA. AUGUST 24, 2016))

- After reaching a settlement in pending litigation, Plaintiff's attorney received an email purportedly from his client, which was visually similar to his client's actual email (aoi.com v. aol.com), directing him to wire the settlement funds to a London bank
- Plaintiff's attorney called his client and was told that email was not valid
- Plaintiff's attorney deleted that email without telling anyone
- Plaintiff's counsel thereafter demanded an accelerated payment from Defendant and threatened to withdraw from the agreement if not made
- Attorneys spoke by phone to discuss how payment would be made, agreeing to remit payment via check, with Plaintiff's counsel stating he would confirm transmission instructions via email
- Defendant's attorney thereafter received an email from Plaintiff's attorney's valid email server requesting the money be wired to a particular account
  - It mirrored the "atypical" greeting and shortened family name of Defendant's attorney
  - It reiterated the demand for early payment
  - It contained typing errors similar to Plaintiff's attorney's prior emails
- The money was wired per the email instructions
- After discovering the account was fraudulent, Defense counsel attempted to recall it, but was unsuccessful

BILE V. RREMC, LLC (CONTINUED)

(2016 U.S. DIST. LEXIS 113874 (E.D. VA. AUGUST 24, 2016))

- Court found Defendant did not breach the settlement agreement since it substantially performed even though it remitted payment to a fraudulent account
- The court relied on Articles 3-420, 3-404 and 3-406 in finding that Defendant substantially complied with the agreement and had exercised reasonable care
- The court further found Plaintiff's attorney had not exercised ordinary care and, thus, Plaintiff was liable for the loss
- Since Defendant was a blameless party, it is entitled to rely on reasonable representations, even if made by fraudsters

c.f.,
2 HAIL, INC. V. BEAVER BUILDERS, LLC
(2017 COLO. DIST. LEXIS 1294 (D. COLO. NOVEMBER 29, 2017))

- Colorado District court rejected the *Biles* court analysis and found no legal theory applicable to allocate responsibility based on relative fault
- Imposed liability on the party whose payment was misdirected

JETCRETE NORTH AMERICA LP
v.
AUSTIN TRUCK & EQUIPMENT, LTD.
(484 F. SUPP. 3D 915 (D. NEV. 2020))

- Plaintiff negotiated a purchase of equipment over the phone and by email
- Defendant sent Plaintiff wire instructions via email and Plaintiff wired a down payment
- Thereafter, Plaintiff received another email with different wire instructions
- Plaintiff remitted the remaining payment to the new bank
- Defendant refused to deliver the equipment until payment was received
- Plaintiff filed suit for breach of contract, along with other claims
- The court found Plaintiff should suffer the loss under Nevada Commercial Code because:
  - It was in the best position to prevent the loss by taking reasonable precaution to verify the wiring instructions by phone
  - "The failure to do so is especially disconcerting after Jetcrete received conflicting email instructions within minutes of each other:
- The court rejected the allegation that the hacker was Defendant's agent

PARMER V. UNITED BANK, INC.

(NO. 20-0013, 2020 WL 7232025 (W. VA. DEC. 7, 2020))

- Parties reach a settlement agreement, which required Plaintiff to pay Defendant
- Plaintiff's counsel requests wire instructions and receives an email purportedly from Defendant's attorney instructing him to wire the money to an account held in a non-party company name located in Texas
  - Plaintiff's prior wire was to an account in Defendant's name located in West Virginia
- Plaintiff's counsel instructs the bank to send the wire to the bank in Texas
- Thereafter, the parties discovered that someone had intervened in the parties' counsels' e-mail communications using defense counsel's identical e-mail address and an e-mail address nearly identical to Plaintiff's counsel's address to provide fraudulent wire transfer instructions
- The court followed the *Arrow Truck Sales* case and applied the "imposter rule" to hold Plaintiff liable since she was "the party who was in the best position to prevent the forgery by exercising reasonable care suffers the loss"
- Specifically, the court found that:
  - Plaintiff or her counsel failed to exercise reasonable care since they did not verify the wire transfer instructions her counsel received
  - The wire transfer instructions were plainly suspect in that they directed payment to an entity uninvolved in the parties' dealings and unknown to Defendant
  - The parties' dealings date back to 2014 and involve one prior wire transfer directly to Defendant in West Virginia, not an uninvolved, outside entity

