WRIGHT KIM DOUGLAS
A Law Corporation

IT'S A TRAP, DON'T FALL FOR IT!

BIOS

DAVID KIM

WRIGHT KIM DOUGLAS ALC- MANAGING PARTNER

130 SOUTH JACKSON STREET, GLENDALE, CA 91205

818-689-0926

DAVID@WKDLEGAL.COM

DAVID KIM, MANAGING PARTNER AT WRIGHT KIM DOUGLAS IS AN EXPERIENCED LITIGATOR WITH AN EXTENSIVE BUSINESS AND REAL ESTATE BACKGROUND, AND HANDLES EXCLUSIVELY PROBATE AND TRUST MATTERS, BOTH LITIGATED AND NON-LITIGATED.

MR. KIM HAS SUCCESSFULLY CONDUCTED SEVERAL NOTABLE TRIALS INVOLVING PROBATE AND TRUST DISPUTES ON BEHALF OF PRIVATE PROFESSIONAL FIDUCIARIES. HE ALSO COUNSELS' CLIENTS IN ALL PHASES OF TRUST ADMINISTRATION, CONSERVATORSHIPS, GUARDIANSHIPS AND PROBATE MATTERS.

ADDITIONALLY, MR. KIM SERVES FROM TIME TO TIME ON HIGHLY CONTESTED CONSERVATORSHIP MATTERS AS COURT APPOINTED COUNSEL AND GUARDIAN AD LITEM FOR TRUST MATTERS.

WRIGHT KIM DOUGLAS

BIOS

TAMRA OTTEN

WRIGHT KIM DOUGLAS ALC- PARTNER

130 SOUTH JACKSON STREET, GLENDALE, CA 91205

626-356-3900

TAMRA@WKDLEGAL.COM

TAMRA OTTEN, PARTNER AT WRIGHT KIM DOUGLAS FOCUSES ON PROBATE, TRUSTS AND CONSERVATORSHIPS. SHE HANDLES BOTH LITIGATION AND ADMINISTRATION, INCLUDING SPECIAL NEEDS TRUSTS.

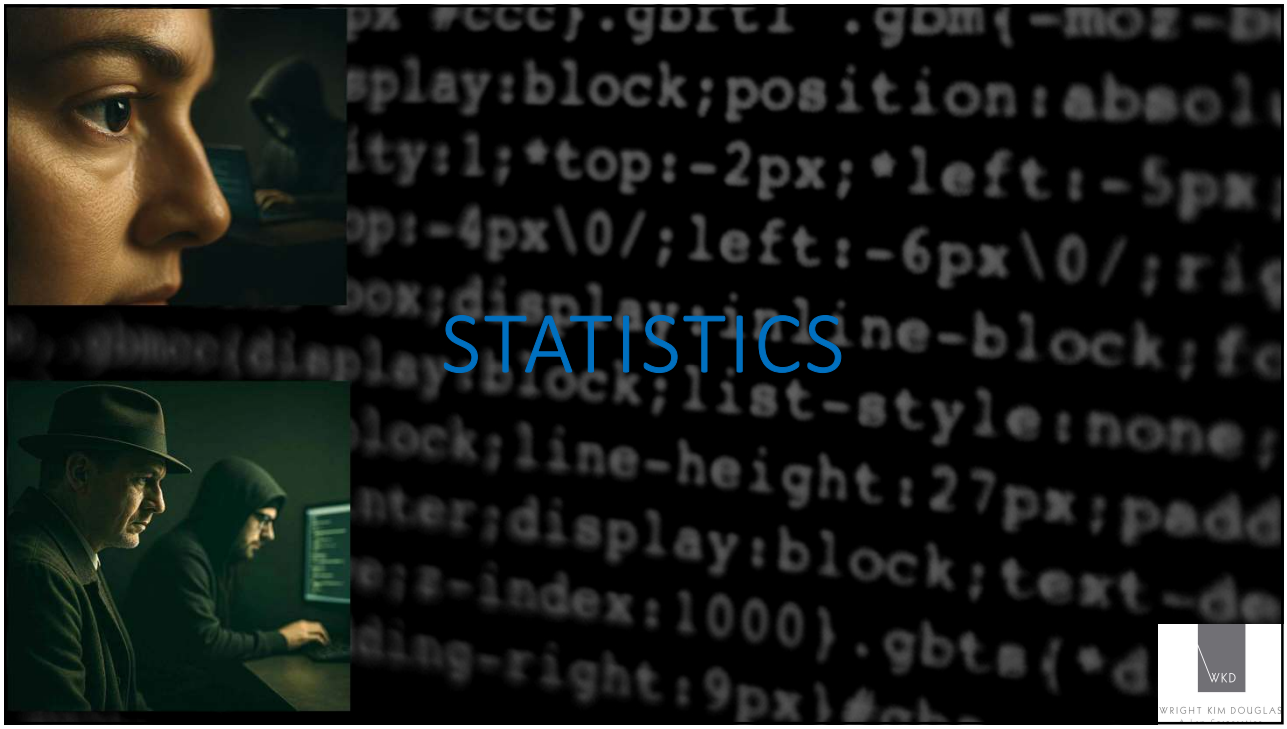
MS. OTTEN REPRESENTS NUMEROUS PRIVATE PROFESSIONAL FIDUCIARIES IN CONTESTED AND UNCONTESTED MATTERS; INCLUDING BENCH TRIALS, EVIDENTIARY HEARINGS AND CONTESTED PETITIONS. SHE SERVES AS COURT APPOINTED COUNSEL FOR VARIOUS MATTERS FROM THE PANEL.

