



An Extended Guide · No. 2072

The FTC Safeguards Rule: Does It Apply to Your Small Business?

Who counts as a financial institution,
and what the rule requires

Tech Made Simple — Service Made Personal

BillsHomeTech.com · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —
billshometech.com/book

! Read this first — the two things that stop most attacks

Almost every small-business break-in starts in one of two ordinary ways: a password that got stolen or guessed, or a convincing email that talked someone into clicking or paying. You do not have to become a computer expert to stop most of it. Turn on two-step sign-in (also called multi-factor authentication, or MFA) everywhere you can, keep a backup you have actually tested, and give yourself permission to slow down before you click a link, open an attachment, or send a payment. That is the whole game, most days. The FTC Safeguards Rule asks businesses it covers to build a written program around exactly those habits — so the question that matters first is whether the rule applies to you at all.

Does this federal rule apply to your small business?

The FTC Safeguards Rule requires certain businesses — called 'financial institutions' — to keep a written security program with specific pieces, and to report some breaches to the FTC. The catch is that 'financial institution' is defined far more broadly than it sounds. This guide helps you figure out if it means you.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping small businesses with their technology. I'm a tech helper, not a lawyer — so my job here is to explain the rule plainly, help you set up the safeguards it asks for, and point you to an attorney for the question of whether, and exactly how, it applies to you.

Here's the headline: a lot of ordinary small businesses that would never call themselves 'financial' are swept in — tax preparers, accountants, auto dealers that arrange financing, mortgage brokers, and more. If that might be you, it's worth ten minutes to understand this.

★ I'll help you build what the rule asks for

The rule calls for MFA, encryption, access controls, monitoring, and an incident plan — the exact things I set up and test for small offices. I'll make the safeguards real; your attorney confirms how the rule applies. Call or text me at (330) 200-8042.

First, the honest disclaimer

Whether this rule applies to you is a genuine legal question, so let me be clear about what this guide can and can't do.

I'll give you the examples, the pieces of the rule, and the deadlines that are well established, so you understand it and can ask good questions. But 'am I a financial institution under this rule?' is an interpretation of federal law, and the rule's text can be updated — so the final word belongs to the FTC's own guidance or an attorney.

! A quick, important note

This guide explains the FTC Safeguards Rule in plain English so you know what to ask about — it is general information, not legal advice, and it is not a substitute for the actual rule (16 CFR Part 314) or the FTC's guidance. Whether the rule applies to your business, and exactly what it requires of you, is a legal question that depends on your situation, and the rule can change. Please confirm the current rule text and how it applies with the FTC's guidance or an attorney before you rely on anything here.

✓ Check the FTC's own small-business guidance

The FTC publishes plain-language guidance for small businesses on the Safeguards Rule at ftc.gov. When in doubt about whether you're covered or what's required this year, that guidance and an attorney are your authoritative sources — not this summary.

The whole guide, on one page

If you remember only these things, you'll know whether to dig deeper and whom to ask.

- ❑ The FTC Safeguards Rule (**16 CFR Part 314**, under GLBA) requires covered businesses to keep a **written security program**.
- ❑ **'Financial institution' is broad** — it catches tax preparers, accountants, auto dealers that arrange financing, mortgage and consumer lenders, collection agencies, and more.
- ❑ The program needs a named **Qualified Individual**, a risk assessment, access controls, encryption, MFA, monitoring, training, vendor oversight, and an incident-response plan.
- ❑ Core amendments took effect **June 9, 2023**.
- ❑ A **breach-notification duty** (16 CFR 314.4(j)) took effect **May 13, 2024**: notify the FTC within **30 days** of a notification event involving **500+ consumers'** unencrypted information.
- ❑ Whether you're covered is a legal question — confirm with the FTC's guidance or an attorney.

! The breach-notification clock is short

If the rule applies and you have a qualifying breach, the window to notify the FTC is as soon as possible and no later than 30 days after you discover it. That's not long when you're also handling the incident — which is exactly why knowing this in advance matters.

What the Safeguards Rule is

A little background makes the whole thing make sense.

The Safeguards Rule is part of how the federal Gramm-Leach-Bliley Act (GLBA) protects consumers' financial information. It lives in the Code of Federal Regulations at 16 CFR Part 314, and it's enforced by the Federal Trade Commission — the FTC. In plain terms, it tells certain businesses: if you handle people's financial information, you must protect it with a real, written security program.