ARTICLE 4A

T. HAMILTON & L. WALKER CLLA WESTERN REGION 2022

ARTICLE 4A

- Under Article 4A, the bank generally bears the risk of loss for any fraudulent payment
- A bank can shift this risk if:
  - It can prove the customer authorized the transaction; or
  - The bank and customer agree to a security procedure designed to protect against fraud and:
    - (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders
    - (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.
- A security procedure is deemed to be commercially reasonable if
  - (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and
  - (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer

CHOICE ESCROW AND LAND TITLE, LLC
V.
BANCORPSOUTH BANK
(754 F.3D 611 (8TH CIR. 2014))

- Plaintiff held a trust account at Defendant bank and performed wire transfers through its online banking platform
- Defendant provided four security measures to ensure only Plaintiff's employees could access the account
  - Plaintiff declined the use of one of the four measures that required a second authorized user to approve any transfer (it declined it twice)
- Plaintiff's employee fell prey to a phishing scam causing the company to contract a computer virus that led to a series of fraudulent transactions
- Because the request was made using Choice's User ID and Password, the bank approved the fraudulent transfer request even though the account lacked sufficient funds to cover the transfer. *Id.* at 616

BREACH OF CONTRACT, ARTICLE 2 & AGENCY LAW

T. HAMILTON & L. WALKER CLLA WESTERN REGION 2022

MERITDIAM, INC. V. FACETS FINE JEWELRY, LLC
(NO. CV1407041MWFCWX, 2015 WL 12660377, AT *6 (C.D. CAL. APR. 27, 2015))

- Plaintiff sent an invoice via email with wire instructions
- Three days later, Defendant received another email with different instructions to an out-of-state bank
- Defendant attempted to make the payment to the new bank, but it could not be processed as the information was incorrect
- After sending an email to Plaintiff, Defendant received new instructions and remitted the payment
- Court denied Plaintiff's motion for summary judgment finding it was an issue of fact
  - "[T]he Court believes that liability will likely lie with the party the jury determines was most greatly at fault in causing the payment to be misdirected. Meritdiam either allowed unauthorized access to its email account or failed to prevent its system from being hacked[.] . . . JB Hudson did not pick-up on certain clues in the emails[.] These are issues for the jury."

TILLAGE COMMODITIES FUND LP V. SS&C TECH., INC.
(151 A.D. 3D 607, 608-609 (1ST APP. DEP'T 2017))

- Service provider to a fund wired $5.9 million out of the funds account based on fraudulent email instructions
- The fund sued for breach of contract, breach of the implied covenant of good faith and fair dealing, and violations of the state's General Business Law code
- Defendant moved to dismiss
- Court sustained the breach of contract claim on the grounds that plaintiff has sufficiently alleged that defendant "failed to comply with basic cybersecurity precautions and actively disregarded its own policies as obvious red flags. This is especially true in light of defendant's awareness that the transfers . . . would result in near depletion of plaintiff's account."

BEAU TOWNSEND FORD LINCOLN INC V. DON HINDS FORD INC.
(759 F. APP. 357 (2018))

- Seller's (Plaintiff) email was compromised
- Hacker filtered out any email from buyer (Defendant) that would have tipped off seller to the fraud
- Fraudster then sent wire instructions for an out-of-state bank and buyer wired the money
- Seller sued for (1) breach of contract, (2) conversion, and (3) unjust enrichment, constructive trust, and disgorgement
- Trial court granted summary judgment against the buyer
- Sixth Circuit reversed summary judgment order and remanded stating the determining factor was "*whether either [party's] failure to exercise ordinary care contributed to the hacker's success*" and that such factual determination required a trial
- Court evaluated case under contract law (mutual mistake), UCC Article 2, and agency law

JF NUT V. SAN SABA PECAN, LP

(2018 WL 7286493 (W.D. TEX., JULY 23, 2019))

- Defendant made 18 purchases of pecans and paid for each using wire instructions that Plaintiff sent via email
- Two months into the purchases, Defendant received updated wiring instructions from Plaintiff's email account which as sent from a fraudster who hacked Plaintiff's email account
- Defendant began wiring payments to the fraudulent account
- Plaintiff sued for breach of contract
- Court concluded that party in the best position to prevent the fraud should suffer the loss for a misdirected payment
- Liability would be determined based on an allocation of fault between the parties as determined by a jury

