K2's Ripped From The Headlines:

Lessons From Interesting Tech Crimes

Course Description

This session dives into real-world cases of financial fraud, cybercrime, and ethics breaches that captivated the business and accounting world. This session analyzes how these crimes unfolded, the warning signs that were missed, and the internal control and technology failures that enabled them. Participants will explore modern threats, including AI-enabled deception, and learn practical steps to strengthen fraud prevention, data protection, and governance. From shocking embezzlements to headline-making cyberattacks, this course turns true stories into powerful lessons for today's accounting and finance professionals.

Learning Objectives

- Analyze real-world financial crime cases to identify root causes and control failures
- Evaluate methods for detecting and preventing fraud and data breaches in accounting environments
- Assess the emerging risks posed by AI-enabled fraud and misuse of automation
- Determine practical steps to enhance internal controls and ethical culture within organizations

K2's Ripped From The Headlines:

Lessons From Interesting Tech Crimes

- **Profile of the Fraudsters**
- **The Insider Threat**: When the Spy/Thief is in the Next Cubicle
- **Electronic Payment Risks**
- **Cybercrimes, Breaches, and Rapid Changes to the Security Landscape**
- **AI-Enabled Fraud:** Faster, Cheaper, and More Convincing
- **Turning Headlines Into Prevention Strategies**

About This Session

- Fraud is not getting more sophisticated — *it's getting more human*
- Internal controls didn't fail because people were dumb — they failed because assumptions were wrong
- Today's crimes blend **trust, technology, and speed**, and accountants sit right in the blast radius
- ALSO:
  - This is not a true-crime podcast
  - This *is* a control-failure autopsy lab
  - Every story answers one question: *"How could this have been stopped?"*

"Global Profiles of the Fraudster" – KPMG, 2025

"Occupational Fraud 2024: A Report to the Nations" – Association of Certified Fraud Examiners, 2024

PROFILE OF THE FRAUDSTERS

Profile Of A Fraudster

The most dangerous assumption is that fraudsters are easy to spot.

ACFE and KPMG suggest otherwise.

ACFE Profile Highlights

1,921
cases analyzed in ACFE's 2024 Report to the Nations

12
months median duration of a fraud scheme

$145K
median loss per case

$3.1B+
combined losses across reported cases

ACFE also notes that **most fraudsters were employees or managers**, while **owners/executives caused far larger median losses**, making authority level a severity issue even when not the most frequent category.

KPMG Profile Highlights

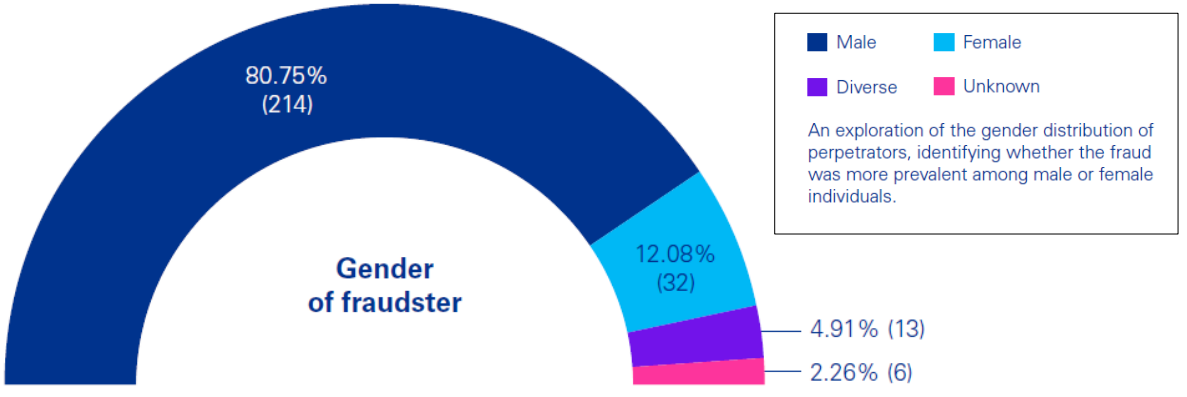
81%
KPMG's 2025 global study reported that 81% of fraudsters were men.

36–55
The typical age band was 36 to 55, not early-career entry level.

6+ years
Fraudsters often had more than six years with the organization and worked in operations, finance, or general management.

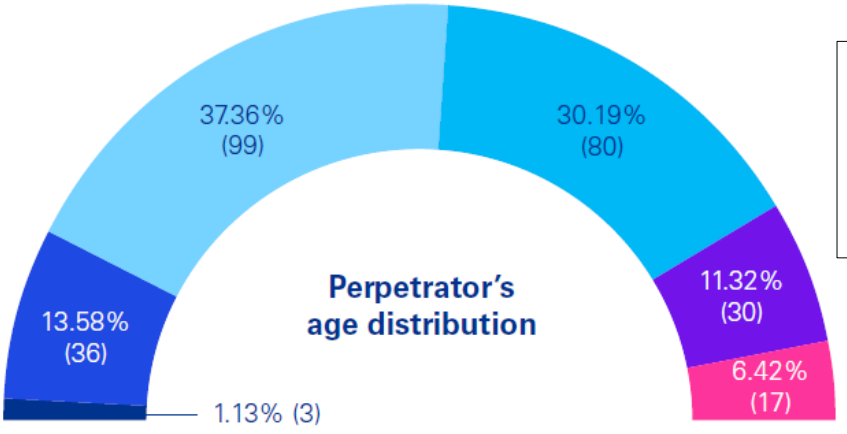
KPMG also found 65% of frauds lasted between one and five years, showing how trusted insiders can avoid detection for long periods when controls are weak or overridden.

KPMG's Global Profiles Of The Fraudster



Source: Global profiles of the fraudster, 2025

KPMG's Global Profiles Of The Fraudster

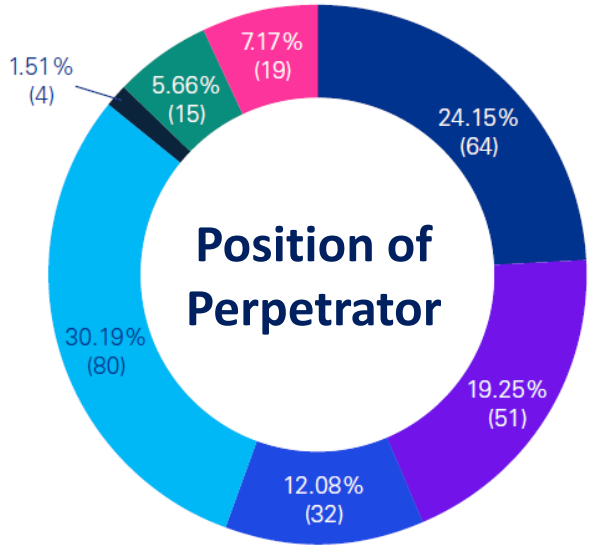


18–25 years old
26–35 years old
36–45 years old
46–55 years old
Older than 55 years
Unknown

A breakdown of the age groups of individuals who committed the fraud, providing insights into how age may correlate with fraudulent behavior.

Source: Global profiles of the fraudster, 2025

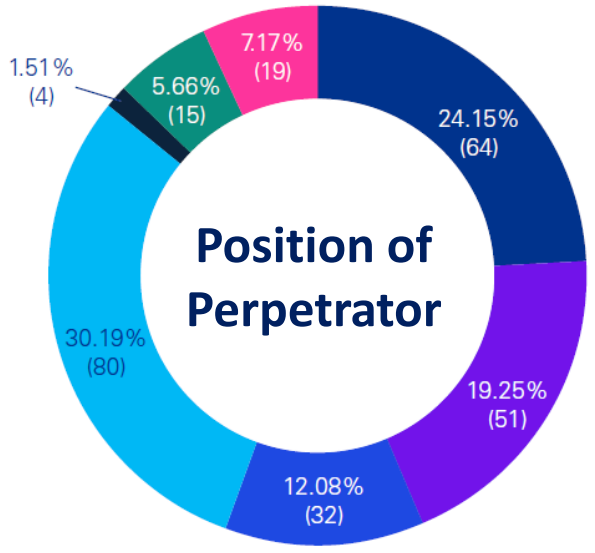
KPMG's Global Profiles Of The Fraudster



Staff member
Executive director
Executive corporate officer
Management (no executive capacity)
Non-executive director
Owner/shareholder
Others

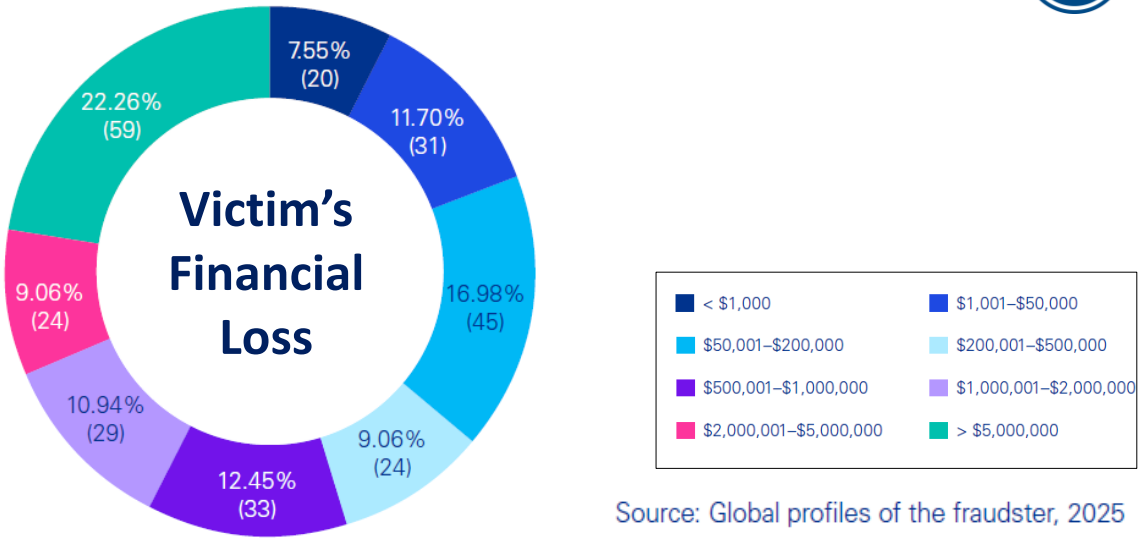
Source: Global profiles of the fraudster, 2025