The FTC strengthened the rule with amendments whose core requirements took effect June 9, 2023, spelling out specific elements a program must include rather than leaving it vague. Then, effective May 13, 2024, it added a duty to report certain breaches to the FTC. So the rule now has real teeth and real specifics.

✓ It's a cousin of the tax-preparer WISP

If you read our tax-preparer plan guide, this will feel familiar — that WISP requirement flows from this very rule. The Safeguards Rule is the broader law; the tax-preparer WISP is one slice of it aimed at one profession.

Who counts as a 'financial institution'

This is the surprise that catches small businesses: the term is far broader than banks.

Under this rule, a 'financial institution' isn't just a bank or a credit union. It's any business significantly engaged in activities that are financial in nature — and that sweeps in a lot of ordinary small businesses. Being paid primarily to prepare taxes, arrange financing, or lend money usually puts you in scope. Examples the FTC points to include:

- **Tax preparers and accountants** — see our tax-preparer plan guide.
- **Mortgage brokers and lenders**, and payday or other consumer lenders.
- **Auto dealers that arrange financing** for buyers.
- **Collection agencies** and check cashers.
- **Financial and investment advisors**, wire-transfer services, and some real-estate settlement services.

! You may be covered without feeling 'financial'

An auto shop that helps buyers get a loan, or an accountant who'd never call themselves a financial institution, can both fall under this rule. Don't rule yourself out by gut feel — if you touch customers' financial information as part of your service, ask whether you're covered.

How to figure out if it's you

You can't answer this with certainty from a guide — but you can get close enough to know whether to call an attorney.

Start with what your business actually does with consumers' financial information. The more central that is to your service — preparing taxes, arranging or making loans, managing money — the more likely you're covered. A business that merely accepts payment for unrelated goods is in a different position than one whose service is financial.

Because the line can be genuinely fuzzy, treat the examples as a prompt, not a verdict. If any of them sound like you, or you're simply not sure, the right move is to confirm with the FTC's published guidance and, for a definite answer, an attorney who knows the rule. This is one of those places where a short legal conversation is money well spent.

✓ 'Not sure' is a reason to ask, not to assume

The costly mistake is assuming the rule doesn't apply and finding out otherwise after a breach. If you can't clearly rule yourself out, treat that uncertainty as your cue to get a professional read — then you'll know, and you can act.

What a compliant program includes

If the rule applies, your written security program needs these pieces. Most are things a well-run small office should do anyway.

- **A named Qualified Individual** — one person responsible for the security program (can be an owner or a vendor you oversee).
- **A written risk assessment** — identifying where your data is and what could go wrong.
- **Access controls and encryption** — limiting who can reach data, and scrambling it at rest and in transit.
- **Multi-factor authentication (MFA)** — a second sign-in step on access to customer information.
- **Monitoring and testing** — watching for problems and checking that your safeguards work.
- **Training, vendor oversight, and an incident-response plan** — people, partners, and a plan for the bad day.

★ Most of this list is my everyday work

MFA, encryption, access controls, monitoring, a tested incident plan — these are exactly what I set up for small offices. I'll make the technical pieces real and provable; your attorney confirms the program meets the rule. Call (330) 200-8042.

The Qualified Individual, in plain English

One requirement trips people up on wording alone, so let's demystify it.

The rule asks you to name a 'Qualified Individual' responsible for overseeing and running your information security program. It sounds grand, but for a small business it usually just means one accountable person — often the owner. The point is that security isn't left as everyone's job and therefore no one's.

You can use an outside provider to help carry out the work, but you remain responsible for overseeing them — you can't simply outsource the accountability and walk away. If you hire help, keep control of your key accounts and stay the one who's ultimately answerable. Our [hiring-outside-IT-help](#) guide covers what to keep in your own hands.

✓ Name the person, even if it's just you

In a one- or two-person shop, writing 'the owner is the Qualified Individual' is a perfectly good answer. What matters is that the name is written down and that person actually owns the program — not the size of the title.

The duty to report breaches to the FTC

This is the newest piece, and the one with a clock on it, so it's worth getting exactly right.

Effective May 13, 2024, the rule added a breach-notification duty, found at 16 CFR 314.4(j). If you have a 'notification event' involving the unencrypted information of 500 or more consumers, you must notify the FTC — using the online form on the FTC's website — as soon as possible and no later than 30 days after you discover it.