COMMON LAW

PROSPER FLORIDA, INC.
V.
SPICY WORLD OF USA, INC.
(NO. 01-20-00104-CV, TEXAS APP. CT. (1ST DIST. 2022))

- Third party accessed both Plaintiff's and Defendant's email accounts
- Defendant received three different sets of wire instructions, each for a different account, but did not notice the difference
- Defendant claims it originally objected to paying via wire transfer
- Defendant also claimed it confirmed by phone that Plaintiff wanted the money wired to a foreign bank, did not verify the account number or specific bank on the phone
  - Plaintiff disputed this fact
- The court relied on Texas common law to find that the buyer was not obligated to make a second payment as seller was most at fault for not preventing the fraud
  - "We likewise are persuaded that the correct rule is that any loss resulting from fraudulently misdirected payments should be placed on whichever party to the contract the factfinder finds to be most at fault for the misdirection."
- *NOTICE: THIS OPINION IS UNPUBLISHED*

ATTORNEY'S DUTIES

BILE V. RREMC, LLC

(2016 U.S. DIST. LEXIS 113874 (E.D. VA. AUGUST 24, 2016))

- Two days before the fraud was perpetrated, both Plaintiff and Plaintiff's attorney were aware that an unidentified third party had targeted the settlement funds for diversion to a foreign bank account
  - Court found that Plaintiff and his attorney "*knew*" that the attorney's email was being used in an effort to perpetrate the fraud
- Plaintiff's attorney failed to pass this information along to Defendants, defense counsel, or the Court.
- Although court found no authority that requires an attorney to notify opposing counsel when the attorney has actual knowledge that a third party has gained access to information that should be confidential, such as the terms of a settlement agreement, or the attorney has knowledge that the funds to be paid pursuant to a settlement agreement have been the target of an attempted fraud, the court found this "principle is an eminently sensible one"
- Applying that standard, the court found that Plaintiff's attorney failed to exercise ordinary care
  - The request redirected a pre-existing payment request, and that preexisting payment request had been discussed via phone as well as email
- The court also found that Defendant's attorney acted reasonably
  - "Sending a wire transfer to a known defendant on behalf of a known client is not the same as receiving a check from an unknown defendant and wiring funds to an unknown client"

HOW TO AVOID BEING A VICTIM OF BEC

Focus on human frailty rather than technical vulnerabilities, as they require a people-centric defense that can prevent, detect, and respond to a wide range of BEC and EAC techniques.

→

Don't be pressured into sending money without doing some additional digging first. It may well prove to be one of the smartest work decisions you'll ever make.

→

Listen to your gut: If something doesn't look or feel right, don't be afraid to investigate.

DON'T RELY SOLELY ON NATIVE EMAIL SECURITY

Audit your existing email security capabilities to find out what you've already invested in.

- Microsoft recently launched a free Office 365 Configuration Analyzer, which will recommend the proper configurations for native O365 email security procedures, helping override rules and guidelines that give organizations lower protection.

Once you clearly understand what your native email security can and cannot do, make a plan to augment these baseline capabilities with security layers that are designed to stop BEC attacks.

WHAT SPECIFIC STEPS CAN YOU TAKE TO AVOID BEING A VICTIM OF BEC?

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- When Reading Emails, Always Be Skeptical
  - Do not rely on information sent in an email
  - Establish rules for suspicious looking emails coming into the organization or being sent around internally
- Change email passwords regularly to prevent hacking
  - Use 2-factor authentication to change passwords
- Deactivate former employee email accounts
- Use secondary methods or two-factor authentication to confirm information and instructions received via email
  - *Confirm information by phone!*
- Do not send sensitive details such as login credentials and personal identifiable information via email
- Do not respond on a mobile device

WHAT SPECIFIC STEPS CAN YOU TAKE TO AVOID BEING A VICTIM OF BEC?