KPMG's Global Profiles Of The Fraudster



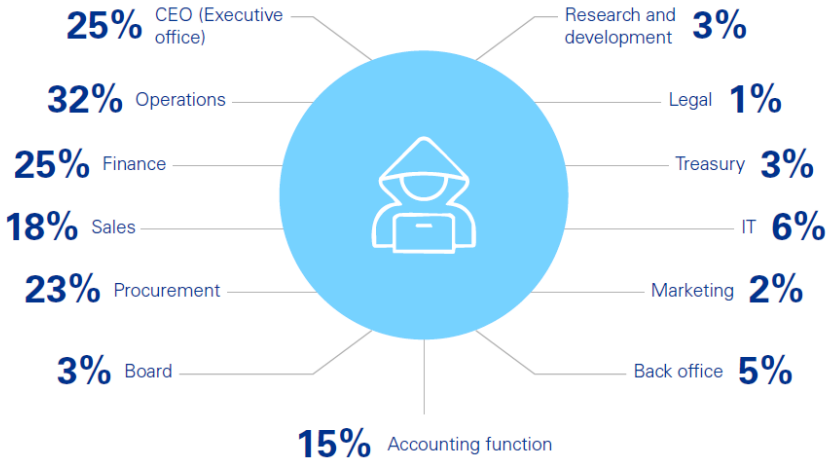
Source: Global profiles of the fraudster, 2025

KPMG's Global Profiles Of The Fraudster



Source: Global profiles of the fraudster, 2025

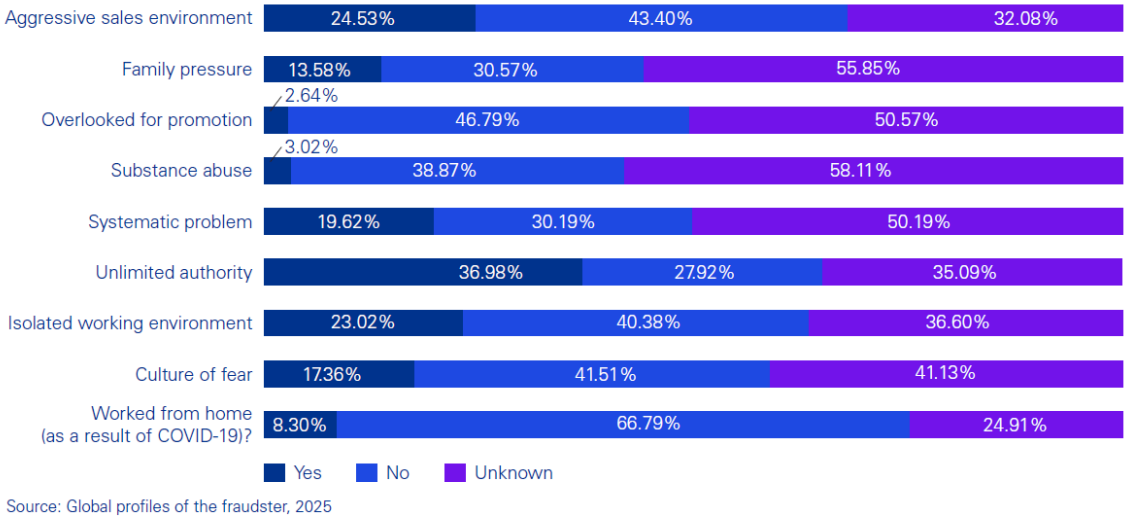
KPMG's Global Profiles Of The Fraudster



Department Where Fraud Occurred

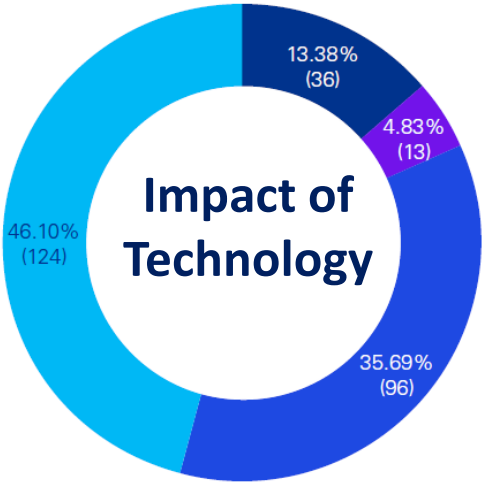
Source: Global profiles of the fraudster, 2025

KPMG's Global Profiles Of The Fraudster: Environmental Factors



Source: Global profiles of the fraudster, 2025

KPMG's Global Profiles Of The Fraudster



- Yes, the fraud could not have been perpetrated without using technology
- Yes, to a large degree technology was used to enable the fraud
- Somewhat, but the fraud could likely have occurred without technology
- Technology was not used at all to perpetrate the fraud

Source: Global profiles of the fraudster, 2025

What The Profile Means

Do Not Over-Focus on Junior Staff

Both ACFE and KPMG suggest mature, trusted, longer-tenured people create significant risk, especially when they hold authority or understand process workarounds.

Collusion Raises Losses

Fraud becomes harder to detect when multiple people participate or when an insider works with an outside party such as a vendor, family member, or competitor.

Behavioral Clues Matter

Lifestyle changes, defensiveness, control issues, financial stress, or unusual closeness with customers and vendors warrant attention without assuming guilt.

Whistleblower Channels Work

Both studies underscore the value of tips and reporting channels because formal audit procedures alone often detect fraud too late.

"The Rippling/Deel corporate spying scandal may have taken another wild turn" – TechCrunch, 1/23/2026

THE INSIDER THREAT: WHEN THE SPY/THIEF IS IN THE NEXT CUBICLE

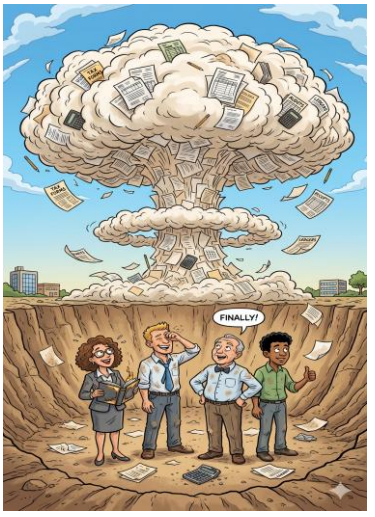
Insider Threat Allegations

Industrial Espionage

Bank ACH Theft

Accountants Are At Ground Zero For Internal Fraud

- CFO's (and some Controllers) are typically the "process owner" for most if not all treasury and accounting functions
- These leaders also have key roles in their internal control
- Industrial espionage is often accompanied by financial difficulty and can be simply a way that a perpetrator monetizes the trusted access they have to fund their compulsive need for cash
- Small internal thefts by people with access to sensitive data should lead to enhanced scrutiny of sensitive data access



The Threat Of Industrial Espionage

- Insider fraud is not only embezzlement. It can also be strategic theft of data, plans, pricing, and customer intelligence.

This image is AI-generated content

Industrial Espionage Risk Map

Target Assets

Pricing models, pipeline data, product roadmaps, source code, customer lists, and contract terms.

Typical Insiders

Employees, contractors, third-party admins, sales reps, and former staff retaining access.

Common Failures

Excessive privileges, poor logging, delayed offboarding, unsupervised exports, and weak device governance.

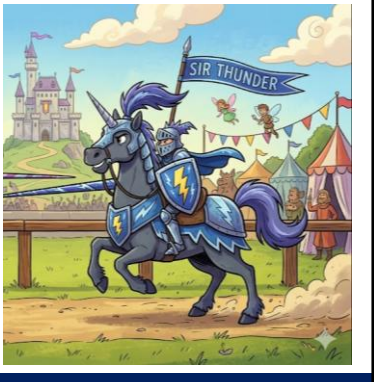
For CPAs, the accounting impact is broader than legal fees: misstatement risk, valuation impact, business interruption, cyber insurance friction, and internal-control deficiencies can all follow an insider data-theft event.

Alleged Espionage: Rippling v. Deel

- Payroll and HR startups Ripping and Deel are referred to as “Unicorns” – venture backed companies with valuations over $1B USD
  - Deel had a $17.3B valuation in October 2025
  - Rippling had a $16.8B valuation in May 2025
- An employee of Rippling interviewed for a job at competitor Deel and was not selected – but during the interview process, this Rippling employee connected on LinkedIn with a senior executive at Deel
- This Rippling employee claims that this senior executive recruited him and paid him to provide Deel with confidential information about sales transactions from Rippling’s internal systems - Slack messaging system, Salesforce CRM, and many others
- Litigation is unresolved and is ongoing

RIPPLING

deel.



Rippling's Allegations Against Deel

- **Alleged Racketeering Enterprise:** Led by Alex and Philippe Bouaziz, the enterprise included Deel executives, outside collaborators, and spies embedded in competitors (notably Keith O'Brien at Rippling).
- **Methods:**
  - Recruitment of spies via disappearing Telegram messages.
  - Payments routed through family members and cryptocurrency to obscure the money trail.
  - Use of codewords and cover-ups (e.g., destruction of evidence, coaching witnesses to lie).
- **Stolen Information:** Product roadmaps, pricing models, sales forecasts, customer lists, recruitment targets, and go-to-market strategies.
- **Weaponization:** Deel allegedly used stolen data to undercut Rippling in sales, retain customers, poach personnel, accelerate product development, and manipulate public narratives.
- **Evidence:** Confession by Keith O'Brien, forensic analysis, honeypot tests, WhatsApp logs, payment records, and court orders

TIMELINE OF EVENTS REGARDING DEEL'S ALLEGED CORPORATE ESPIONAGE SCHEME AND SUBSEQUENT LAWSUIT

March 2024
- O'Brien interviews with Deel for a job
- Deel CEO Alex Bouaziz contacts O'Brien via LinkedIn

August/September 2024
Deel finalizes spying arrangement including payments in exchange for Rippling trade secrets

November 2024 - March 2025
O'Brien begins getting paid (initially on Revolut by Alba Basha) and searches over 6,000 times through Rippling's Slack channels, downloads 1,300 documents

February 18, 2025
Rippling becomes aware of possible spying activity after a message from a reporter at The Information

March 4, 2025
Deel leadership instructs O'Brien to search for the "#d-defectors" Slack channel, which was created by Rippling and sent to Deel's CFO and lawyers, and after realizing it might be a trap, and when told O'Brien had already ran the search, responded "oh shit"

March 12, 2025
Rippling obtains an order from the High Court in Ireland to seize O'Brien's phone

March 14, 2025
- Independent Irish solicitor confronts O'Brien
- O'Brien speaks with Deel and is directed to buy a burner phone and offers to move O'Brien and his family to Dubai

March 16, 2025
At direction of Deel's lawyer Asif Malik, O'Brien smashes his old phone with an axe and puts it down the drain at his mother in law's house

March 17, 2025
Rippling files lawsuit against Deel alleging RICO violations and misappropriation of trade secrets

March 18, 2025
At the direction of Deel, O'Brien makes a false report to the Central Bank of Ireland about "Russian payments" at Rippling

March 19, 2025
O'Brien appears in Court and admits he "destroyed" his phone. The Court tells him to get counsel and that this is "very serious."

