

INCIDENT REPORT

Sample Dental Group (made up) · Office manager mailbox compromise and fake invoice · ID IR-SAMPLE-031

Report date Oct 16, 2026, 10:00 AM · Status: Recovering

SUMMARY

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.

Client / organization	Sample Dental Group (made up)
Type	Business email compromise
Severity	High
Status	Recovering
Impact started	Oct 9, 2026, 4:12 PM
Detected	Oct 13, 2026, 9:40 AM
Contained	Oct 13, 2026, 1:20 PM
Time to detect	3 d 17 h
Time to contain	3 h 40 min
Reported by	Lab vendor (phone call)
Incident lead	Alex Sample (Example Security Partners)
Prepared by	Alex Sample, CISSP

WHAT WAS AFFECTED

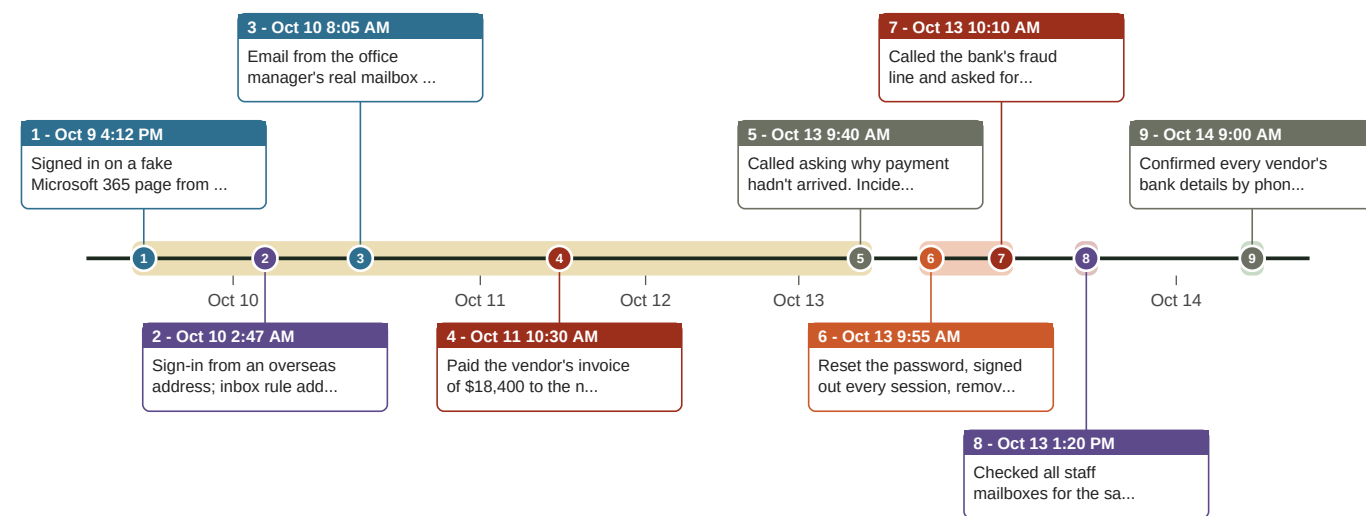
Systems and devices	Office manager's Microsoft 365 mailbox; front desk PC
Accounts	office.manager@ (sample) mailbox
Data that may be exposed	Names and contact details, Financial or bank details
People who may be affected	1 vendor; patient data not found in the mailbox so far
Money lost or at risk	\$18,400
Downtime	Mailbox locked for 2 hours during containment
Business impact	One payment sent to a fraudulent account; recall in progress.

RESPONSE CHECKLIST

Phase	Step	Done
Detect and analyze	Confirm what happened, and when it started	Done
Detect and analyze	Name an incident lead and the client's decision-maker	Done

Phase	Step	Done
Detect and analyze	Call the cyber insurer's breach line before hiring outside help, if the policy requires it	Done
Detect and analyze	Check sign-in logs for the account: locations, times, devices	Done
Detect and analyze	Find emails the attacker sent, and who received them	Done
Detect and analyze	Report to the FBI at ic3.gov (fast reports help recall wires)	Done
Contain	Preserve evidence before wiping or rebuilding anything	Done
Contain	Reset the password and sign out every session	Done
Contain	Remove forwarding rules, inbox rules and delegates the attacker added	Done
Contain	Turn on or re-register the second sign-in step	Open
Contain	Warn contacts who got messages from the account	Open
Contain	If money moved: call the bank's fraud line now and ask for a recall	Open
Recover	Confirm normal operations with the client	Open
Post-incident	Hold a lessons-learned review within two weeks	Open
Post-incident	Add each improvement to the Risk Register	Open
Post-incident	Give the customer the incident report	Open

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 happened or was done	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

#	Time	Phase	Who	What happened or was done	Source
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 TAKEN AND PLANNED

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
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	Contact and 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.

Who	Deadline	Notified	Reference	Contact and notes
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.

INDICATORS OF COMPROMISE

Kind	Value	Note
IP address	203.0.113.47	Overseas sign-in (documentation address range)
Domain or website	microsoft-sharedinvoice.example	Phishing page

EVIDENCE

Item	Where it's stored	Collected	SHA-256
Phishing email (.eml)	Case folder, encrypted share	Oct 13, 2026, 10:05 AM, Alex Sample	9f2c4e8b1a7d36f0c5e2b8a41d7f93e6c0b5a2d8e4f17c39a6b0d2e5f8c1a734
Microsoft 365 audit log export	Case folder, encrypted share	Oct 13, 2026, 11:20 AM, Alex Sample	3b7e1d9c5a2f08e64c1b7d3a9e5f2c08b6d4a1e7f3c95b2d08e6a4c1f7b3d952

DECISIONS

When	Decided by	Decision
Oct 13, 2026, 10:15 AM	Dr. R. Example	Report to IC3 and the insurer before hiring outside help, as the policy requires.

POST-INCIDENT REVIEW

Root cause	The office manager entered her password on a phishing page, and the mailbox had no second sign-in step.
Contributing factors	No second sign-in step on staff mailboxes. No call-back rule before changing a vendor's bank details. Nobody watched sign-in alerts.
What limited the damage	The vendor called within two days. The bank's fraud team acted on the recall the same morning.
Risks this uncovered	Other staff mailboxes had the same gap. Vendor bank changes are approved by one person.
What worked	Containment within 15 minutes of the call.
What to improve	Second sign-in step everywhere; call-back rule and two approvers for payments.

FOLLOW-UP ACTIONS

Action	Owner	Phase	Status
Ask the bank to recall the wire	Practice owner	Contain	In progress
Turn on the second sign-in step for every staff mailbox	J. Rivera	Recover	In progress

Action	Owner	Phase	Status
Adopt a call-back rule and two approvers for payments over \$2,500	Practice owner	Post-incident	Planned

RESPONSE TEAM AND CONTACTS

Role	Name	Organization	Phone or email
Incident lead	Alex Sample	Example Security Partners	(555) 010-0199
Client decision-maker	Dr. R. Example	Sample Dental Group	(555) 010-0142
Cyber insurer breach line	Claims desk	Sample Mutual Insurance	(555) 010-0170

This report records what was known and done at the time it was written. It is not legal advice, and it does not promise insurance coverage or recovery of money. Confirm notification duties and deadlines with counsel.