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- Verify emails are legitimate
  - Check for subtle misspellings or changes in domain names and email addresses
    - View full email extensions
  - Especially emails that include:
    - High-level executives asking for unusual information
    - Requests to not communicate with others
    - Requests that bypass normal channels
    - Requests that drop others from the email chain
- Limit the amount of social media data
  - Use generic “catch-all” email addresses on the contact page
  - Don’t tell everyone on social media that the CEO/CFO is on vacation or travelling
- Do not open suspicious emails from random addresses with attachments
  - Quarantine or delete

IMPLEMENT WIRE/ACH TRANSFER PROTOCOLS

- Instruct employees to ignore requests for wire transfers without verifying the information, especially if urgent or it has last minute account changes
  - Phone call is best to verify!
- Require some form of authentication to confirm the transfer *before sending any* transfer
- Use Multi-Factor Authentication for any financial activity
  - App-based authentication or a physical hardware token
  - Sometimes attackers aren't just spoofing real emails, they're compromising them to send money requests too

SUGGESTED WIRE TRANSFER PROTOCOLS IF SENDING BY EMAIL

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- Use encrypted email
- Send password protected instructions
- Truncate the account number on the instructions
- After sending the email, call the number of your contact person to give them the password and only the truncated digits of the account number
  - The sending office should initiate the call to the person they routinely deal with *at the number* in the account
  - Do not give the information out to anyone who calls
  - Do not give the full account number
- Once the password and last three digits are provided, request that the recipient call back before sending the wire to verify the full account number

CHECK THEFTS

- Thieves alter checks by changing the amount or the payee name
- They cash the check over the counter, deposit it into a new account and withdraw the funds before anyone detects anything or find other methods of getting the cash
- Used in a variety of schemes
  - Can be inside job

TYPES OF CHECK FRAUD

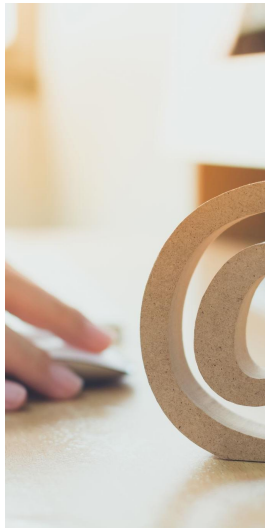
Altered, either as to the payee or the amount

Counterfeited

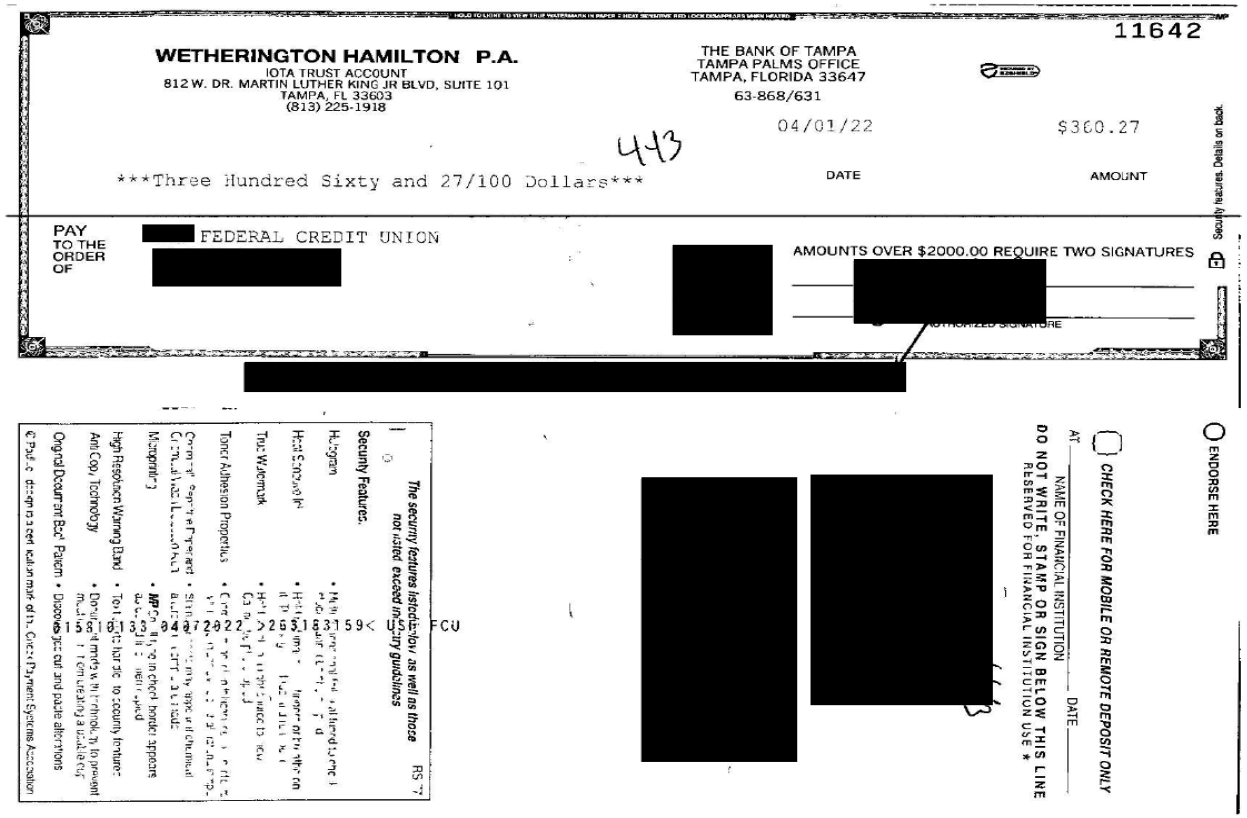
Forged, either as to signature or endorsement