March 21, 2025
Deel connects O'Brien with its legal counsel

March 25, 2025
O'Brien has his last contact with Malik/Deel

March 26, 2025
O'Brien agrees to cooperate with Rippling

April 2, 2025
Keith O'Brien's sworn affidavit is filed in court and Rippling adds Deel CEO Alex Bouaziz, Asif Malik, David Mieli and Deel Inc. as defendants

April 3 & 4, 2025
- Deel's head of communications Elisabeth Diana resigns
- Paul Weiss and Elsberg resign from representing Deel

April 10, 2025
English bailiffs cannot locate Deel's in-house lawyer Asif Malik, and Rippling is told he moved to Dubai

April 13, 2025
French bailiffs cannot locate Deel CEO Alex Bouaziz to serve him with legal papers

April 15, 2025
TechCrunch reports Deel CEO Alex Bouaziz has relocated to Dubai, noting it is a "safe haven for extradition"

April 22, 2025
Toku files lawsuit against one of Deel's partners (LiquiFi), alleging the company hired Toku's former general counsel and utilized his misappropriated trade secrets

April 25, 2025
Deel files countersuit against Rippling but fails to deny the allegations that its CEO recruited and managed a paid spy or serve Rippling

April 28, 2025
Solicitors accept service on behalf of Deel executives, including Deel CEO Alex Bouaziz, who are unable to be located and seemingly in Dubai

June 3, 2025
Deel files an amended complaint against Rippling that fails to deny the allegations that its CEO recruited and managed a paid spy and backtracks from some of its original claims

June 5, 2025
Rippling shares new information about Bouaziz Racketeering Enterprise with court and files amended complaint

Source: *Rippling's timeline of allegations in USDC N.CA case 3:25-cv-02576-CRB, document 57-2, filed 6/5/2025*

Deel's Counterclaims Against Rippling

- **RICO Violations:** Rippling, led by CEO Parker Conrad, allegedly operates a criminal enterprise to harm Deel, including bribery, wire fraud, and witness tampering.
- **Computer Fraud & Abuse Act (CFAA):** Rippling allegedly fraudulently accessed Deel's platform using fake accounts to steal proprietary information, contracts, and pricing documents.
- **Trademark & Cybersquatting:** Rippling allegedly used a deceptive domain (<deal.com>) to redirect users to its own site and abused Deel's trademarks.
- **False Advertising:** Rippling allegedly disseminated misleading statements about Deel's products and compliance.

Alleged Espionage: Rippling v. Deel

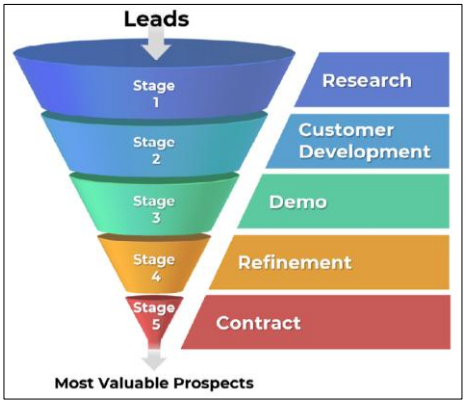
- Rippling alleged Deel cultivated a Rippling employee to conduct thousands of searches and pass confidential intelligence to Deel
- A federal judge later allowed civil RICO and trade-secret claims against Deel and certain executives to move forward toward trial in California
- A January news story reported that the US Department of Justice has opened a criminal investigation into these matters
- In March 2026 reporting, Deel acknowledged a roughly $6,000 payment to the employee but disputed Rippling's interpretation of that payment

INSIGHTS AND OBSERVATIONS

- Sales, HR, and customer data in internal messaging systems like **Teams, Slack**, and **CRM** tools like **Salesforce** can be as strategically sensitive as financial statements – and much more damaging to the wrong people
- **"Need to know" access matters** even inside high-growth firms with open information cultures
- Small payments, side-channel messaging, and unusual searches may be signs of a larger scheme

Rippling's Sales Systems

- Leads are generated with targeted ads, LinkedIn posts, Google AdSense, and social media
- A single lead could be the result of thousands of dollars of advertising
- Sales professionals use many systems to shepherd leads through the sales process and turn them into customers
- As prospects are moved further into the sales funnel, they are increasingly valuable to the company



Rippling's Sales Process, as presented in their complaint in San Francisco US District Court case 3:25-cv-02576-CRB

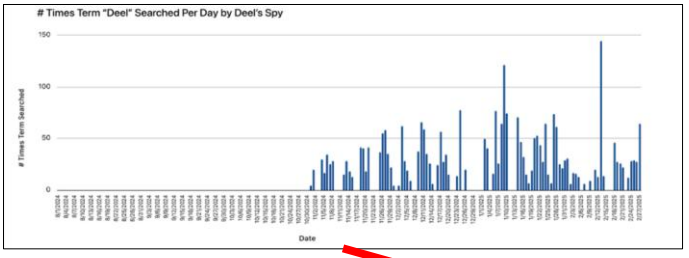
Rippling's Sales Systems

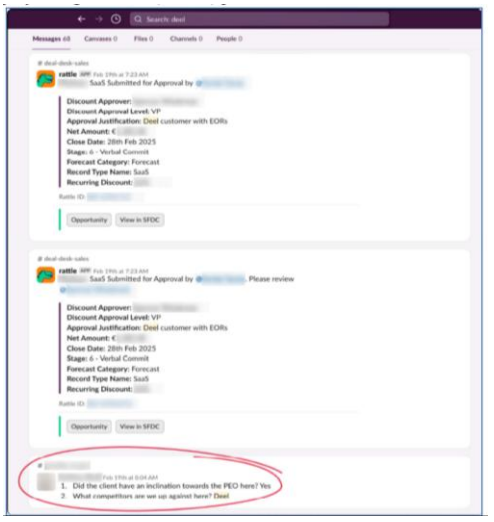
Tools and intellectual property to be protected include:

- **Salesforce** Customer Relationship Management system, which automates routine correspondence and workflow
  - Routine e-mail messages, letters, and agreements
  - White papers and product information documents
  - Many CRM's also allow firms to organize and share their competitive intelligence and guidance with their team through CRM
- **Slack** chat/team collaboration
  - **Gong** AI-generated and summarized transcripts of customer interactions
  - Events, progress and next steps between sales, implementation, support, and other teams
  - Win/loss analysis of sales efforts and prospect interviews listing reasons for selecting/not selecting Rippling
  - Identification of "at risk" customers who are considered likely to leave Rippling for another solution ("churn")
  - Internal discussions about problems not publicly acknowledged
- All access to these systems requires two-factor authentication, and use of these systems is monitored using access and activity logs

K2 Enterprises
Copyright 2026, K2 Enterprises, LLC

Slack Searches For “Deel” In Rippling’s Systems





Source: *Rippling’s complaint in San Francisco US District Court case 3:25-cv-02576-CRB document one, page 17*

Slack Searches For “Deel” In Rippling’s Systems

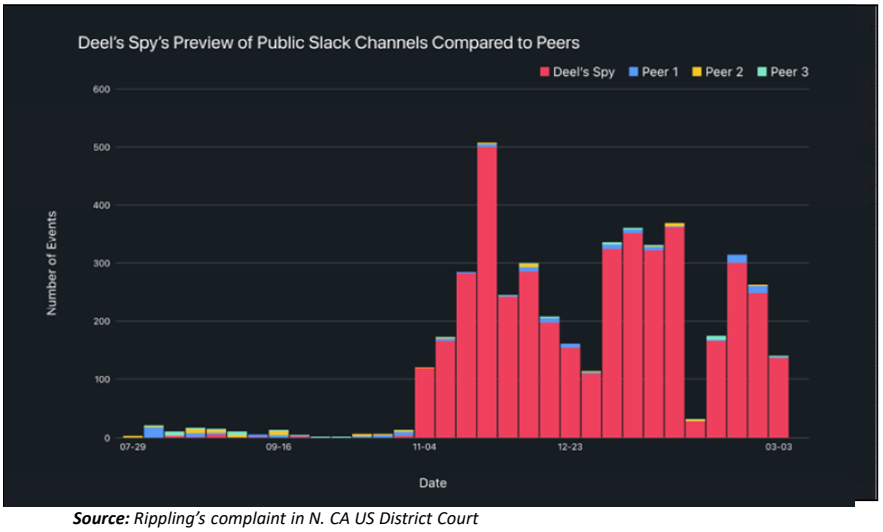
- Note how the search activity changed from almost no competitive information through October 2024 to a constant search for competitive information beginning in November 2024

Aug 2024		Sep 2024		Oct 2024	
Channel	Views	Channel	Views	Channel	Views
oasis-ytd-import	4	[redacted]	2	[redacted]	2
ppl-dogs	3	poland	1	churn_updates	1
payments	1	hub	1		
incident-response	1				