Two details matter. First, the trigger is **unencrypted** information — which is one more reason encryption is on the required list. Second, this duty to notify the FTC is separate from any state breach-notification law you may also have to follow, like Ohio's — see our Ohio breach-notification guide. A lawyer helps you sort out all the notices that may apply.

! Report to the FTC within 30 days — on their form

When the duty applies, the notification goes to the FTC through its online reporting form, as soon as possible and no later than 30 days after discovery. Know this before you ever need it, because 30 days goes fast when you're also cleaning up a breach.

Covered or not, the safeguards are worth doing

Whether the rule reaches you changes the stakes, not the basic to-do list — the safeguards it names protect any small business.

If you're likely covered (tax, lending, financing)

If your service is financial — preparing taxes, arranging loans, financing cars — treat the rule as applying until an attorney tells you otherwise, and build the full written program.

- Name your Qualified Individual and write the risk assessment the rule expects.
- Put the required safeguards in place: MFA, encryption, access controls, monitoring, training.
- Know the breach-notification steps and the 30-day FTC clock before you ever need them.
- Get an attorney to confirm your program meets the rule — see our tax-preparer plan guide if you prepare taxes.

If you're probably not covered

If you don't handle consumers' financial information as your service, the rule may not reach you — but the same habits are still the cheapest insurance you can buy against a hack.

- You still want MFA, tested backups, updates, and individual logins — see our one-page security plan guide.
- A breach can still trigger Ohio's notification law — see our Ohio breach-notification guide.
- If you grow into financial services later, revisit whether the rule now applies.
- If you're unsure which group you're in, that uncertainty itself is a reason to ask an attorney.

★ Not sure which side of the line you're on?

Tell me what your business does with customers' financial information, and I'll help you understand the question and set up the safeguards either way — then an attorney gives you the legal answer. Call (330) 200-8042.

What if you're very small?

The rule bends a little for the smallest institutions — but it doesn't let them off the hook.

The Safeguards Rule gives institutions that handle information on fewer than 5,000 consumers some relief from a few of its more formal program elements. It's a recognition that a tiny shop can't be held to the same paperwork as a large firm. But 'some relief' is not 'exempt' — smaller covered businesses still must protect customer data and comply with the rule broadly.

So if you're a small covered business, don't read the relief as permission to skip the basics. You still need real safeguards — MFA, encryption, access controls, an incident plan — and the breach-notification duty still applies. The relief trims some formality, not the protection itself.

✓ Let an attorney tell you what you can trim

Exactly which elements a smaller institution can scale back is a detail of the rule, and it can change. Don't guess at it. Confirm with the FTC's guidance or an attorney which parts apply to a business your size, so you trim the right things, not the protections that matter.

Two requirements worth a closer look

Of all the pieces, two come up most and do the most good: MFA and encryption.

Multi-factor authentication

The rule expects MFA on access to customer information. In plain terms, a password alone shouldn't be enough to reach customer data — there's a second step, like a code from an app or a tap on your phone. It's the single highest-value control, and our Microsoft 365 and Google Workspace sign-in guides show how to turn it on.

Encryption

The rule expects customer information to be encrypted, both when it's stored and when it's sent. For a small office that means turning on disk encryption (BitLocker on Windows, FileVault on Mac) and using secure, encrypted connections for data in transit. Encryption also matters for the breach duty, since the clock is triggered by exposure of **unencrypted** information.

★ I'll turn both on and show you the proof

MFA and disk encryption are quick wins I set up and verify all the time. I'll get them working across your office and leave you with dated proof they're on — useful for the rule and for insurance. Call (330) 200-8042.

The vendors who touch your data

The rule expects you to oversee the service providers who handle customer information for you — not just your own systems.

Most small businesses rely on outside services: cloud storage, software providers, an IT helper, a payment processor. The rule expects you to choose providers capable of protecting your data, to require them by contract to maintain safeguards, and to keep an eye on them over time. You can delegate the work; you can't delegate away the responsibility.

Practically, that means knowing who can reach your customer data, what they're supposed to do to protect it, and removing access that's no longer needed. Vendor and remote access is a common break-in path, so this isn't just paperwork — it's one of the real doors you need to keep watched.

✓ Keep a short list of who can reach your data

Write down every vendor and helper who can touch customer information, what access they have, and when you last reviewed it. Removing one unused account can close a door you didn't realize was open — and it's exactly the oversight the rule has in mind.

Writing it all down

The rule doesn't just want you to do these things — it wants them written into a program you keep and follow.

