Lock Down the Account After a Security Scare

Last Modified on 11/10/2026 12:23 pm EST

Something looks wrong — a document nobody remembers uploading, a client contacted by someone posing as your title company. Here's how to find out what happened and shut the door, in the order that matters.

Introduction

Real estate transactions are a favourite target for wire fraud, and the pattern is consistent: someone gets sight of a live deal, waits for the closing, and emails the buyer new wiring instructions. Which means a security scare in a transaction management system is never really about the software. It's about a closing that's about to go wrong.

So this runs in two halves. First, find out what actually happened: we can pull a login report for your account, and that usually answers the question in an afternoon. Then close the gaps, in the order that closes the biggest one first, which is almost never the one people expect.

Work through it now, in one sitting. Every step below is quick, and none of them are worth doing next week.

When to Use This

- A document appeared on a transaction and the person it's attributed to says it wasn't them.
- A client has been emailed wiring instructions that didn't come from your office.
- Someone who left the company may still know a password that works.
- A staff member's email account was compromised and you don't know what else it reached.
- You've been sharing one login between several people and have realised what that means.

Why This Beats Changing the Passwords and Moving On

The instinct is to reset everybody's Pipeline password and consider it handled. It isn't, for two reasons.

The first is that the way in usually wasn't Pipeline. Almost every incident of this shape starts with a compromised *email* account, and email is also where a Pipeline security code would be sent — so resetting Pipeline passwords while leaving the mailbox open changes nothing at all. The second is that without a login report you're guessing about what happened, and a guess is a poor basis for telling a client whether their deal was exposed. Look first, then close, and close the email side as seriously as the Pipeline side.

1. Ask Us for a Login Report

Email us and say what you're seeing. As a courtesy we can generate a login report for your account — recent sign-ins with the timestamp, the IP address, and the email address used.

That report is usually what turns a suspicion into a fact: an unfamiliar IP on a Sunday night, or a run of logins on one address from two places at once. Send us the specifics that worried you — the transaction, the document, the date — so we can look at the right window.

Need a hand? The quickest way to reach us is right inside Pipeline — and a real person on our team reads every message.

See Get Help

> Alongside it, pull the Usage by Agent report yourself — it shows who's been signing in and uploading, which is a useful second view over the same period. Download the Usage by Agent report to see who's logging in, who's uploading, and who hasn't touched Pipeline at all. See Usage by Agent.

2. Close the Shared-Credential Hole

This is the step people skip, and it's frequently the whole explanation. If two people use one login, Pipeline has no way to tell them apart — the activity history records the profile, not the person behind it, and there's no session or IP detail exposed on your side to work back from. A document "uploaded by" a name is only ever evidence that somebody was signed in as that name.

So before anything else: one profile per person, no exceptions, and no passwords passed around the office. Anyone who needs access gets their own.

Add the agents and staff on your team so each person can log in and work in Pipeline under their own account.

See Adding a User

> This is also why an incident on a shared login can't be fully investigated after the fact — for anyone, including us. Fixing it now is what makes the *next* question answerable.

3. Reset Pipeline Passwords — and Email Passwords

Have everyone change their Pipeline password. Then have them change their **email** password too, and treat that as the more important of the two.

The email account is the soft target in every version of this. It's where the fraud usually starts, and it's where a Pipeline security code would arrive — so an attacker sitting in someone's mailbox has both halves. Strong, unique passwords on both, and multi-factor on the mail system if it offers it.

Reset a password you've forgotten, change one you know, or reset one for an agent.

See Password Reset

> Someone unreachable, or a reset email that never arrives? We can set a temporary password on a user's profile at an admin's request, and they change it from their own profile once they're in.

4. Ask Us to Force Everyone Out

Resetting a password doesn't end a session that's already open. If you think someone is currently in the account, ask us to log every user out — our Tech Team can do it, and there's no self-service button for it anywhere.

It's worth pairing with the next step. If two-factor is on when everyone signs back in, every session that comes back is one that passed a code sent to a mailbox you've just secured.

5. Turn On Two-factor Authentication

This is the durable fix, and it's the one that makes a stolen password stop being enough. A master admin switches it on from Company Settings — for the whole office, or for specific people if you're rolling it out gradually.

It has to be you. We can't enable or disable it on your behalf, by design: a support team that could turn off a customer's two-factor would be a way around it.

Two-factor authentication adds a second step when you log in on a device Pipeline doesn't recognize: an email to finish logging in, with a link to click or a code to type.

See Two-factor Authentication

> Expect a few calls about codes not arriving in the first week — it's nearly always mail filtering rather than Pipeline. When two-factor authentication is on but the code never reaches your inbox, it's almost always an email-delivery problem — not your Pipeline account. See Not Receiving Your Security Code.

6. Tell Us What You're Seeing

Keep us in it rather than closing the ticket once the passwords are changed. Our security team wants the details of anything that looks like a targeted attempt on a real estate transaction, and what you've seen may line up with something we're already tracking.

One distinction that shapes the response: if clients are being contacted *outside* Pipeline — emails that appear to come from your title company, sent to addresses that were never in the system — that's an email compromise rather than a Pipeline one. It still matters to us, and it changes where you should be looking hardest.

Paperless Pipeline protects your data with bank-grade encryption, isolated accounts, and PCI-certified infrastructure — with simple ways to add your own layer on top.

See Paperless Pipeline Security