Nov 2024		Dec 2024		Jan 2025		Feb 2025	
Channel	Views	Channel	Views	Channel	Views	Channel	Views
deal-desk-sales	113	gong-stream-deel-compete	104	deal-desk-sales	164	[redacted]-peo	71
am-sales-updates	85	deal-desk-sales	98	gong-stream-deel-compete	105	im-gong-calls	54
gong-stream-deel-compete	73	im-gong-calls	63	im-gong-calls	88	deal-desk-sales	53
sdr-segment-drift	53	deel-gongstream	47	am-sales-updates	75	gong-stream-deel-compete	51
deel-gongstream	36	peo-quote-updates	41	notifications	57	emea-global-only-ob-notifications	28
global-apac-sdr-qualification	32	emea-sales-global-core	40	sdr-segment-drift	42	payroll-ukraine-russia	21
rattle-mops-testing	26	client-[redacted]-eor	37	peo-quote-updates	39	client-[redacted]-peo	21
foundgold-global-nls	25	mops-inbound-request-alerts	30	exec-escalations	38	am-sales-updates	17
emea-global-routing	24	deal-room-[redacted]	25	foundgold-global-nls	38	sales	17
ind-sdr-ae-opps	24	am-sales-updates	23	prospect-[redacted]	37	emea-sc-requests	16
comms-competitor-news	22	global-sc-requests	20	deel-gongstream	36	global-sc-requests	16
notifications	21	uki-s1-routing	15	bemie-wow	35	exec-escalations	15
sales-alerts	18	competitive-deal-insights	15	emea-sales-global-core	31	competitive-deal-insights	12
delighted-nps	18	foundgold-global-nls	15	client-[redacted]	30	namedaccount-[redacted]	12
uki-s1-routing	17	hr-sc-requests	13	uki-s1-routing	26	peo-quote-updates	12
sales-wins	14	delighted-nps	13	emea-global-routing	25	[redacted]-strategy	11
notifications	14	sdr-segment-drift	12	rattle-mops-testing	24	coaching	11
proj-deel-remote-compete	13	im_churn_updates	11	competitive-deal-insights	22	content-posting-hq	11
emea-sc-requests	13	peo-prospect-[redacted]	11	delighted-nps	20	mops-inbound-request-alerts	10
page-load-alerts	12	apac-forecast-updates	10	comms-competitor-news	18	foundgold-global-nls	10
ask-data-deletion	12	emea-global-routing	9	sdr-creating-referral-partner-optys	17	test-escalations-catch-all	10
aus-apac-background-checks-xevo	12	mm-global-high-intent-notifications	9	emea-sc-requests	17	sdr-segment-drift	10
emea-global-outbound-pods	11	competitor-marketing-in-the-wild	9	client-[redacted]-peo	17	mm-global-high-intent-notifications	10
in-product-cross-sell	10	mid-market-wins	8	client-[redacted]	16	am-ts-missedopportunities	9
hr-sc-requests	10	escalation-[redacted]	8	hr-sc-requests	14	gong-stream-justworks	9

Source: *Rippling’s complaint in N. CA US District Court case 3:25-cv-02576-CRB document one, page 18*

Slack Searches For “Deel” In Rippling’s Systems



Source: *Rippling’s complaint in N. CA US District Court case 3:25-cv-02576-CRB document one, page 18*

- Note that the log activity is analyzed for the individual over time….
- And is analyzed over time as compared to peers in similar corporate jobs within Rippling

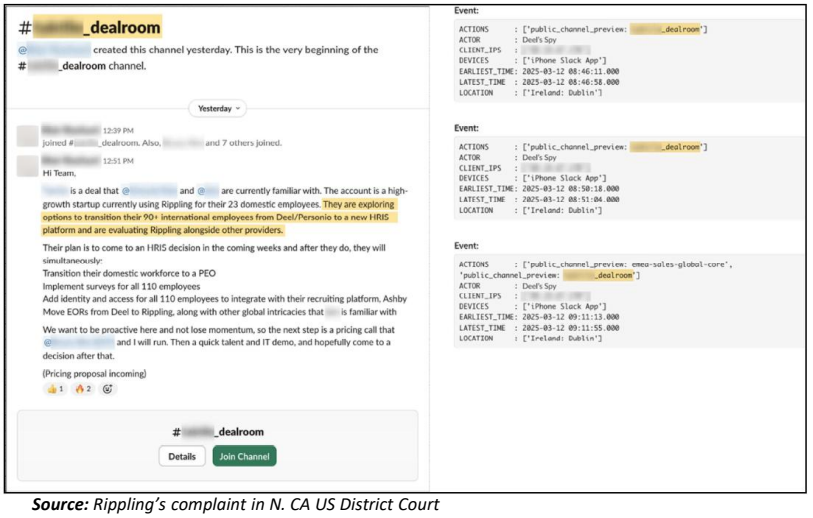
Top Slack Searches By Alleged Spy November 2024-February 2025

	A	B
1	**Channel name**	**Total count of events**
2	deal-desk-sales	428
3	gong-stream-deel-compete	333
4	im-gong-calls	209
5	am-sales-updates	200
6	deel-gongstream	123
7	sdr-segment-drift	117
8	peo-quote-updates	101
9	emea-global-only-ob-notifications	99
10	foundgold-global-nls	88

Source: *Rippling’s complaint in N. CA US District Court case 3:25-cv-02576-CRB document one, page 20*

- Even though the alleged spy’s job as a global payroll compliance manager had little need for sensitive sales information, suddenly this area was the focus of their use of Slack

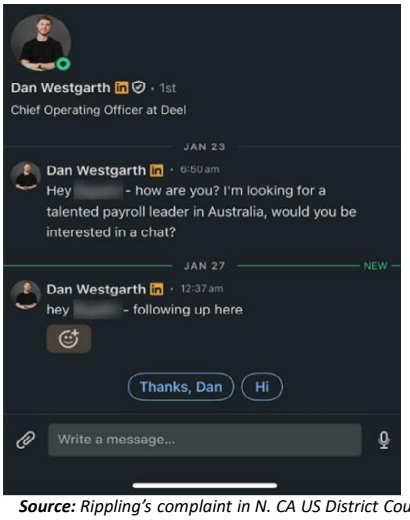
Example – Information Viewed

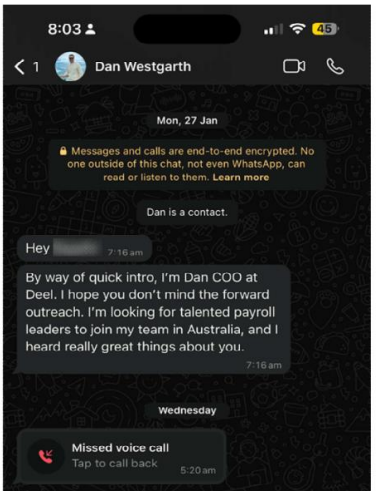


Source: *Rippling's complaint in N. CA US District Court case 3:25-cv-02576-CRB document one, page 22*

- A sales rep posted that a customer who used both Rippling and Deel told Rippling they were thinking about leaving Deel and consolidating all HRIS functions on Deel
- This post was viewed three times by the alleged spy

Example – Information Viewed





Source: *Rippling's complaint in N. CA US District Court case 3:25-cv-02576-CRB document one, page 26*

- In a three week period, 17 members of Rippling's Global Payroll Operations Team were solicited about jobs at Deel on their personal cell phone numbers – and ten of them received offers without having interviews!

Perp Allegedly Identified With A Honeypot

- **The Digital Trap:** Rippling set a "honeypot" via a fake Slack channel named #d-defectors
- **The Evidence:** O'Brien was flagged searching for the channel immediately after Deel execs were baited
- **The Legal Stakes:** Allegations include corporate espionage and RICO violations
- **The Denial:** Deel maintains the suit is a competitive tactic targeting a former employee.

The Honeypot - ***#d-defectors***

Dear Mr. Distelburger,

While I appreciate Deel's ongoing fascination with Rippling's hires and especially Deel defectors [redacted] and [redacted] rest assured, Rippling does not want Deel's confidential information[1].

But since you wrote, I wanted to raise our concerns. For starters, as Deel is surely aware, [redacted] no longer works here because of Deel. As Rippling's CRO Matt Plank recently learned:

Thursday, February 27th

Matt Plank 12:41 AM
Just learned a few crazy things in the #d-defectors channel...

#2 and #3 seem like real wtf's

I know this isn't my area of expertise, but those two things seem like they're pretty illegal...or really bad if it became public for them?

- **I learned the real reason [redacted] left; Deel cancelled all of his vested equity b/c he joined Rippling** - it was suddenly cancelled in Carta, which is how he found out. Csuite at Deel called him and basically said, *"You chose Rippling, so you're not going to get any of your equity."* And then gave it back when he resigned.
- **Deel is actively [redacted] and is knowingly processing [redacted]**
- **Someone apparently knows [redacted] at Deel, and said they have firsthand knowledge of some [redacted]** – for example [redacted] They included a pretty damning screenshot along with it (sender, timestamps, etc.).

[1] Rippling respects the intellectual property rights of others and takes the requisite precautions and measures to ensure that Rippling competes on fair terms. We have no reason to believe that any Deel confidential information or lawful restrictive covenant will be compromised by these hires. Specifically, our employees sign agreements that state they will not bring any third-party confidential information to Rippling, including that of any former employer. Beyond contractual controls, we employ several administrative and technical controls to ensure that our new hires are well versed on their continuing obligations to their prior employers, including policies, trainings, and restrictions on our referral bonus program. I trust that this addresses Deel's concerns with our existing and future hires from Deel.