Your safeguards need to live in a written information security program: who the Qualified Individual is, what your risk assessment found, which safeguards you use, how you train and oversee vendors, and your incident-response plan. If that sounds like a bigger version of our one-page security plan, it is — the one page is the seed, and this is the fuller document.

Keep it current. The rule contemplates periodic risk assessments and updates as your business and the threats change. A dated program you actually review beats a polished one written once and forgotten — both for real protection and for showing good-faith effort if you're ever asked.

✓ Start from the one-page plan and grow it

If writing a full program feels daunting, begin with our one-page security plan guide and expand each section into the detail the rule asks for. You'll find you already have the bones; you're just adding the required specifics.

This isn't the only rule that may apply

The Safeguards Rule often sits alongside other obligations. Knowing that keeps you from thinking one checkbox covers everything.

Meeting the FTC Safeguards Rule doesn't automatically satisfy every other duty you may have. A breach can trigger state notification laws like Ohio's at the same time as the federal FTC duty, and different rules can apply if you handle medical or card data. These overlap rather than replace each other.

- **Ohio breach notification** — a separate state duty to notify affected residents; see our Ohio breach-notification guide.
- **Ohio Data Protection Act (Safe Harbor)** — a voluntary legal defense for keeping a written program; see that guide.
- **Tax-preparer WISP** — the slice of this rule aimed at preparers; see our tax-preparer plan guide.
- **Card or medical data rules** — PCI or HIPAA may add duties if you handle those.

! One rule met is not all rules met

Don't assume that satisfying the Safeguards Rule clears you of state laws or industry rules — or the other way around. When a breach happens, several clocks can start at once. A lawyer helps you see the whole set of notices and duties, not just one.

A calm path to getting compliant

If the rule applies, here's a sensible order of operations that doesn't require panic.

- ❑ Confirm with an attorney whether — and how — the rule applies to your business.
- ❑ Name your Qualified Individual and do a written risk assessment of where your data lives.
- ❑ Turn on the core safeguards: MFA, disk encryption, access controls, backups, monitoring.
- ❑ Write the program: safeguards, training, vendor oversight, incident response — grow it from the one-page plan.
- ❑ Learn the breach-notification steps and the 30-day FTC clock before you ever need them.
- ❑ Set a schedule to reassess risk and update the program as things change.

★ I'll take the technical load off your plate

You and your attorney own the legal shape of the program; I'll handle the hands-on safeguards — MFA, encryption, monitoring, a tested backup — and leave you proof each one is on. Call (330) 200-8042.

The mistakes that cause trouble

Most problems with this rule come from a handful of misunderstandings. Now you'll sidestep them.

- **Assuming you're not covered** because you don't feel 'financial' — check, don't guess.
- **Treating the smaller-business relief as an exemption** — it trims formality, not the core duty.
- **Skipping encryption** — it's required, and it's what keeps a breach below the notification trigger.
- **Not knowing the 30-day FTC breach clock** until a breach is already underway.
- **Outsourcing and walking away** — you still oversee vendors and remain responsible.
- **Writing the program once and never revisiting it** — the rule expects ongoing reassessment.

! The riskiest move is assuming it doesn't apply

Every other mistake here is fixable with a little work. Wrongly deciding the rule doesn't cover you can leave you with no program and a legal duty you didn't know you had. If there's any doubt, that doubt is worth a short attorney conversation.

Where to get reliable help

You don't have to interpret a federal rule alone. Here's who to lean on for which part.

- **The FTC ([ftc.gov](https://www.ftc.gov)):** plain-language small-business guidance on the Safeguards Rule, and the breach-reporting form.
- **An attorney:** for the legal question of whether you're covered and exactly what's required.
- **CISA ([cisa.gov](https://www.cisa.gov)):** free guides and vulnerability-scanning help for small businesses.
- **Ohio's free small-business cyber resources:** CyberOhio and state programs — confirm current offerings.
- **Me, for the technical safeguards:** MFA, encryption, monitoring, backups, and the proof they're on.

✓ Match the question to the right helper

'Does this rule apply to me?' is for an attorney. 'How do I turn on the safeguards it wants?' is for someone like me. Using each for what they do best gets you a solid, defensible program without overpaying for either.

How this connects to cyber insurance

The rule and a cyber-insurance policy reinforce each other — doing one makes the other easier and cheaper.

The safeguards the Safeguards Rule requires — MFA, encryption, backups, an incident plan — are the very same ones a cyber-insurance application asks about. So the work you do to meet the rule tends to improve your insurability and may lower your premium. Our cyber-insurance application guide walks through those questions.