WRIGHT KIM DOUGLAS

TOPICS

- STATISTICS
- IDENTIFYING CYBER SCAMS
- AFTER SCAM IS COMMITTED WHAT ARE THE OPTIONS?
- WHO IS RESPONSIBLE WHEN FUNDS ARE COMPROMISED?
- BEST PRACTICES TO PREVENT CYBERFRAUD

WRIGHT KIM DOUGLAS



STATISTICS

FBI'S INTERNET CRIME REPORT 2024:

859,532	Total Complaints in 2024
$16.6 Billion	Losses in 2024
33%	Increase in Losses from 2023
256,256	Complaints with Actual Loss
$19,372	Average Loss

STATISTICS

FBI'S INTERNET CRIME REPORT 2024:

2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441
*Descriptor***			
Cryptocurrency	149,686		

WRIGHT KIM DOUGLAS

STATISTICS

FBI'S INTERNET CRIME REPORT 2024:

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss	Crime Type	Loss
Investment	$6,570,639,864	Extortion	$143,185,736
Business Email Compromise	$2,770,151,146	Lottery/Sweepstakes/ Inheritance	$102,212,250
Tech Support	$1,464,755,976	Advanced Fee	$102,074,512
Personal Data Breach	$1,453,296,303	Phishing/Spoofing	$70,013,036
Non-Payment/Non-Delivery	$785,436,888	SIM Swap	$25,983,946
Confidence/Romance	$672,009,052	Overpayment	$21,452,521
Government Impersonation	$405,624,084	Ransomware *	$12,473,156
Data Breach	$364,855,818	Harassment/Stalking	$10,611,223
Other	$280,278,325	Botnet	$8,860,202
Employment	$264,223,271	IPR/Copyright and Counterfeit	$8,715,512
Credit Card/Check Fraud	$199,889,841	Threats of Violence	$1,842,186
Identity Theft	$174,354,745	Malware	$1,365,945
Real Estate	$173,586,820	Crimes Against Children	$519,424
*Descriptor***			
Cryptocurrency	$9,322,335,911		

WRIGHT KIM DOUGLAS

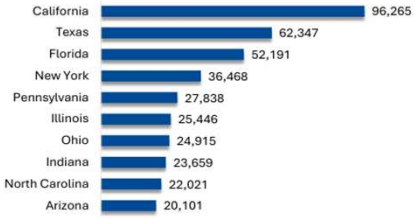
STATISTICS

FBI'S INTERNET CRIME REPORT 2024:

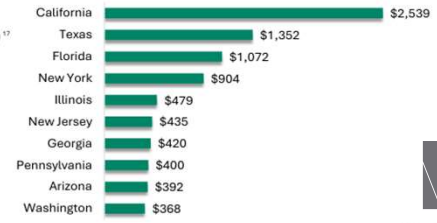
TOP REPORTED TRANSACTION TYPES[15]

Transaction information provided in IC3 complaints helps FBI understand how victims are losing funds to fraud and assists the Recovery Asset Team Financial Fraud Kill Chain process when complaints are filed as quickly as possible. This chart identifies the top ways complainants reported financial loss in fraud.