Source: *Rippling's complaint in N. CA US District Court case 3:25-cv-02576-CRB document one, page 26*

- On March 3, 2025, Rippling's general counsel sent a letter to Deel's Board Chair, Deel's head of US Legal, and an employment attorney at Deel's outside law firm
- The letter's real purpose was to see who would try to access the information on the channel based on the "bait" placed in a letter sent to three Deel executives by Rippling
- **The bait was a Slack channel called #d-defectors** was a Slack channel which purportedly contained information about Deel from its ex-employees who now worked at Rippling
- The alleged spy reportedly responded with searches for "d defector" and "Matt Plank" the next morning

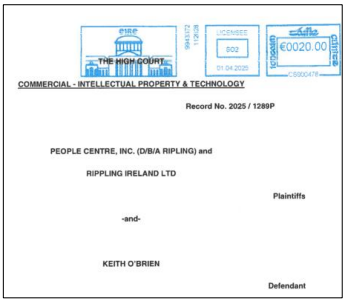
230	2025-03-04	matt plank
231	2025-03-04	matt plank
232	2025-03-04	matt plank
233	2025-03-04	matt plank
234	2025-03-04	matt plank
235	2025-03-04	matt plank
236	2025-03-04	matt plank
237	2025-03-04	matt plank
238	2025-03-04	matt plank
239	2025-03-04	d defector
240	2025-03-04	d defector
241	2025-03-04	d defector
242	2025-03-04	d defector
243	2025-03-04	d defector
244	2025-03-04	defector
245	2025-03-04	defector
246	2025-03-04	defector
247	2025-03-04	defector
248	2025-03-04	defector

Alleged spy's search history – 3/4/25

Alleged Dublin Subpoena Incident

The Confrontation

According to news reports and an affidavit published online, Irish court solicitors cornered the accused spy at Rippling's Dublin office on March 14, 2025.


THE HIGH COURT
COMMERCIAL - INTELLECTUAL PROPERTY & TECHNOLOGY
Record No. 2025 / 1289P
PEOPLE CENTRE, INC. (D/B/A RIPLING) and
RIPPLING IRELAND LTD
Plaintiffs
-and-
KEITH O'BRIEN
Defendant

Source Document: cpate.ch/dubsup

Alleged Dublin Subpoena Incident

- **The Barricade:** O'Brien allegedly fled to a bathroom and **locked himself inside to avoid surrendering his device**.
- **The Defiance**: Warned of potential jail time for deleting evidence, he reportedly shouted "*I'm willing to take that risk.*" and fled the location.

AI-Generated Image

Alleged Dublin Subpoena Incident

- O'Brien reportedly testified in court that he **destroyed the phone in question with an ax** and threw it down the drain at his mother-in-law's home
- This destruction happened after he had been served with a court order directing him to preserve and hand over the device for forensic inspection, meaning the axe incident was a direct breach of that order
- O'Brien is now cooperating with law enforcement

*(**Note:** Image is AI-generated content)*

Rippling v. Deel

Control Failure Themes

Search monitoring, download surveillance, privileged access recertification, and conflict-of-interest reporting appear central to the allegations.

Red Flags For Finance

Unusual report pulls near renewals or bids, abnormal CRM/HRIS queries, and staff accessing information outside normal role patterns.

Governance Lesson

Insider-risk programs need cross-functional ownership across legal, finance, information security, HR, and internal audit.

CPE Takeaway

Treat sensitive operational data as a key asset class, with detective controls and evidence preservation plans before litigation starts.

Rippling v. Deel

CPA-Focused Questions

- Which data sets would change revenue forecasts or deal pricing if leaked?
- Who can export full customer, payroll, or pricing files today?
- Are audit logs retained long enough to reconstruct insider activity?
- Is offboarding immediate for resignations, leaves, and role transfers?

Practical Safeguards

- Tight role-based access and quarterly access recertification.
- Alerts for bulk search, export, forwarding, and print activity.
- Mandatory disclosure of competitor contact and side payments.
- Preserve logs, laptops, chat records, and cloud trails at first suspicion.

Common Team Messaging Tools

Messaging Tool	Best Fit / How Commonly Used
Slack	Chat-first, heavy integrations, SaaS-heavy teams
Microsoft Teams	Microsoft 365 organizations, meeting-heavy environments
Google Chat	Google Workspace-centric orgs needing built-in chat
Zoho Cliq	Zoho One organizations needing chat-based communications
Zoom Team Chat	Teams already living in Zoom meetings or using Zoom Phone
Webex App	Enterprises standardizing on Cisco calling/meetings
Discord	Always-on voice and casual/channel based collaboration
Element	Self-hosted / federated security-conscious teams
Rocket.Chat	Open-source, on-premises Slack alternative
Zulip	Long-lived, topic-threaded conversations

Common Team AI Meeting Tools

- **Core "AI Notetaker"**: These tools join calls (Zoom/Teams/Meet, dialers) to handle transcription, summaries, and action items
- **Revenue / Conversation Intelligence:** These are more "sales-ops" oriented, often used by larger teams for analytics, coaching, and pipeline intelligence
- **Sales-Focused Meeting Automation & Follow-Up**: These tools emphasize post-meeting workflows like CRM updates, tasks, and follow-up emails.
- **Built-In Meeting Platform Assistants**: Used when teams sell via one platform and want native AI

Core AI Notetaking Tools	Revenue/Conversation Intelligence Platforms	Sales-Focused Meeting Automation & Follow-up	Built-in Meeting Platform Assistants
Fireflies.ai	Gong	Ask Elephant	Zoom AI Companion
Otter.ai	Chorus	Coffee AI	Microsoft Teams AI/Recap
Avoma	Salesloft	Meetingflow	Google Meet AI Features
Fathom	Zoominfo Copilot	Demodesk	RingCentral RingSense
tl;dv	RingCentral RingSense	Aloware AI Voice Analytics	
Tactiq	Salesken	MaxIQ	

Team Chat Security & Governance

- **Enforce strong identity controls**: SSO + MFA; least-privilege admin roles; quarterly access reviews
- **Control external collaboration**: clear guest/federation policy; approved domains/use cases; remove stale guests
- **Protect data:** DLP for chats/files; retention aligned to legal needs; test eDiscovery/holds/recovery
- **Set device/session conditions**: managed devices for full access; limit risky devices; monitor anomalous sign-ins
- **Govern apps & integrations:** restrict installs; review permissions; security-review high-risk apps/bots/webhooks
- **Be incident-ready:** audit logs to SIEM; alert on admin/app/sign-in/data-export risks; defined IR playbook
- **Sustain governance:** acceptable-use policy, recurring training, and annual cross-functional oversight

Lessons Learned

- If configured properly, the security, logging, and archiving of your team messaging tool can help you identify data leakage out of
- Digital workflows add many tools to work processes that handle sensitive data – and minor misconfigurations can create opportunities for data leaks
- The time to prepare for a breach is before one happens, and Rippling's log management and incident response plan helped management identify a spy in their midst – and gave them evidence for litigation when he was caught
- A well thought out security and data governance program can reduce, but will not eliminate risk of data leakage
- When you want to catch someone where they shouldn't be, traps called honeypots can be deployed which provide an irresistible target for spies and gossips bent on sharing sensitive information

"Online banking fraud leaves Winnipeg woman on hook for $174K debt" – CBC Manitoba, 12/2/2025

"Ex-Jaguars employee faces grand theft charges in Florida" – ESPN, 7/10/2025

"Former community bank vice-president to plead guilty to embezzling over $2 million" – PaymentsDive.com, 8/18/2025

ELECTRONIC PAYMENT RISKS

Bank Debit Card And ACH Theft

Electronic funds transfer fraud often starts with an insider failure: a bad account change, weak approval, or compromised employee workflow.

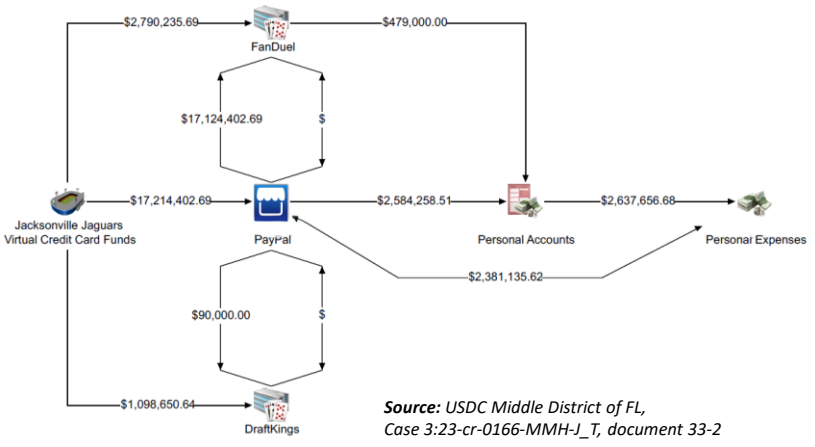
Linda Klassen, Hacking Victim

- 78 year old resident of Winnipeg, Manitoba
- Computer was hacked in May 2024
- Two bogus cheques totaling $100K CAD deposited into a disused checking account and money was transferred out to fraudulent payees at one credit union – this credit union covered the loss
- Four fraudulent cheques totaling $292K CAD then paid out with online bill pay at another credit union
  - The second credit union recovered $25K CAD from insurance and $92K CAD from tracing and recovery efforts
  - The institution refused to cover the remaining $174K in overdraft and the Klassens are now responsible for repaying those funds

Jacksonville Jaguars Credit Card Fraud

- Virtual Credit Card Administrator for NFL Jacksonville Jaguars (Name redacted, but let's call him "Bob")
- Diverted $22.2M USD over 3 ½ years through the Team's virtual credit card program, with the funds flowing through either PayPal or two gambling websites (FanDuel and DraftKings)
- Covered up the fraud with fraudulent accounting entries, fake transactions with real vendors, inflated real transaction amounts, fake transactions with fake vendors, largely funded through a PayPal account
- Spent most of the money on gambling losses, but approximately $5M was spend on personal expenses

Flows Of Funds
January 2021-March 2023



Source: *USDC Middle District of FL, Case 3:23-cr-0166-MMH-J_T, document 33-2*

- This diagram shows that the vast majority of the funds stolen from the virtual credit card program by Bob during the most active period of his theft ($21.1M) flowed through:
  - PayPal - $17.2M
  - FanDuel - $2.8M
  - DraftKings - $1.1M
- During this time period, prosecutors report that $17.2M was spend from PayPal to fund gambling, while $5.0M was spent on personal expenses

The Receipts: Living XXL

Court filings report that "Bob" stole more than $22 million – here's where it went (according to court filings and news reports)