The reverse is true too: insurance is a backstop, not a substitute for the rule. A policy won't make you compliant, and being compliant won't pay your recovery costs. If you're a covered business, you likely want both — a real program to meet the law, and coverage for the day something gets through anyway. See our 'Do You Need Cyber Insurance?' guide.

✓ Do the work once, benefit twice

Set up MFA, encryption, and a tested backup, and you've moved toward meeting the rule and toward a better insurance quote in a single effort. The habits that satisfy the FTC are the same ones carriers reward.

Keeping the program alive

Compliance isn't a one-time event. The rule expects a living program — here's how to keep it that way without it taking over your life.

- ❑ Reassess your risks periodically and whenever your business changes meaningfully.
- ❑ Confirm the core safeguards are still on — MFA for everyone, backups tested, encryption in place.
- ❑ Review vendor access and remove what's no longer needed.
- ❑ Refresh staff training and keep a dated record it happened.
- ❑ Re-read the current FTC guidance now and then, since the rule can change.
- ❑ Re-date the written program at each review so it stays demonstrably current.

★ Let me handle the periodic tech check-up

I can do a yearly pass over your safeguards — confirm MFA, test a restore, check for end-of-support software, review who has access — so your program stays real, not just written. Call (330) 200-8042.

Common Questions

The questions I hear most from owners wondering about the FTC Safeguards Rule, answered plainly.

Q: I'm not a bank — how could this rule apply to me?

Because 'financial institution' is defined broadly. It catches businesses significantly engaged in financial activities — tax preparers, accountants, mortgage and consumer lenders, auto dealers that arrange financing, collection agencies, and more. If you handle customers' financial information as part of your service, ask whether you're covered.

Q: How do I know for sure whether I'm covered?

You confirm it with the FTC's own guidance and, for a definite answer, an attorney who knows the rule. Whether it applies is a legal question that depends on exactly what your business does — a guide like this can tell you when to ask, but not give you the final word.

Q: What does the rule actually require?

A written security program with a named Qualified Individual, a risk assessment, access controls, encryption, MFA, monitoring and testing, staff training, vendor oversight, and an incident-response plan. Most of it is what a well-run small office should do anyway.

Q: What's the breach-notification duty?

Effective May 13, 2024 (16 CFR 314.4(j)), if you have a notification event involving the unencrypted information of 500 or more consumers, you must notify the FTC on its online form as soon as possible and no later than 30 days after discovering it. State laws like Ohio's may also apply.

Q: I'm tiny — am I exempt?

Not exempt, but there's some relief. Institutions handling information on fewer than 5,000 consumers are excused from a few formal program elements, yet still must protect data and comply broadly, including the breach duty. An attorney can tell you exactly what you can scale back.

★ Wondering if this rule is about you?

Give me a call and we'll talk through what your business does and what the rule asks for, in plain English — then I'll help you set up the safeguards and point you to an attorney for the legal call. Call or text (330) 200-8042.

You don't have to do this alone

You just have to remember that a friendly, patient person is one call away.

I hope this guide made the FTC Safeguards Rule feel a little less daunting and a lot more doable. Keep it with your other business papers, come back to a page whenever you need it, and don't worry about memorizing anything.

When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a 30-day, come-back-free guarantee. I'm a tech helper, not a lawyer or your insurance agent — for the legal and insurance pieces I'll help you understand the questions and line up the right professional.

★ Bill's Home Tech — real help, close to home

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County. 30+ years of patient, plain-English tech help — and if you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

Who the Rule May Catch

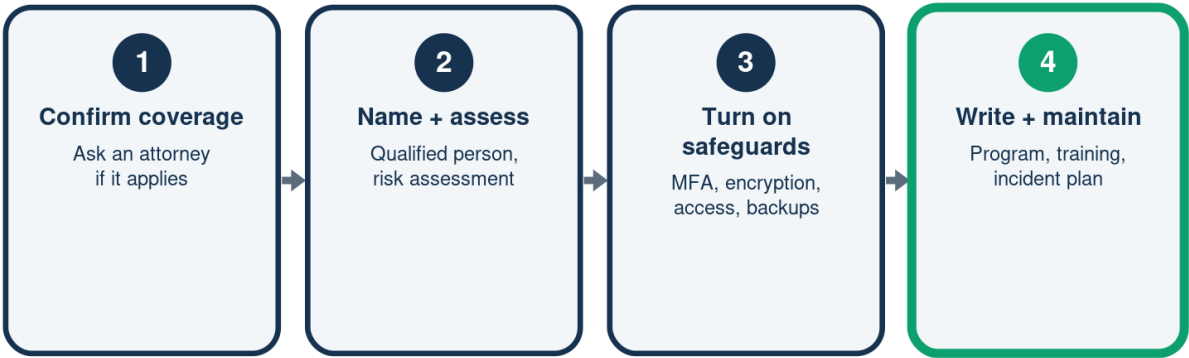
'Financial institution' is broader than banks

