

INSIGHTS, THE MAP ITSELF

The notification clock map, on one page and behind nothing.

The whole map: no form, no address collected, nothing gated. Each row gives the duty, what starts it, its window, and who it does not reach, the column most versions leave out.

Compiled by Red Stick Solutions. Analysis by Adam Pounders, Chief Technology Officer. Published 2 September 2026. Map published 9 September 2026.

THE MAP

Fourteen duties, one row each.

Your charter, licenses and counterparties decide which rows are yours.

Who owes it	What starts it	The window	Who it does not reach
Banking organizations	DETERMINATION Determining that a notification incident has occurred, not detecting one	36 hours, to the primary federal regulator	Not credit unions. No asset size threshold, because the threshold sits in the materiality definition.
Bank service providers	DETERMINATION Determining that an incident has caused, or is reasonably likely to cause, a material disruption or degradation of covered services for four or more hours	As soon as possible, to each affected bank customer	Only providers of covered services to banking organizations. Scheduled maintenance, testing or software updates previously communicated to the bank are excluded.
Federally insured credit unions	REASONABLE BELIEF Reasonably believing a reportable cyber incident has been experienced	72 hours, to NCUA	Not banks. No size exemption. Good faith activity at the system owner's or operator's request is outside it.
NYDFS Covered Entities	DETERMINATION Determining that a cybersecurity incident has occurred, which is narrower than a cybersecurity event	72 hours, to the Superintendent	Holders of a DFS authorization only, and the 500.19(a) limited exemption does not remove this duty. Not a firm that merely lends to a New York resident.
NYDFS Covered Entities, extortion payment	PAYMENT Making an extortion payment in connection with a cybersecurity event	24 hours to the Superintendent, then a written explanation within 30 days, under 500.17(c)	Holders of a DFS authorization only. Not removed by the limited exemption.
Institutions covered by the FTC Safeguards Rule	DISCOVERY Discovering a notification event at 500 or more consumers	30 days, to the Federal Trade Commission	Not banks, savings associations or federally insured credit unions. No consumer count relieves it, but it triggers only at 500 or more.
SEC reporting companies	DETERMINATION Determining that a cybersecurity incident is material	Four business days, on Form 8-K	No application to private companies at all, which is most of this market.

Who owes it	What starts it	The window	Who it does not reach
Fannie Mae sellers and servicers	☐ IDENTIFICATION Identification, or the reasonable conclusion that an incident may have occurred	36 hours, to Fannie Mae, without undue delay	Contractual, not supervisory. Nobody outside a Fannie Mae relationship. No size threshold.
Freddie Mac Sellers and Servicers	☐ DISCOVERY Discovery of a security incident, including one affecting a third party	48 hours, to Freddie Mac	Contractual. Nobody outside that relationship. No small company exemption of any kind.
Approved Ginnie Mae Issuers	☐ DETECTION Detecting that a Significant Cybersecurity Incident may have occurred	48 hours, to Ginnie Mae	Approved Issuers, subservicers included. A document custodian or other Ginnie Mae participant confirms its own position under the current memoranda.
FHA approved mortgagees	☐ DETERMINATION Determining that a Reportable Cyber Incident has occurred, meaning one that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, the ability to originate or service FHA insured mortgages	36 hours, to the FHA Resource Center and HUD's Security Operations Center, under Mortgagee Letter 2024-23	Only FHA approved mortgagees, bank and nonbank alike. Mortgagee Letter 2024-10 and its twelve hour clock were superseded on 2 December 2024.
Insurance licensees under an enacted Model #668	☐ DETERMINATION Determining that a cybersecurity event has occurred, where the state is the domicile or home state, or 250 or more of the state's consumers are involved and a further notice or harm test is met	72 hours, to the commissioner	Only in a state that has enacted it, where the enacted text governs and states vary it. The conditions are on Insurance.
Louisiana insurance licensees	☐ DETERMINATION Determining that a cybersecurity event involving nonpublic information has occurred, where Louisiana is the domicile or home state and harm is reasonably likely, or 250 or more Louisiana consumers are involved and a further test is met	Three business days, to the Commissioner of Insurance	Only Louisiana licensees. The program exemptions do not remove it.
Anyone holding residents' personal information	☐ DISCOVERY Discovery of a breach, as each state defines one	Varies by state. Louisiana: 60 days to residents, then 10 days to the Attorney General	Follows the residency of the affected individual, not the location of the business. Triggers and exemptions vary, so no general rule of state law can be stated.

Each instrument is in full on Financial Services, Mortgage or Insurance, and dated on Sources.

WHY THE WORDS DIFFER

Which clock started, and when did it start.

The words are not synonyms, and no rule uses them loosely. One event can start one duty on one day and another two days later, with nothing changed but who concluded what.

The trigger word	The duties that start there
Detection No judgment yet	Ginnie Mae Issuers, 48 hours
Identification A counterparty's word	Fannie Mae Seller/Serviceicers, 36 hours
Discovery A defined event	Freddie Mac Seller/Serviceicers, 48 hours Safeguards Rule institutions, 30 days State breach laws, varies by state
Reasonable belief Probably occurred	Federally insured credit unions, 72 hours
Determination A threshold is met	Banks and FHA mortgagees, 36 hours. Bank service providers, as soon as possible. NYDFS and Model #668 licensees, 72 hours. Louisiana licensees, three business days. SEC reporting companies, four business days.

Earliest to latest. One event starts these duties on different days.

One event starts Ginnie Mae's clock at detection and a bank's at determination, days apart. Order, not time: indicative and not to scale.

The five words, earliest to latest		
Word	What it asks	Rows that start there
☐ DETECTION	Somebody or something noticed. No judgment yet.	Ginnie Mae
☐ IDENTIFICATION	Or a reasonable conclusion an incident may have occurred; a counterparty's word, almost as early.	Fannie Mae
☐ DISCOVERY	Later. It attaches to a defined event, not an alert.	Freddie Mac, the FTC, state breach laws
☐ REASONABLE BELIEF	Would a competent person, on what is known, conclude a defined incident probably occurred?	Credit unions
☐ DETERMINATION	The latest and most demanding: the institution concludes a defined threshold is met.	Banks and their providers, NYDFS, FHA, Model #668, Louisiana, the SEC

An extortion payment is a sixth start: an act, not a finding. None of the five is a technical question, and no tool answers one: each is a judgment made by a person, on a date, and recorded.

HOW TO USE IT

Build the composite timeline while nothing is happening.

- 1 Keep your rows,**
and the ones you do not owe, with the reason. A duty established as not yours is one decision nobody makes at speed.
- 2 Name a person against each trigger,**
not a department: who makes that judgment, the alternate, and the record they leave.

3 Rehearse the moment, not the outage.

Give the named people partial, ambiguous facts; ask whether their threshold is met. The answer may reasonably be no, and a documented no is an output.

4 Keep the timeline as it happens:

what was known, by whom and at what hour. Every duty is read against it.

No new tooling is needed; whoever owns the incident response plan writes most of it. Date your version, then read it once with counsel and once with whoever would be woken up: they find different gaps. Related: the seller servicer information security stack, Examination and Evidence Readiness for the evidence afterwards, and Cyber Defense for detection and response design.

Review area eight of the Full scope, readiness to respond, asks which of these clocks would start for you and who would make the call.