- More than $20 million lost at betting site **FanDuel** and $1 million lost to **DraftKings**
- Over $278,000 for **hotels, rental properties and travel**, including $78,800 for private jet charters and $70,362 with Delta, United, American, Southwest and JetBlue airlines
- $140,412 on **eBay**
- $69,025 with **Ticketmaste**r
- > $200,000 for **golf memorabilia**, including $47,113.92 to purchase Tiger Woods' 1996 U.S. Amateur Champion Scotty Cameron gifted putter
- More than $77,000 at the private **Ponte Vedra Beach Inn & Club**, including a $25,581 initiation fee and $5,508 for spa treatments
- $9,477 with the **Jacksonville Jaguars** and related outlets

Name	Amount ($)
FanDuel	$ 20,079,874.07
DraftKings	1,188,650.64
Apple	580,628.53
Newegg	297,084.11
Amazon	31,490.94
Palm Tree Music Festival	22,240.18
Best Buy	10,485.93
Fantasy Sports	1,000.00
Grand Total	**$ 22,211,454.40**

Photo credits: Top, ESPN.com pic of Amit Patel
Bottom, Jacksonville Jaguars 2026 Media Guide

Sources: *USDC Middle District of FL, Court case 3:23-cr-0166-MMH-J_T, USA Sentencing Memo & media reports*

Litigation Against FanDuel/DraftKings

- In a strange twist, in 2025, "Bob" filed suit against FanDuel for $250M in Federal Court in New York City alleging that FanDuel had a duty under numerous standards to determine that the source of the funds were not stolen or another illegitimate source under regulations like
  - Know Your Customer (KYC)
  - Anti-Money Laundering (AML) (Bob had over 1,000 transactions >$10K)
  - Customer Due Diligence (CDD)
- "Bob" alleges in the complaint that FanDuel *"actively and intentionally targeted and preyed on Plaintiff with incentives, credits, and gifts to create, nurture, expedite, and/or exacerbate his addiction with the only possible outcome that he would ultimately hit rock bottom."*

Source: *USDC Southern District of NY, Court case 1:24-cv-07402-VSB, Document 36*

Litigation Against FanDuel/DraftKings

- As a VIP gambler, FanDuel assigned a VIP Host to provide "Bob" with incentives and assistance, including trips, experiences, and tickets during this period, including the Ritz Carlton Amelia Island, Miami Formula One Grand Prix, Sea Island, a Jaguars game in London, a trip to Kansas City for a Jaguars game, and a trip to the Pegasus World Cup
- The VIP Host also reportedly intervened when one of Bob's transactions was deemed to be "suspicious" by FanDuel's AML systems and told "Bob" that they got around the challenge
- As of April 18, this countersuit is still pending

Source: *USDC Southern District of NY, Court case 1:24-cv-07402-VSB, Document 36*

Community Bank ACH Fraud

- Small community bank vice president, 25 years service
- Embezzled $2.3 million between July 2013 and June 2023
  - Initiated 273 fraudulent ACH transfers from the banks Federal Reserve account to pay her personal credit card bills
- The fraud was concealed from management, auditors, and bank examiners by multiple methods:
  - Falsified general ledger entries
  - Deleted ACH transactions
  - Altered bank statements
- Fraud was discovered when the bank's president was notified by the Federal Reserve that the bank's ACH account was overdrawn
- Sentenced in August 2025 to 60 years in prison and 60 months supervised release, currently at FCI Marianna, FL

How ACH Theft Happens

1. Social Engineering

BEC or vendor impersonation convinces staff to change banking details or release a payment.

2. Master File Change

An insider or compromised user edits vendor or payroll bank information.

3. ACH Origination

Payment is sent through normal bank channels, often appearing routine.

4. Rapid Withdrawal

Funds are moved out before the business notices, limiting recovery options.

Critical ACH Controls

Risk	Risk Level
Vendor master maintenance	**Highest Risk**
Payroll account changes	**Very High**
Email-based approval workflows	**High**
Single-user ACH release	**High**
Callback verification gaps	**High**

- When was the last time you reviewed and tested these key controls in your organization?
- If you are an auditor, are these risky controls adequately documented and tested every time?

ACH Control Stack For CPAs

Authentication

Use MFA, bank-side entitlements, and separate credentials for setup versus release of ACH batches.

Verification

Require independent callback verification using known-good contact data before bank detail changes or urgent payments.

Segregation

No single user should create, approve, and release vendor, payroll, or treasury transactions.

Detection

Use bank alerts, velocity thresholds, payee-change reports, and anomaly review for dollar amount and timing outliers.

Response

Document same-day escalation steps with treasury, legal, cyber, insurer, and law enforcement contacts.

Training

Finance and AP staff need recurring drills on BEC, urgent tone fraud, and fake executive or vendor requests.

2026 NACHA Rule Changes

What Changed

NACHA's 2026 rule changes require risk-based processes to detect ACH credit entries initiated due to fraud, expanding fraud monitoring duties beyond prior narrower use cases.

Phase 1 applies **March 20, 2026** for high-volume non-consumer originators and third parties;

Phase 2 expands **June 19, 2026** to remaining originators and third-party providers.

Why It Matters to CPAs

Treasury and controllership teams should expect stronger expectations for baseline monitoring, exception handling, documentation, and coordination with ODFIs and RDFIs.

The rule direction supports a broader control narrative: ACH fraud detection is now a network-wide responsibility, not just a back-office issue.

Lessons Learned

- Checks/Cheques are risky, and electronic payments are more secure, transparent, and less susceptible to theft than cash or checks, but controls are often harder to implement due to system limitations
- Long overdue upgrades to electronic payments roll out this year – which may change your risks and responsibilities, and require revision of your internal controls
- Frauds related to electronic payments may not have as many institutional/government protections as traditional checks/cheques – so understand your risks here before your first loss
- Organizations often overlook the review of transactions executed by long-time senior employees, resulting in greater losses
- Controls over review, approval, reconciliation, and governance over electronic payments – for both bank accounts and credit cards are easy to overlook or ignore, and should be examined at least annually
- Alcohol and drugs aren't the only addictive habits that can destroy you – gambling, shopping, cars, food, sex, and almost anything else can become an addiction – so watch for those warning signs and help your employees get help if they need it

The New York Times

WAR ON THE ROCKS

"Anthropic Claims Its New A.I. Model, Mythos, Is a Cybersecurity 'Reckoning'" – New York Times, 4/8/2026

"Anthropic's Nuclear Bomb" –War on the Rocks national security blog, 4/16/2026

CYBERCRIMES, BREACHES, AND RAPID CHANGES TO THE SECURITY LANDSCAPE

Claude Mythos And Cybersecurity

- In April 2026, Anthropic introduced **Claude Mythos Preview** as a frontier model unusually strong at computer security tasks and framed it as a major shift in the cyber landscape
- The company said the model was *"strikingly capable at computer security tasks"* and described the moment as a *"watershed moment for security"*
- Anthropic's public writeup argues the same capabilities that help patch bugs can also help find, weaponize, and chain vulnerabilities faster
- This is why Anthropic paired the release with Project Glasswing, a limited-access defensive initiative aimed at securing critical software before similar capabilities are more widely available

Why Is Mythos "A Reckoning"?

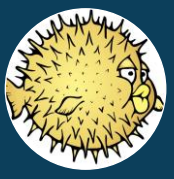
The New York Times

*The **New York Times** described Anthropic's framing of Mythos as a cybersecurity "reckoning," capturing the idea that the security industry may be entering a period where elite exploit development becomes far more accessible*

- It suggests a discontinuity, not just another incremental model improvement
- It implies pressure on patching velocity, secure coding, and exploit validation
- It shifts the conversation from "AI for SOC productivity" to "AI as force multiplier for offense and defense"

What Mythos Reportedly Found

Zero-day exploits discovered in EVERY major operating system and web browser



Mythos highlighted a now-patched 27-year-old OpenBSD Linux vulnerability

Anthropic also cited a 16-year-old FFmpeg video player bug it said Mythos identified

THN

The Hacker News summarized the effort as "**thousands of high-severity zero-days across major systems**."

Benchmark Signals From Anthropic

- Anthropic reported 10 full control-flow hijacks against **fully patched** OSS-Fuzz targets in its internal Tier-5 benchmark
- It also said Mythos generated 181 working JavaScript shell exploits for patched Firefox vulnerabilities, versus 2 for Opus 4.6
- On vulnerability severity assessments, human reviewers exactly matched Claude on 89% of 198 reports and were within one level 98% of the time

By the Numbers:

- ***10** Tier-5 control flow hijacks*
- ***181** Firefox JavaScript shell exploits identified*
- ***89%** Exact validator match for severity*
- ***98%** within one level for severity*

How Mythos Changes Cybersecurity

DISCOVERY COMPRESSES

- Models can accelerate vulnerability discovery, proof-of-concept generation, and exploit refinement in one loop rather than several separate workflows

SCALE IMPROVES OFFENSE

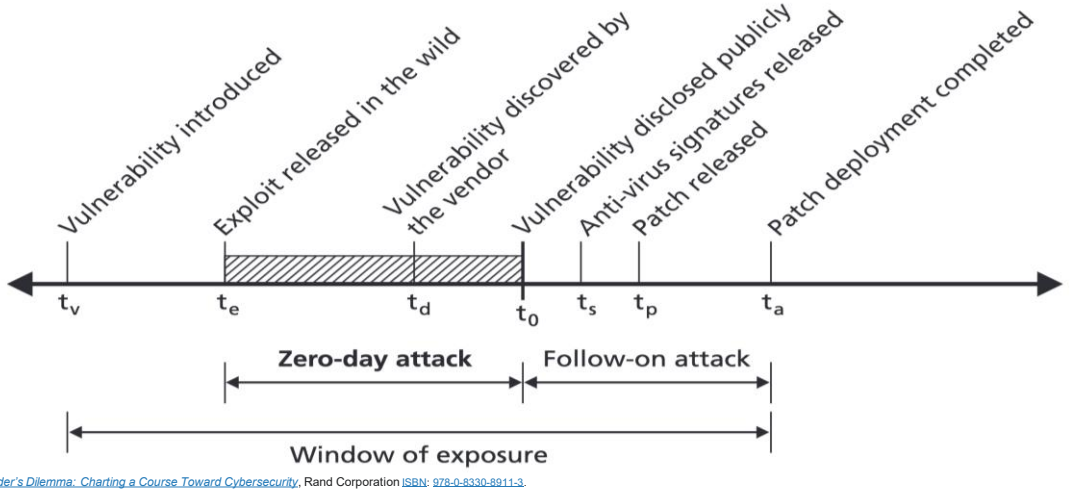
- An attacker can test more hypotheses, targets, and bypasses at lower marginal cost once the model handles repetitive technical work