	Why covered	Also see
Tax preparers	Handle tax data	Our WISP guide
Auto dealers	Arrange financing	If they finance
Mortgage brokers	Arrange loans	Lenders too
Collection agency	Handle finances	Check cashers too

Whether you're covered is a legal question -- confirm with an attorney.

Building a Compliant Program

The order that keeps it calm



Reassess risk periodically and update the program as things change.

What the Program Needs

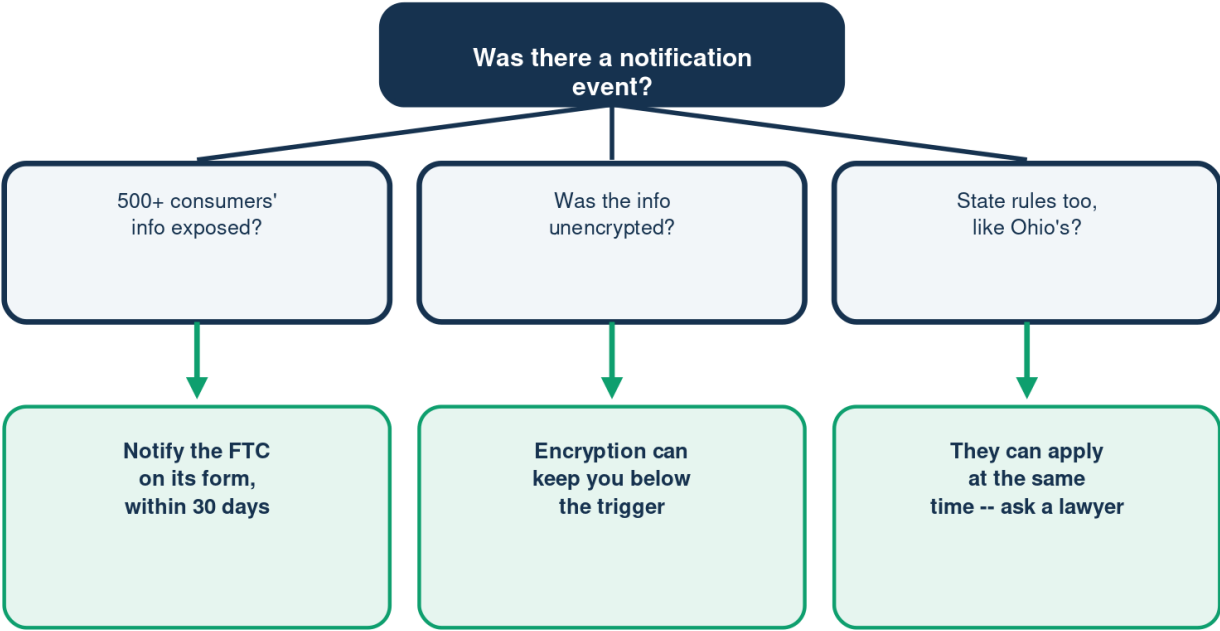
The pieces the rule expects

	In plain terms	Example
Qualified person	One person owns it	Often the owner
Safeguards	MFA, encryption	Access, backups
Oversight	Monitor + test	Train, vendors
Incident plan	Who to call	The 30-day clock

Core amendments took effect June 9, 2023.

Must You Notify the FTC?

The breach duty took effect May 13, 2024



Notify as soon as possible, no later than 30 days after discovery.

Illustration - a schematic, not to scale. Your setup may differ.



Need a Real Person?

You do not have to remember all of it.
You just have to remember you can call.
Friendly, in-person tech help -- I come to you.

BILL'S PROMISE

If you are not 100% happy with a visit, I will make it right -- or refund it. No awkwardness, no fine print. That is how I would want to be treated.

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



A Note From Bill

A quick note from Bill.

I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —
billshometech.com/book

Use of these guides is subject to our Terms of Use (billshometech.com/terms-of-use).

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech