

SAMPLE: a made-up incident. The organization, people and reference numbers are invented.



MANSIOSEC · INCIDENT TIMELINE

Incident timeline

Confidential
www.mansiosec.com

Made with the free MansioSec Incident Timeline. For the full response record and a customer report in your firm's name, see the Incident Log at www.mansiosec.com.

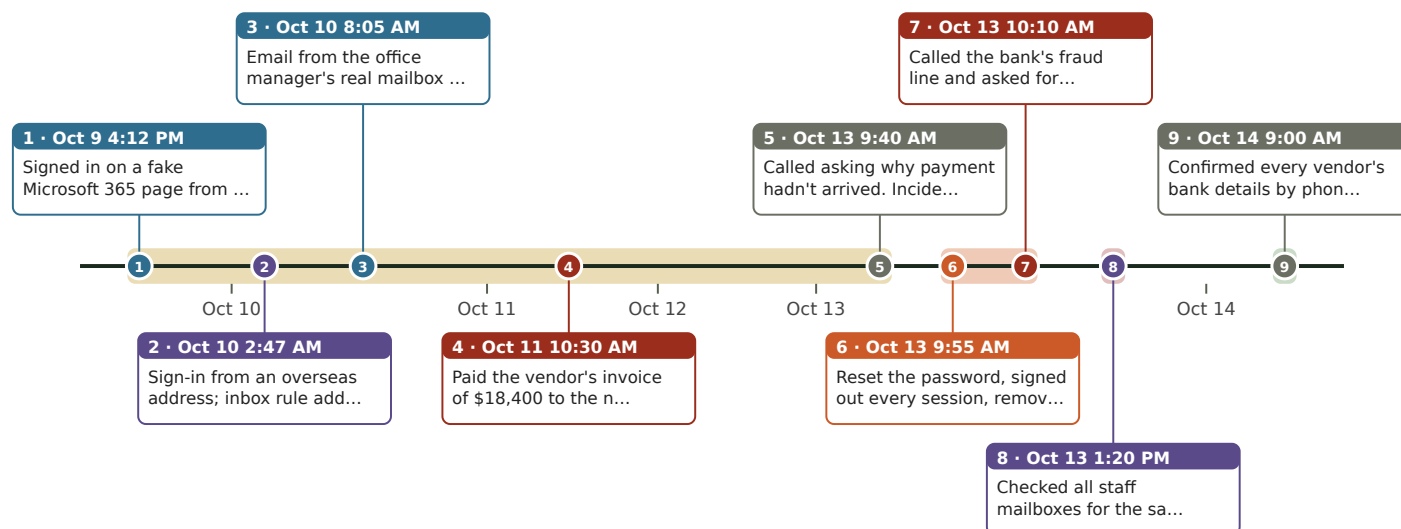
Office manager mailbox compromise and fake invoice

Client / organization: Sample Dental Group (made up) · ID IR-SAMPLE-031 · Business email compromise · Severity: High · Status: Recovering · Printed Oct 16, 2026, 10:00 AM

IMPACT STARTED Oct 9, 2026, 4:12 PM	DETECTED Oct 13, 2026, 9:40 AM	CONTAINED Oct 13, 2026, 1:20 PM	REPORTED BY Lab vendor (phone call)
TIME TO DETECT 3 d 17 h	TIME TO CONTAIN 3 h 40 min		

The office manager's mailbox was signed into from outside the US after a phishing page captured the password. The attacker added a rule hiding replies, then emailed the lab vendor's accounts team from the real mailbox with "new bank details". One \$18,400 payment was sent before the vendor called to ask about it.

Timeline



Source ■ Email or mailbox logs ■ Sign-in or audit logs ■ Bank or payment records ■ Phone or call records
■ Responder notes **Phase** ■ Detect and analyze ■ Contain ■ Eradicate ■ Recover

Numbers follow the table below. Spacing is stretched where events are close together, so the axis isn't to scale.

#	TIME	PHASE	WHO	WHAT	SOURCE
Friday, October 9, 2026					
1	4:12 PM	Detect and analyze	Office manager	Signed in on a fake Microsoft 365 page from an email about a "shared invoice".	● Email or mailbox logs: Phishing email kept; sign-in log
Saturday, October 10, 2026					
2	2:47 AM	Detect and analyze	Attacker	Sign-in from an overseas address; inbox rule added moving replies from the lab vendor to RSS Feeds.	● Sign-in or audit logs: Microsoft 365 audit log
3	8:05 AM	Detect and analyze	Attacker	Email from the office manager's real mailbox to the vendor: "our bank has changed, please update before Friday's payment".	● Email or mailbox logs: Sent items
Sunday, October 11, 2026					
4	10:30 AM	Detect and analyze	Bookkeeper	Paid the vendor's invoice of \$18,400 to the new account details.	● Bank or payment records: Bank portal
Tuesday, October 13, 2026					
5	9:40 AM	Detect and analyze	Lab vendor	Called asking why payment hadn't arrived. Incident opened.	● Phone or call records: Call notes
6	9:55 AM	Contain	J. Rivera (consultant)	Reset the password, signed out every session, removed the inbox rule, turned on the second sign-in step.	● Responder notes: Admin center
7	10:10 AM	Contain	Practice owner	Called the bank's fraud line and asked for a recall of the \$18,400 wire.	● Bank or payment records: Bank reference SAMPLE-RC-4471
8	1:20 PM	Eradicate	J. Rivera (consultant)	Checked all staff mailboxes for the same rule and sign-ins: none found.	● Sign-in or audit logs: Audit log search
Wednesday, October 14, 2026					
9	9:00 AM	Recover	Practice owner	Confirmed every vendor's bank details by phone, using numbers already on file.	● Phone or call records: Vendor call list

Actions

WHEN	PHASE	ACTION	BY	STATUS
Oct 13, 2026, 9:55 AM	Contain	Reset password, revoke sessions, remove inbox rule, require second sign-in step	J. Rivera	Done

WHEN	PHASE	ACTION	BY	STATUS
Oct 13, 2026, 10:10 AM	Contain	Ask the bank to recall the wire	Practice owner	In progress
Oct 14, 2026, 9:00 AM	Recover	Turn on the second sign-in step for every staff mailbox	J. Rivera	In progress
Oct 15, 2026, 12:00 PM	Post-incident	Adopt a call-back rule and two approvers for payments over \$2,500	Practice owner	Planned

Notifications

WHO	DEADLINE	NOTIFIED	REFERENCE	NOTES
Cyber insurer	Oct 14, 2026, 5:00 PM	Oct 13, 2026, 11:15 AM	SAMPLE-CLM-88211	Breach line called before any outside help was hired.
Bank or card company	Oct 13, 2026, 12:00 PM	Oct 13, 2026, 10:10 AM	SAMPLE-RC-4471	Wire recall requested.
Law enforcement (FBI IC3, local police)	Oct 13, 2026, 5:00 PM	Oct 13, 2026, 10:40 AM	SAMPLE-IC3-0093	
Legal counsel	Oct 16, 2026, 5:00 PM	Not yet		Ask whether any patient data was in the mailbox.

MansioSec Incident Timeline (free) · www.mansiosec.com · © 2026 JCady LLC. A working record of what was known at the time, prepared by the person who filled it in. Not legal advice, and no promise of insurance coverage or recovery of money.