DEFENSE MUST AUTOMATE ALSO

- Security teams that stay manual will fall behind teams that use AI for patch verification, regression testing, exploit replay, and code hardening

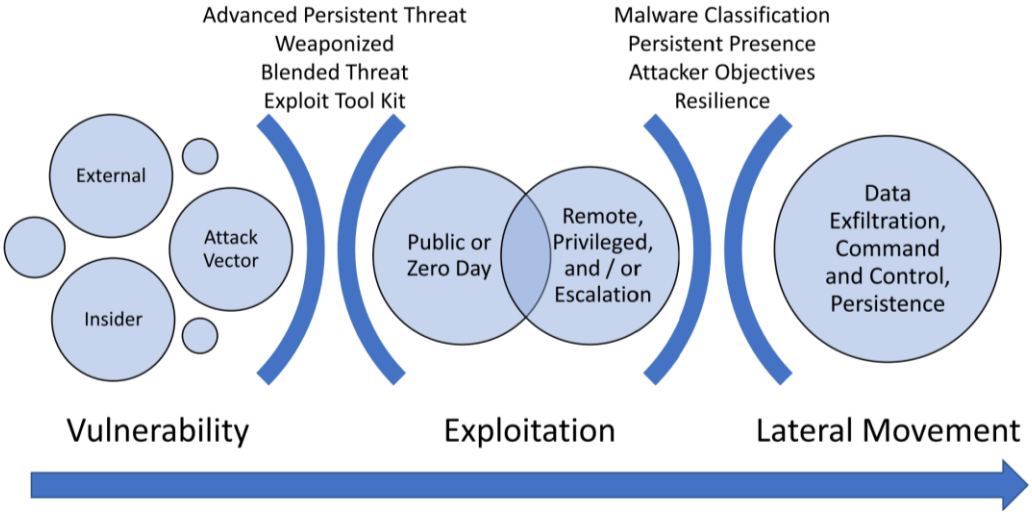
War on the Rocks cast Mythos as a strategic inflection point rather than merely a product launch, because the real issue is how quickly frontier-model cyber capabilities diffuse into state, criminal, and commercial ecosystems.

Timeline Of A Security Vulnerability



(2015) *The Defender's Dilemma: Charting a Course Toward Cybersecurity*, Rand Corporation ISBN: 978-0-8330-8911-3.

The Cyberattack Process



Project Glasswing / Mythos Rollout

- Anthropic said Mythos Preview access is limited to a small group of organizations rather than open broad release
- Named collaborators include AWS, Apple, Cisco, CrowdStrike, Google, JPMorgan Chase, Microsoft, NVIDIA, Palo Alto Networks, and the Linux Foundation
- The company said it would provide up to $100 million in usage credits and $4 million in direct donations to open-source security organizations

Project Glasswing

Securing critical software for the AI era

Anthropic described the Project Glasswing effort as an "urgent attempt" to use frontier model capabilities for defense before enemies can exploit comparable capabilities at scale.

Conclusion

***Mythos* Points To A Future Where Security Speed IS Strategy**

- If Anthropic's claims hold up, the main lesson is not that defenders are doomed; **it is that cybersecurity is becoming even more of an engineering-speed contest**
  - *Teams that can rapidly discover, validate, patch, and harden will benefit*
  - *Teams that depend on slow manual processes and latent technical debt will face rising risk*

Lessons Learned

- The cybersecurity landscape is changing rapidly, and AI continues to be used by both attackers and defenders
- Anthropic's Claude Mythos platform is the first of many large language models which can enhance or defeat the cybersecurity of organizations
- This uncertainty means that firms should both apply AI-based defense tools as well as redouble their efforts to maintain logs through their Security Information and Event Management (SIEM) systems

AI-ENABLED FRAUD: FASTER, CHEAPER, AND MORE CONVINCING

HOW TO DETECT A DEEPFAKE

LOOK FOR INCONSISTENCIES:

- Are any of the facial features blurry or distorted?
- Does the person blink too much or too little?
- Do the hair and teeth look real?
- Are the audio and video out of sync?
- Is the voice tone flat or unnatural?
- Does the visual show odd or unnatural shadows or lighting?

TIPS TO STAY SAFE

STOP AND THINK. Is someone trying to scare you or pressure you into sending money or sharing personal information?

VERIFY the legitimacy of people and requests by using trusted numbers, official websites and online reverse image/video search tools.

CREATE CODEWORDS or phrases with loved ones to confirm identities.

LIMIT YOUR DIGITAL FOOTPRINT. Photos, voice clips and videos can be used to train deepfake models.

NEVER REPOST videos or images without verifying the source.

RED FLAGS OF A DEEPFAKE SCAM

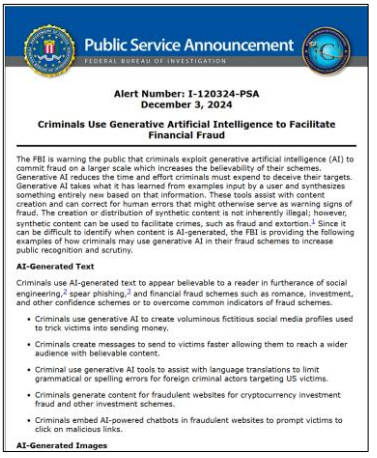
Unexpected requests for money, passwords, personal information or secrecy.

Emotional manipulation involving fear or urgency.

Uncharacteristic communication from someone you know, especially over text, phone or video.

FBI/IC3 Alerts On AI-Based Frauds

- **FBI/Internet Crime Complaint Center (IC3) – some relevant posts**
  - **Alert I-120324-PSA** – *"Criminals Use Generative AI to Facilitate Financial Fraud" (12/3/2024)*
  - **Alert I-040225-PSA** – *"Criminal Actors Steal US Taxpayer Identity to File False Tax Returns and Claim Refunds" (4/2/2025)*



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-120324-PSA
December 3, 2024

Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud

The FBI is warning the public that criminals exploit generative artificial intelligence (AI) to commit fraud on a larger scale which increases the believability of their schemes. Generative AI reduces the time and effort criminals must expend to deceive their targets. Generative AI takes what it has learned from examples input by a user and synthesizes something entirely new based on that information. These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud. The creation or distribution of synthetic content is not inherently illegal; however, synthetic content can be used to facilitate crimes, such as fraud and extortion.[1] Since it can be difficult to identify when content is AI-generated, the FBI is providing the following examples of how criminals may use generative AI in their fraud schemes to increase public recognition and scrutiny.

AI-Generated Text

Criminals use AI-generated text to appear believable to a reader in furtherance of social engineering,[2] spear phishing,[3] and financial fraud schemes such as romance, investment, and other confidence schemes or to overcome common indicators of fraud schemes.

- Criminals use generative AI to create voluminous fictitious social media profiles used to trick victims into sending money.
- Criminals create messages to send to victims faster allowing them to reach a wider audience with believable content.
- Criminal use generative AI tools to assist with language translations to limit grammatical or spelling errors for foreign criminal actors targeting US victims.
- Criminals generate content for fraudulent websites for cryptocurrency investment fraud and other investment schemes.
- Criminals embed AI-powered chatbots in fraudulent websites to prompt victims to click on malicious links.

AI-Generated Images

AI-Generated Text

- Criminals use AI-generated text to appear believable to a reader in furtherance of social engineering,[2] spear phishing,[3] and financial fraud schemes such as romance, investment, and other confidence schemes or to overcome common indicators of fraud schemes.
- Criminals use generative AI to create voluminous fictitious social media profiles used to trick victims into sending money.
- Criminals create messages to send to victims faster allowing them to reach a wider audience with believable content.
- Criminal use generative AI tools to assist with language translations to limit grammatical or spelling errors for foreign criminal actors targeting US victims.
- Criminals generate content for fraudulent websites for cryptocurrency investment fraud and other investment schemes.
- Criminals embed AI-powered chatbots in fraudulent websites to prompt victims to click on malicious links.

AI Supercharges Phishing And Business E-mail Compromises (BEC)

Attackers now use large language models (LLMs) to:

- **Scrape LinkedIn profiles, websites, and social media** to build hyper-personalized messages referencing real colleagues, projects, and business language
- **Generate thousands of unique, tailored spear-phishing emails per hour**, bypassing spam filters
- **Clone executive voices** from just seconds of publicly available audio to authorize fraudulent payments by phone
- **Fabricate deepfake documents** to support fraudulent wire transfers or invoice manipulation

Introduction To Business Email Compromise (BEC)

The Billion-Dollar Threat: Understanding BEC

- **What is BEC?** A targeted fraud where criminals impersonate trusted individuals (executives, clients, vendors) to trick a business into sending money or sensitive data.
- **The Approach:** Unlike generic spam, it relies on social engineering, spear phishing, and abusing established business trust.
- **The Threat in Canada:** BEC and spear phishing are among the most financially damaging online crimes in Canada.
- **Financial Impact:** In the first half of 2025 alone, Canadian businesses reported **$26.7 million** in BEC losses

Who Do Attackers Impersonate?

- **Executives (CEO Fraud):** Urgent requests from leadership demanding immediate wire transfers or confidentiality.
- **Vendors/Suppliers:** Spoofed invoices or emails advising of a "new bank account" for future payments.
- **Legal Counsel/Advisors:** Requests for sensitive financial records or transaction facilitation.
- **Internal Employees:** Payroll redirection schemes targeting HR departments.

The Vancouver Law Firm Incident (Mid-2025)

- **Target**: A law firm based in the metro Vancouver area in British Columbia
- **Method**: Spear phishing/BEC impersonation of a trusted business contact.
- **Loss Amount**: CAD $2.3 Million.
- **Destination**: A fraudulent bank account located in Hong Kong.
- **Significance**: A massive cross-border attack that highlights the vulnerability of professional services.