Drawn on closed accounts

WAYS THIEVES OBTAIN CHECKS



- Getting customer information from insiders
- Stealing bank statements and checks
- Working with dishonest employees of merchants who accept payments by check
- Rifling through trash for information about bank relationships



11642

WETHERINGTON HAMILTON P.A.
IOTA TRUST ACCOUNT
812 W. DR. MARTIN LUTHER KING JR BLVD, SUITE 101
TAMPA, FL 33603
(813) 225-1918

THE BANK OF TAMPA
TAMPA PALMS OFFICE
TAMPA, FLORIDA 33647
63-868/631

04/01/22 DATE

$360.27 AMOUNT

443

Three Hundred Sixty and 27/100 Dollars

PAY TO THE ORDER OF [redacted] FEDERAL CREDIT UNION [redacted]

[redacted]

AMOUNTS OVER $2000.00 REQUIRE TWO SIGNATURES

[redacted] AUTHORIZED SIGNATURE

[redacted]

[redacted]

ENDORSE HERE

CHECK HERE FOR MOBILE OR REMOTE DEPOSIT ONLY

AT _____ NAME OF FINANCIAL INSTITUTION _____ DATE _____

DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE
RESERVED FOR FINANCIAL INSTITUTION USE *

The security features listed do not include all security features. Details on back.

Security Features.

Hologram

Heat Sensitive Ink

True Watermark

Toner Adhesion Properties

Copy Void Pantograph

Microprinting

High Resolution Warning Band

Anti-Copy Technology

Original Document Bed Pattern

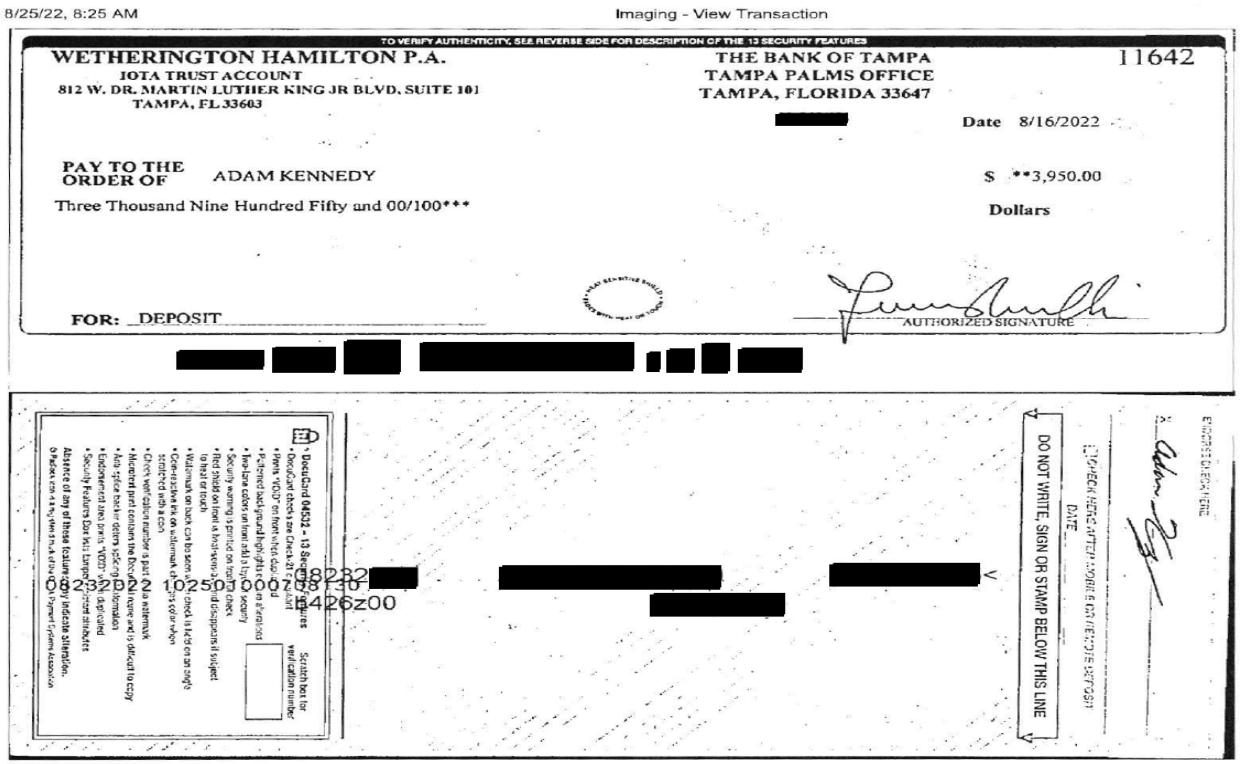
⑈[redacted]⑈ ⑆[redacted]⑆ [redacted] FCU

EXAMPLES

- Check Forgery:

T. HAMILTON & L. WALKER CLLA WESTERN REGION 2022

FORGED CHECK



8/25/22, 8:25 AM Imaging - View Transaction

TO VERIFY AUTHENTICITY, SEE REVERSE SIDE FOR DESCRIPTION OF THE 13 SECURITY FEATURES

WETHERINGTON HAMILTON P.A.
IOTA TRUST ACCOUNT
812 W. DR. MARTIN LUTHER KING JR BLVD. SUITE 101
TAMPA, FL 33603

THE BANK OF TAMPA
TAMPA PALMS OFFICE
TAMPA, FLORIDA 33647

11642

[redacted] Date 8/16/2022

PAY TO THE ORDER OF ADAM KENNEDY

$ **3,950.00

Three Thousand Nine Hundred Fifty and 00/100***

Dollars

FOR: DEPOSIT

AUTHORIZED SIGNATURE

[redacted]

DO NOT WRITE, SIGN OR STAMP BELOW THIS LINE

ENDORSE HERE

DATE

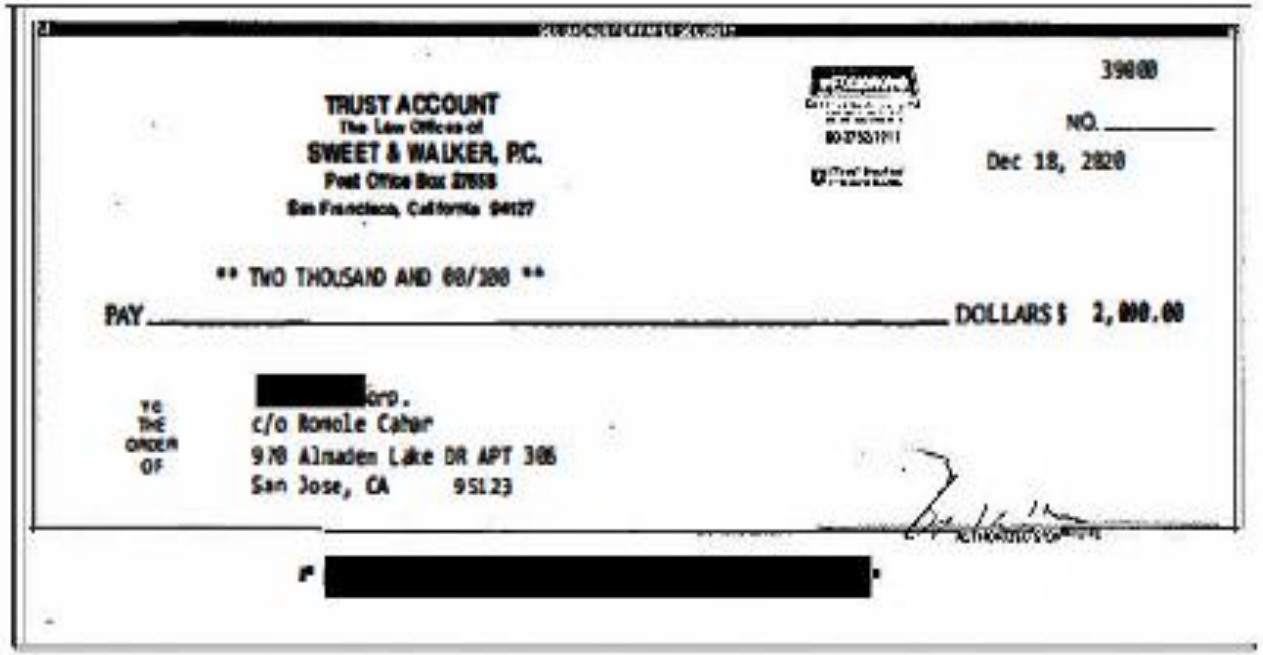
[redacted]

https://commercial.bankoftampa.com/IMG_IMG1151/IMG1151.ashx?Action=ViewTransaction&TokenLookup=NL085SBmqqQvkUUQIjHbIgw3rdbxyQh... 1/1

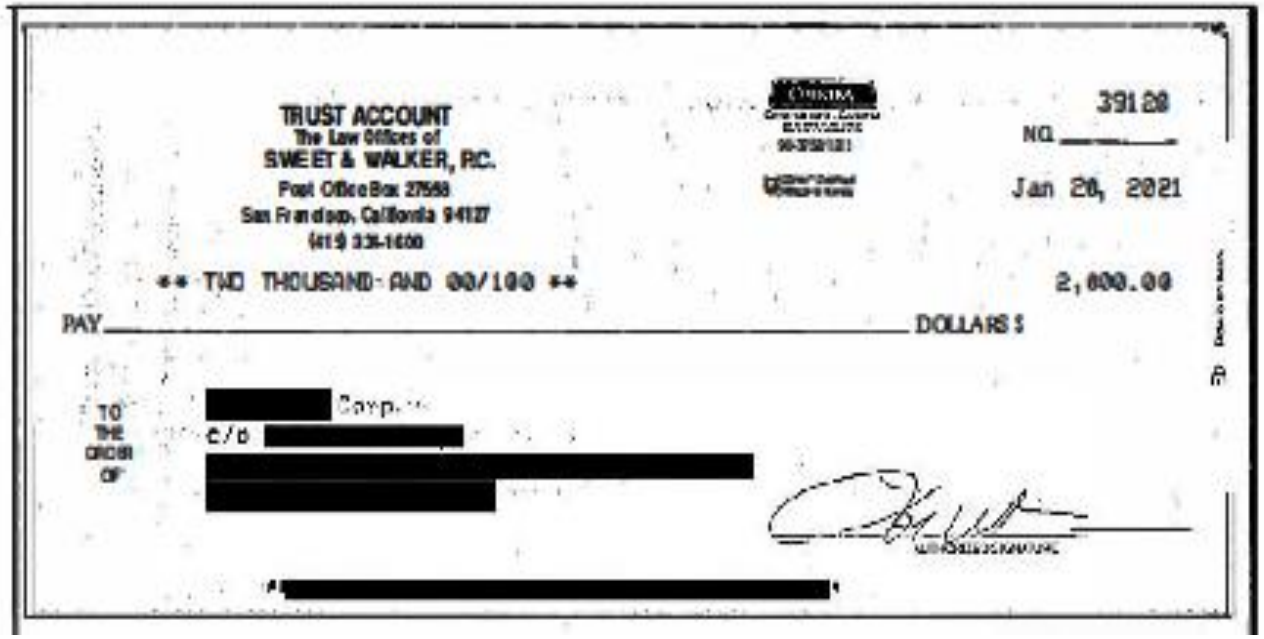
WHICH CHECK IS FORGED?

T. HAMILTON & L. WALKER CLLA WESTERN REGION 2022

JAN 22 2021 | 44243 | CHECK (SUBSTITUTE) | -$2,000.00 | $



JAN 22 2021 | 44237 | CHECK (SUBSTITUTE) | -$2,000.00 | $



WHAT SPECIFIC STEPS CAN YOU TAKE TO AVOID BEING A VICTIM OF CHECK THEFTS?