TOP 10 STATES BY NUMBER OF COMPLAINTS[16]

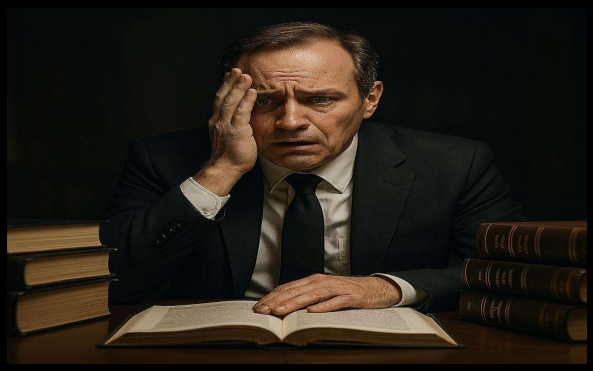


TOP 10 STATES BY LOSS (IN MILLIONS)[17]



WKD
WRIGHT KIM DOUGLAS

IDENTIFY CYBERSCAMS



WKD
WRIGHT KIM DOUGLAS

BUSINESS EMAIL COMPROMISE

(UNAUTHORIZED CHANGES TO WIRE INSTRUCTIONS ARE A GROWING THREAT)

SCAMMERS GAIN ACCESS TO EMAILED WIRING INSTRUCTIONS AND REPLACE THEM WITH FRAUDULENT WIRE INSTRUCTIONS.

WKD

WRIGHT KIM DOUGLAS

HOW DOES BUSINESS EMAIL COMPROMISE WORK?

1. OBTAIN A LEGITIMATE EMAIL DOMAIN (E.G. @BUSINESS.COM).
2. THE SCAMMER CREATES A SIMILAR DOMAIN NAME, FOR INSTANCE - @BUSLNESS.COM.
3. USE LEGITIMATE COMPANY INFORMATION TO CREATE AN IMPOSTER EMAIL ADDRESS – OWNER@BUSLNESS.COM.
4. DIFFERENCE BETWEEN: OWNER@BUSLNESS.COM AND OWNER@BUSINESS.COM.
5. SCAMMER USES THIS FRAUDULENT EMAIL TO DIRECT OTHERS IN THE BUSINESS TO TRANSFER FUNDS TO SCAMMERS ACCOUNT.

WKD

WRIGHT KIM DOUGLAS

ACCOUNT TAKEOVER

- ACCOUNT TAKEOVER OCCURS WHEN THE SCAMMER TAKES CONTROL OF THE ACTUAL BUSINESS ACCOUNT.
- WHEN THE SCAMMER TAKES OVER, THEY INSTRUCT CLIENTS AND/OR BANKS TO SEND PAYMENTS TO AN UNAUTHORIZED ACCOUNT.

WRIGHT KIM DOUGLAS

ATTORNEY TRUST ACCOUNT SCAMS

- INVOLVES SCAMMER WHO CONTACTS ATTORNEY AS A PROSPECTIVE CLIENT.
- RETAINER AGREEMENT IS SIGNED.
- SCAMMER TELLS ATTORNEY THAT THE OTHER SIDE IS SETTLING AND THAT THE ATTORNEY SHOULD RECEIVE A SETTLEMENT CHECK.
- ATTORNEY RECEIVES THE SETTLEMENT CHECK.
- SCAMMER CONTACTS ATTORNEY WITH URGENT REQUEST TO SEND FUNDS.
- ATTORNEY WIRES FUNDS TO SCAMMER BEFORE REALIZING CHECK IS FAKE.

WRIGHT KIM DOUGLAS

RANSOMWARE

RANSOMWARE IS A TYPE OF MALICIOUS SOFTWARE—OR MALWARE—THAT PREVENTS YOU FROM ACCESSING YOUR COMPUTER FILES, SYSTEMS, OR NETWORKS AND DEMANDS YOU PAY A RANSOM FOR THEIR RETURN.