Step 1: Reconnaissance

- **Studying the Target**: The attackers likely monitored the firm's operations, identifying key personnel and existing financial relationships
- **Impersonation:** The threat actors created a highly convincing email that mirrored the communication style, domain, and signature of a legitimate, trusted party involved with the firm
- At this point, the firm and its personnel would likely have no idea that they were being surveilled

Step 2: The Hook

- **The Spear Phishing Email:** The law firm received an email that appeared completely routine but contained fraudulent instructions
- **The Trap:** The email requested the wire transfer of CAD $2.3 million to an account in Hong Kong, posing as a legitimate business transaction or vendor payment
- **The Error:** Believing the request was genuine, the firm bypassed secondary verification (such as a phone call) and authorized the wire transfer

Step 3: The Alarm / Discovery

- **The Catch**: The fraud was initially flagged not by the firm, but by a local bank in Hong Kong that noticed the highly suspicious $2.3 million incoming transfer
- **Immediate Escalation**: The Hong Kong bank promptly alerted the Hong Kong Police Force's Anti-Deception Coordination Centre (ADCC)
- **Firm Notification:** The Vancouver law firm was made aware of the fraudulent nature of the transaction shortly after the funds had been sent

Step 4: The Response

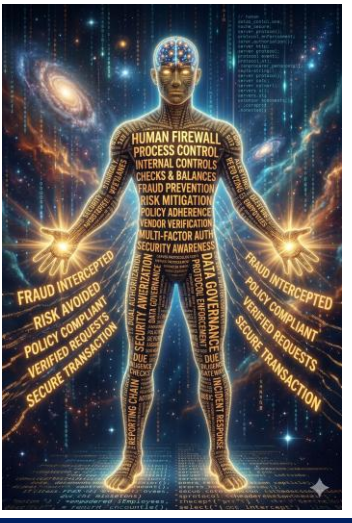
- ***How the Firm Responded - Cross-Border Action***
- **Rapid Reporting**: The firm and authorities immediately engaged the Canadian Anti-Fraud Centre (CAFC)
- **Law Enforcement Synergy:** The CAFC worked in real-time with the Hong Kong ADCC
- **The Outcome**: Because the alarm was raised quickly and international agencies cooperated flawlessly, the entire CAD $2.3 million was intercepted and returned to the firm

Responding To The BEC Threat:
Hardening the Perimeter

- **Multifactor Authentication** (MFA): Mandatory for all corporate email accounts to prevent initial account takeovers
- **Email Authentication**: Implement DMARC, SPF, and DKIM to make it harder for attackers to spoof the firm's domain
- **Security Tools:** Utilize advanced threat protection (like Defender for Office 365) to flag domain mismatches and suspicious forwarding rules

Responding To The BEC Threat:
Process Controls/Human Firewall

- **Out-of-Band Verification:** Always verify changes to payment instructions or urgent wire requests by calling the contact directly using a trusted, pre-established phone number
- **Dual Authorization:** Require multiple levels of sign-off for large fund transfers
- **Awareness Training:** Regularly train staff to spot BEC red flags, such as sudden urgency, secrecy, or unexpected changes to banking details



WIRED

"'A Billion Streams and No Fans': Inside a $10 Million AI Music Fraud Case" – Kate Knibbs, Wired, May 25, 2025

FAKE MUSIC AS A BUSINESS MODEL AND THE LAW

Fake Music, Real Dollars

- **Michael Smit**h, a 54-year-old resident of Cornelius, North Carolina, formerly an aspiring musician and songwriter with a modest legitimate catalog of songs recorded by artists such as Snoop Dogg, Billy Ray Cyrus, and the Avila Brothers
- Smith was indicted in late 2024 and pleaded guilty on March 19, 2026, to one count of conspiracy to commit wire fraud for creating hundreds of thousands of AI-generated songs and then profiting by deploying thousands of bots that generated over $10 million in royalties from streaming services
- The case highlights the intersection of generative AI, high-frequency automation, and the financial structures of the modern digital music economy – just as some were caught up in the music industry's overreach in the early days of digital music, Smith is the first of many cases which will define the caselaw associated with streaming and other digital entertainment

The $10MM “Ghost” Revenue Model

- Between 2017 and 2024, the scheme successfully siphoned over $10 million (prosecutors later settled on a forfeiture amount of approximately $8.1 million) in royalty payments.
- Funds were diverted from major streaming platforms including Spotify, Apple Music, and Amazon Music, effectively stealing from the "royalty pool" meant for legitimate human artists.
- Because streaming services pay out based on a percentage of total plays, Smith’s "fake" streams directly reduced the per-stream rate for every other artist on the platforms.

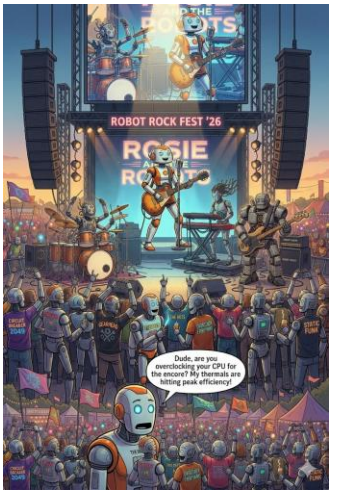
amazon music

Spotify

Music

Phase One: Mass Production via Generative AI

- To avoid detection, Smith couldn't simply loop one song. He needed a massive, varied catalog to blend into the platforms' global traffic.
- In 2018, Smith partnered with the CEO of an unnamed **AI music company** and a music promoter to create songs at scale.
- At its peak, the operation generated and uploaded **hundreds of thousands** of AI-generated tracks.
- Tracks were given randomized, nonsensical names like *"Zygotes"* or *"Zyme Bedewing"* and attributed to thousands of fake artist personas like *"Calms Scorching."*



Phase Two:
The Bot Army And Infrastructure

- Smith deployed a sophisticated network of up to **10,000 bot accounts** programmed to stream his music 24/7.
- The defendant purchased thousands of fake email addresses in bulk and used outsourced labor to bypass account registration security.
- Prosecutors estimated the bots could generate approximately **661,440 streams per day**, totaling billions of plays over the life of the scheme.

Phase Three:
Evading Fraud Detection Systems

- **The "Human-Like" Mimicry:** To prevent the platforms from flagging the activity, Smith coded his bots to behave like real users—shuffling tracks, stopping at random intervals, and "listening" to varied artists within his own fake catalog.
- **Technical Obfuscation:** The bots utilized **Virtual Private Networks (VPNs)** to mask their IP addresses, making it appear as though the listeners were distributed across the globe rather than localized in a North Carolina server farm.
- **The Dilution Strategy:** Smith intentionally spread the streams across hundreds of thousands of songs so that no single track reached a level of popularity that would trigger a manual audit by platform moderators.

The Smoking Gun

- **Calculated Intent:** Internal communications seized by the FBI showed Smith was fully aware of the illegality and the anti-fraud hurdles.
- In a 2018 email to co-conspirators, Smith wrote:
  "We need to get a TON of songs fast to make this work around the anti-fraud policies these guys are all using now."
- By February 2024, Smith emailed himself a financial breakdown, boasting of generating over **4 billion streams** and over **$12 million** in projected royalties since the inception of the bot farm.

Intervention By The Mechanical Licensing Collective (MLC)

- In 2023, the **Mechanical Licensing Collective (MLC)**, a nonprofit that administers blanket mechanical licenses to streaming services, became suspicious of Smith's astronomical streaming numbers
- When the MLC challenged Smith to provide proof of his "legitimate" audience or the origins of his massive catalog, he reportedly provided false information to maintain the flow of royalties
- The MLC's data-sharing with federal authorities provided the critical evidence needed for the SDNY to build a criminal case rather than a simple civil copyright suit

THE MLC
MECHANICAL LICENSING COLLECTIVE

The Guilty Plea & Legal Repercussions

- **The Plea Agreement:** On March 19, 2026, Smith appeared before **U.S. District Judge John G. Koeltl** and admitted to the conspiracy
- **Financial Penalties:** As part of his plea, Smith agreed to a massive **forfeiture of $8 million**, representing the illicit gains from the streaming manipulation
- **Sentencing Outlook:** Smith faces a maximum of **five years in federal prison**
  - His sentencing is currently scheduled for **July 29, 2026**
- U.S. Attorney **Jay Clayton** emphasized that while the tech was modern, the crime was "old-fashioned thievery"
  - *"Although the songs and listeners were fake, the millions of dollars Smith stole was real... Smith's brazen scheme is over, as he stands convicted of a federal crime for his AI-assisted fraud"*
- **The Precedent:** This case serves as a warning to the "AI-slop" industry that manipulating platform algorithms for financial gain can now carry criminal—not just civil—consequences

Lessons Learned

- As AI and our society evolve together, the rules of how to use AI and the lines between acceptable use, shameful (but legal) use, and illegal use will become more clear
- This uncertainty increases the risk but also increases the potential rewards associated with being the “first movers” in a particular category
- Overreach will occur in this uncertain period – in a few decades, this will be settled law – but this uncertainty creates risk in the short term
  - A generation ago, file sharing platforms like Napster ran dragnets at universities to catch people pirating music
  - 20 years ago, Sony settled a class action for placing a special kind of malware called a “rootkit” in their aggressive zeal to stop computer users from making digital copies of their audio CD collections
- **Smith’s actions to create billions of streams with no fans force all of us to open our minds to consider the new kinds of fraud that will be dreamed up in the age of AI – and beyond**

Conclusion: Turning Headlines Into Actionable Anti-Fraud Strategies

- The advent of AI supercharges the ability of fraudsters to compromise your systems while covering their tracks
  - Reconnaissance using AI tools and web scraping
  - Identification of systems and selection of compromise attacks
  - Creating fake supporting documents
- New ways to steal will be invented which have never been seen before – like creating and having bots stream AI generated music
  - Monitor current events
  - Conduct internal and external security reviews/audit
  - Harden your controls, especially around authentication
  - Train your team and test them with targeted simulations
  - Implement security incident and event management (SIEM) tools
  - Revise your incident response plan
- While you may not be able to stop everything, you can be ready to respond

QUESTIONS