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

Use Available Bank Services

- Positive Pay - company uploads check information to bank
- Reverse Positive Pay - bank downloads check information to company
- Expedited return information
- Signature verification systems

Reconcile Bank Account Regularly

- Review Physical Checks – front and back

Establish Company Policies and Procedures

- Limit who can issue and approve check payments
- Limit the dollar limits of their authorization
- Identify who can order new check stock
- Store blank checks in a secure limited location, with limited employee access
- Require Dual Signatures
- Designate Employees to Respond to Bank Inquiries

Purchase check stock from well-established vendors

- Use safety paper

If fraud occurs, close the account as soon as possible

Use electronic payment options, if possible

COMPUTER SYSTEM COMPROMISE (HACKING)

- Scam that targets both individuals and businesses
  - Malware
  - Ransomware
  - Viruses

CASE LAW ADDRESSING COMPUTER HACKING

RESNICK V. AVMED, INC.

(693 F.3D 1317, 1330 (11TH CIR. 2012))

- Laptops were stolen from Defendant's office that contained personal information about its members
- The information was not encrypted or protected
- Plaintiffs became victims of identity theft and sued under Florida law
- Plaintiffs stated claims for negligence, breach of fiduciary duty, breach of contract, and breach of implied contract
- The 11th Circuit found that Plaintiffs "pled a cognizable injury and have pled sufficient facts to allow for a plausible inference that AvMed's failures in securing their data resulted in their identities being stolen"
- However, the court dismissed their negligence per se and breach of the implied covenant claims

IN RE BRINKER DATA INCIDENT LITIGATION

(2020 WL 691848, AT *7 (M.D. FLA. JAN. 27, 2020))

- Brinker, the parent company for Chili's Grill and Bar, had its system hacked resulting in the theft of Plaintiffs' payment card information
- Plaintiffs stated multiple claims against Defendant, including for breach of implied contract and negligence where plaintiffs sufficiently alleged a duty to use reasonable care to protect customer data from theft
- Court upheld the breach of implied contract, negligence claims, and unfair business practices pertaining to the FTC Act, California Civil Code Section 1798.81.5 (unlawful business practices and unfair business practices), but dismissed the other claims
  - **The case was recently certified as a class action*

TORRES V. WENDY'S INTERNATIONAL, LLC

(195 F. SUPP. 3D 1278 (M.D. FLA. 2016))

- Wendy's had its system hacked resulting in the theft of Plaintiffs' payment card information
- Plaintiff filed a class action for breach of implied contract, negligence, and deceptive and unfair trade practice under Florida law
- Court originally held that plaintiffs failed to state claims for breach of implied contract and negligence where plaintiffs showed no injury from the data breach
- In a later ruling, the court let certain claims stand and the case proceeded under those claims including breach of implied covenant and negligence

(*Torres v. Wendy's Int'l* (2017) U.S. district Lexis 221548 (Fla M.D. 2017))

WHAT SPECIFIC STEPS CAN YOU TAKE TO AVOID BEING A VICTIM OF COMPUTER HACKING?

T. HAMILTON & L. WALKER
CLLA WESTERN REGION 2022

- Limit requests for and acceptance of confidential information
- Lock your PC, laptop, and server with a PIN
- Encrypt discs on all devices, including thumb drive and removal hard drives
- Update your software and operating systems, including anti-virus and anti-malware
- Do not use administrative logins for daily work
  - Set up a separate login
- Use a Virtual Private Network
- Back-up your critical data
- Buy cybersecurity insurance
- Turnoff Bluetooth and use Wi-Fi only when necessary
  - Use a personal hotspot instead of Wi-Fi
- Use a privacy screen
- Avoid using free/personal email accounts
- Send sensitive documents through secure file transfer software, not email
- Confirm the sender before opening any attachments before clicking on links
- Use complex passwords
- Use different passwords for different accounts
- Do not have your browser save passwords
- Use multi-factor authentication when available

REPORT FRAUD

- If you do become a victim of email compromise fraud, immediately call the business's bank and report it to the FBI. Authorities say, if it's done within 48 hours, there is a chance the money could be recovered.
- The federal law enforcement agency advises those who fall victim to BEC fraud to immediately reach out to their bank to request a recall of funds.
- They're also urged to file a complaint with the FBI at BEC.ic3.gov, regardless of the lost amount, and as soon as possible.