HOW IT WORKS:

OPEN AN EMAIL ATTACHMENT

CLICK AN AD/LINK

VISIT A WEBSITE

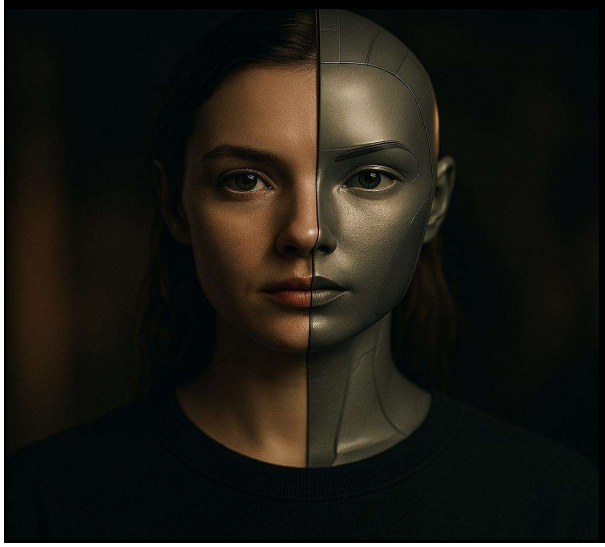
WRIGHT KIM DOUGLAS

RANSOMWARE

- You may not know that malware is on your computer until the scammer locks you out.
- The scammer will demand a ransom payment.

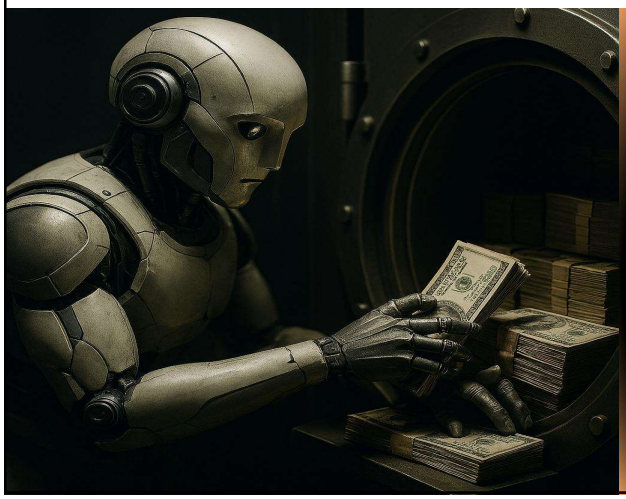
WRIGHT KIM DOUGLAS

DEEP FAKE SCAMS



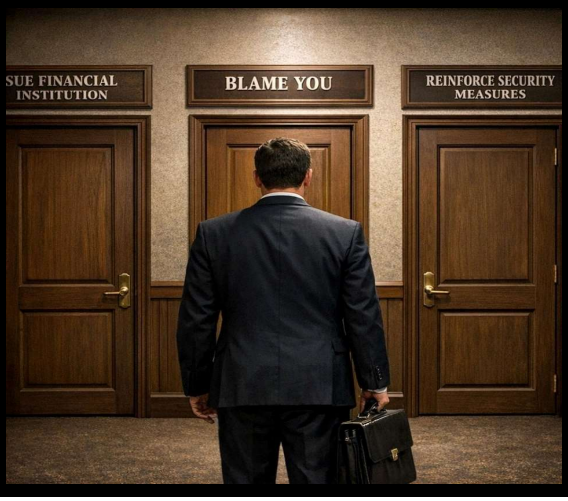
IMPOSTER SCAMS ON THE RISE IN THE AGE OF ARTIFICIAL INTELLIGENCE. SCAMMERS ARE USING DEEP FAKES, OR AI THAT LOOKS LIKE AND SOUNDS LIKE SOMEONE YOU KNOW.

DEEP FAKE SCAMS



A FINANCE WORKER TRANSFERRED $25 MILLION TO A SCAMMER WHO THEY THOUGHT WAS THE CFO. THE SCAMMER CREATED A VIDEO USED IN A CONFERENCE THAT LOOKED AND SOUNDED LIKE HIS COWORKERS BY PULLING AVAILABLE VIDEOS ONLINE OF THE CFO.

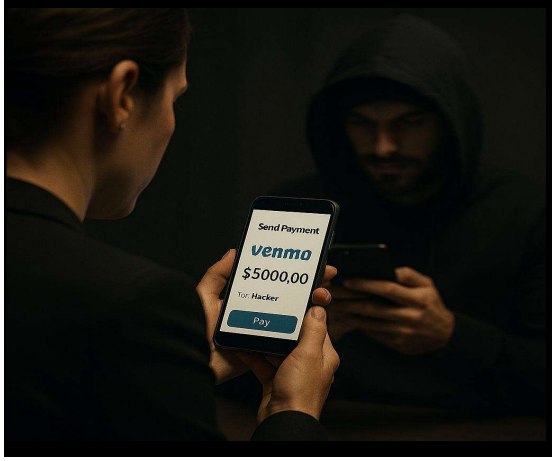
AFTER SCAM IS COMMITTED WHAT ARE THE OPTIONS?



CONTACT BANK IMMEDIATELY

- USE A PHONE NUMBER YOU TRUST (DON'T USE THE NUMBER IN THE EMAIL ADDRESS).
- DON'T WAIT, THE QUICKER YOU ACT, THE BETTER CHANCE THAT THE BANK CAN FREEZE/REVERSE THE TRANSFER.

DID YOU SEND MONEY THROUGH A MONEY TRANSFER APP?



REPORT THE FRAUDULENT TRANSACTION TO THE COMPANY BEHIND THE MONEY TRANSFER APP AND ASK THEM TO REVERSE THE PAYMENT. IF YOU LINKED THE APP TO A CREDIT CARD OR DEBIT CARD, REPORT THE FRAUD TO YOUR CREDIT CARD COMPANY OR BANK. ASK THEM TO REVERSE THE CHARGE.

WKD
WRIGHT KIM DOUGLAS

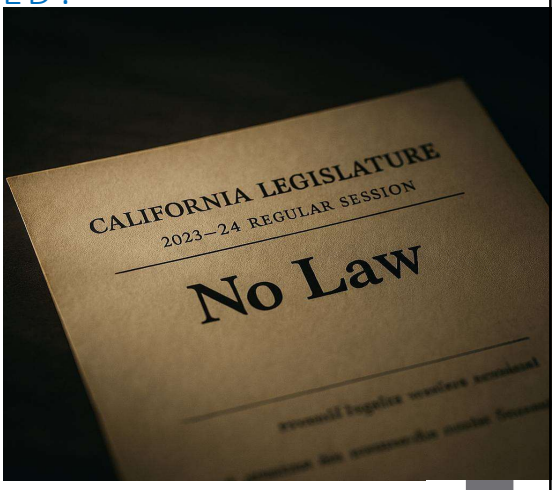
REPORT SCAM

REPORT THE SCAM TO THE FEDERAL TRADE COMMISSION, THE FBI'S INTERNET CRIME COMPLAINT CENTER (IC3), AND LOCAL LAW ENFORCEMENT.

IF YOU MAILED A CHECK, REPORT SCAM TO USPS AND SEE IF THEY CAN HOLD THE CHECK.

WKD
WRIGHT KIM DOUGLAS

WHO IS RESPONSIBLE WHEN FUNDS ARE COMPROMISED?



BANK VS CUSTOMER
UCC ARTICLE 4A

UCC § 4A-202(b): If bank and customer agree payments will be verified pursuant to a commercially reasonable security procedure and the payment and the bank proves payment order is accepted in good faith, customer bears the loss – even if transfer was unauthorized.

- UCC § 4A-203: If the payment order is unauthorized and not properly verified, the bank cannot charge the customer's account.
- UCC § 4A-204: If receiving bank accepts payment order which is not authorized and not effective or not enforceable, the bank shall refund the payment order and shall pay interest.

BANK VS CUSTOMER
UCC ARTICLE 4A

- Security Procedure - "means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure."(UCC Section 4A-201).
- Good Faith - "except as otherwise provided in Article 5, means honesty in fact and the observance of reasonable commercial standards of fair dealing." (UCC Section 1-201(20)).

THOMAS V. CORBYN RESTAURANT DEVELOPMENT CORP. 111 CAL.APP.5TH 439 (MAY 27, 2025)

- Case of first impression in California.
- Issue: “Which party bears the risk of loss when an imposter causes one party to a settlement to wire settlement proceeds to the imposter instead of the other settling party?”
- Facts: “After plaintiff and defendants settled a personal injury lawsuit for $475,000, an unknown third party purporting to be plaintiff's counsel sent “spoofed” emails to defendants' counsel providing fraudulent wire instructions for the settlement proceeds. Defendants' counsel wired the settlement proceeds to the fraudulent account and the third party absconded with the funds. Once the fraud was discovered, plaintiff asked for the settlement money, but defendants refused to pay. Plaintiff then applied ex parte to enforce the settlement agreement.”

THOMAS V. CORBYN RESTAURANT DEVELOPMENT CORP.

Holding: "The risk of loss from an imposter's fraudulent diversion of a wire transfer shall be borne by the party in the best position to prevent the fraud. In making this factual determination, trial courts must consider the extent to which each party exercised ordinary care with respect to preventing the fraud and may apportion the loss accordingly. (See Beau Townsend Ford, supra, 759 Fed.Appx. at p. 359.) In doing so, courts must consider the totality of the circumstances."

THOMAS V. CORBYN RESTAURANT DEVELOPMENT CORP.

Court found the following red flags:

- First: "the imposter's 'wiring instructions conflicted with the payment procedure established by the parties' written Settlement Agreement and Release.'"
- Second: "substantial evidence supports the trial court's finding that if a law firm's primary phone number was 'inoperable,' that was another warning sign to Defendants' counsel."
- Third: "the imposter's use of a spoofed email address for Mattson, which differed in both her name (it omitted the letter "c") and the domain name (it added the letter "r"), was yet another red flag to Defendants' counsel."
- Fourth: "the fact the imposter carelessly sent two identical requests for wire instructions within a matter of minutes is akin to typographical errors that courts have deemed significant in shifting the risk of loss."

"These numerous red flags, backed by substantial evidence in the record, support the trial court's factual finding that Defendants were in the best position to prevent the fraud."

BEST PRACTICES TO PREVENT CYBERFRAUD

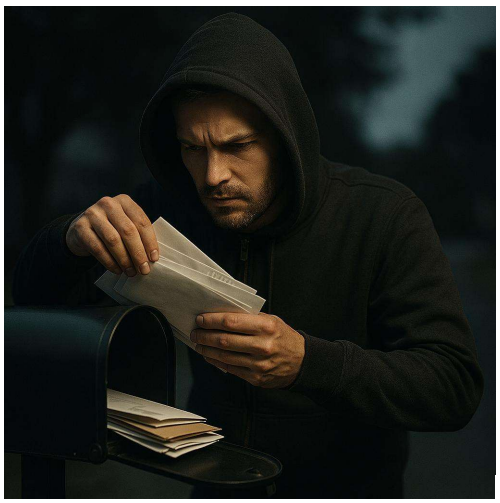
-CHECKS AS ALTERNATIVES?
- INDEPENDENT CONFIRMATION OF WIRE INSTRUCTIONS
- FOR ATTORNEYS, WAIT FOR FUNDS TO CLEAR
-CYBER POLICIES
-CYBER INSURANCE

WRIGHT KIM DOUGLAS

WHAT ABOUT CHECKS AS AN ALTERNATIVE?

CHECK FRAUD IS STILL PREVALENT. THE COMMON CHECK FRAUD OCCURS BY:

SCAMMERS INTERCEPTING A CHECK



WRIGHT KIM DOUGLAS

SCAMMERS INTERCEPTION CHECKS

- Scammers are intercepting checks by vandalizing/tampering with legitimate mailboxes.
- Safer to drop off mail directly at the post office.

But wait…

METRO DETROIT USPS EMPLOYEES CHARGED IN $63M CHECK FRAUD SCHEME

$63 million stolen check scheme by stealing checks from the mail and selling the checks online. Four people were charged, two were U.S.P.S. employees.

BEST PRACTICES FOR WIRE INSTRUCTIONS

- If you receive an email containing Wire Transfer instructions, **DO NOT RESPOND TO THE EMAIL!**
- Call the recipient using previously known phone number and **NOT** a number provided in the email, to verify the info prior to sending funds.
- If you receive new wiring instructions, please notify the recipient immediately.
- Also check for misspelled words and email addresses.

WKD
WRIGHT KIM DOUGLAS

BEST PRACTICES FOR ATTORNEYS

- State Bar issued a fraud alert as there is an increase in scams targeting lawyers.
- Be careful when you receive a check from someone you do not know.
- Wait for funds to clear before issuing payment to client.

WKD
WRIGHT KIM DOUGLAS

POLICIES

DO YOU HAVE POLICIES IN PLACE FOR SENDING FUNDS?

- IF NOT, CREATE ONE!
- ENSURE POLICY IS CONSISTENTLY USED BY EVERYONE.
- POLICY SHOULD INCLUDE VERIFYING FUNDS THROUGH TRUSTED CONTACT (CALLING RECIPIENT FROM A TRUSTED NUMBER, NOT NUMBER IN EMAIL).
- CONDUCT REGULAR TRAINING ON CYBER SECURITY.

WRIGHT KIM DOUGLAS

CYBER INSURANCE

- CYBER INSURANCE IS BECOMING MORE POPULAR.
- MAY COVER EXPENSES YOU INCUR AND EXPENSES FROM CLAIMS/LAWSUITS.
- CHECK WITH YOUR E/O POLICY IF IT'S AVAILBLE TO ADD.
- POLICY MAY REQUIRE:
  - Strict cybersecurity controls, i.e., multi-factor authentication
  - Maintain good data backups
  - Identify access management (only certain users have access)
  - Enforce data classification

WRIGHT KIM DOUGLAS

ERNST AND HAAS MANAGEMENT COMPANY, INC. V. HISCOX, INC.

23 F.4TH 1195 (9TH CIRC. 2022)

- Issue: whether commercial crime insurance policy covers computer fraud when scammer instructs employee to send funds via a wire transfer to scammers account.
- Employee received emails from what she thought was her boss to pay invoices via a wire transfer. First, she paid $50,000. Then she received instructions for $150,000 and $470,000. She transferred $150,000 and then became suspicious and contacted her real boss. Her real boss informed her that he did not instruct her to make these payments.
- The company's policy included coverage for computer fraud and funds transfer fraud. Her boss submitted a claim after trying to get the funds back from the bank. The carrier denied the claim.
- The District Court agreed with the carrier and "found that Ernst's alleged loss did not result directly from fraudulent emails instructing an Ernst employee to transfer funds to a deceptive third party. And because the court reasoned that both the computer fraud and funds transfer fraud provisions required the loss to result directly from the fraudulent emails, it found neither provision applied to Ernst."

ERNST AND HAAS MANAGEMENT COMPANY, INC. V. HISCOX, INC. CONTINUED

- "The district court erred by limiting its interpretation of a loss "result[ing] directly from use of a computer to fraudulently cause transfer" to only a loss resulting directly from unauthorized use of Ernst's computers or hacking. The district court's interpretation that Ernst's alleged loss did not result "immediately" and "directly" from computer fraud because Ernst, through Allen, "authorized its bank to initiate the wire transfers from its account, albeit through an unwitting employee," eliminates the possibility of coverage whenever an employee is defrauded into taking an action. By relying on Pestmaster to reach this conclusion, the district court endorsed a faulty circular premise—that Allen "authorized" a transfer of $200,000, curing any prior fraud, when she initiated a transfer of $200,000 based on fraud. That reasoning—that this fraud became "authorized" precisely when it succeeded—cannot be the correct reading of the contract."

ERNST AND HAAS MANAGEMENT COMPANY, INC. V. HISCOX, INC. CONTINUED

- "Here, the computer fraud provision provides that Ernst's loss must "result directly" from the fraud. In other words, like ATC, Ernst must suffer a direct loss. And like ATC, Ernst immediately lost its funds when those funds were transferred to Zang as directed by the fraudulent email. There was no intervening event—Allen acting pursuant to the fraudulent instruction "directly" caused the loss of the funds. Thus, taking the pleaded facts as true, Ernst suffered a loss resulting "directly" from the fraud, arguably entitling Ernst to coverage under the policy. So here, as in American Tooling, we cannot conclude that Ernst's alleged immediate loss of funds based on the fraudulent email was not "direct." Id. at 461. Accordingly, we reverse the district court and remand with instructions to reconsider the case with the recognition that, under the facts as alleged by Ernst, Ernst's loss falls within the computer fraud provision of the 2012 policy."

TAKE AWAYS

- When sending a wire transfer, call and confirm the instructions using a known/trusted phone number.
- Establish internal polices for sending funds.
- Consider cyber insurance.


WKD
WRIGHT KIM DOUGLAS
A Law Corporation
THANK YOU
David Kim
Wright Kim Douglas ALC
Managing Partner
130 South Jackson Street
Glendale, CA 91205
818-689-0926
david@wkdlegal.com
Tamra Otten
Wright Kim Douglas ALC
Partner
130 South Jackson Street
Glendale, CA 91205
626-356-3900
tamra@wkdlegal.com