TOP NOTCH
Technology • Cybersecurity

2026

# FINANCIAL SERVICES TECHNOLOGY & CYBERSECURITY

*A PRACTICAL RESOURCE FOR BANKS, ADVISORS & ACCOUNTING FIRMS*

**In financial services, technology isn't just infrastructure. *It's client trust.***
**Enjoy this free resource from Top Notch Computers, built for firms like yours.**







## WHAT'S INSIDE

*The state of financial services IT | Key industry challenges | What changed in 2026 | A six question readiness check | Why firms choose Top Notch*

THE STATE OF FINANCIAL SERVICES IT

# EVERY TRANSACTION RUNS ON TECHNOLOGY

Every wire, every trade, every return filed, every loan decision and every client record depends on secure, reliable technology working quietly in the background. That dependence is exactly why financial services now sits second only to healthcare on the breach cost table, and why attackers hit this sector harder, per device, than any other industry measured.

## AVERAGE COST OF DATA BREACH BY INDUSTRY




**$6.29M**

Average cost of a financial services data breach.

**Second costliest industry, up 13% in a single year**

Financial services climbed from $5.56M as costs rose across every sector studied.

**One in four malicious breaches is now AI enabled**

Financial services and energy absorb the highest concentration of those attacks.

## THREE NUMBERS BEHIND THE NUMBER

**$11.5M**

The average breach cost for a US organization. More than double the global figure and a record high, driven by regulatory penalties and litigation exposure.

**132,378**

Attack attempts per device against financial services in the first half of 2026. More than double the cross sector average and the highest intensity of any industry tracked.

**76%**

The year over year rise in direct ransomware attacks on financial institutions in the first quarter of 2026, after a 30% increase the year before.

**Read the gap, not just the bar.**

A breach in financial services costs about 26% more than the average across every industry studied. That premium has almost nothing to do with the size of the institution. It is driven by regulatory exposure, class action litigation, and the simple fact that stolen financial data converts to money faster than almost anything else on the market.

*Sources: IBM Cost of a Data Breach Report 2026, conducted by Ponemon Institute across 602 organizations in 16 countries and 17 industries, covering incidents from March 2025 to February 2026. SonicWall 2026 Financial Services Protect Brief, drawn from more than one million sensors. Black Kite 2026 State of Financial Services Report.*

KEY INDUSTRY CHALLENGES

# WHERE FIRMS GET CAUGHT OUT

Four pressures account for most of what we are called in to fix. None of them arrive as a single dramatic event. They build quietly until something breaks in the middle of a closing, a filing deadline or a Monday morning wire run.

### Ransomware & Credential Theft

Direct ransomware attacks on financial institutions rose 30% in 2025, then jumped 76% year over year in the first quarter of 2026. Forty eight distinct threat groups now target the sector. Credential abuse appears somewhere in 39% of all breaches, more than any other technique, and a valid stolen login does not trip an alarm.

### Overlapping Regulation

Few sectors answer to as many rules at once: GLBA and the FTC Safeguards Rule, SEC Regulation S-P, FINRA, NYDFS Part 500, PCI DSS and IRS Publication 4557. FTC penalties reach $53,088 per violation, per day. The same framework applies to a solo tax practice that applies to a regional bank, with no size exemption.

### Wire Fraud & Credential Theft

Business email compromise cost US organizations $3.05 billion in 2025 across fewer than 25,000 reported incidents, an average north of $120,000 each. AI has sharpened it considerably. Deepfake impersonation accounted for 45% of AI driven attacks this year, and AI related complaints alone reached $893 million in losses.

### Aging & Unpatched Technology

Exploiting known vulnerabilities is now the single most common way attackers get in, at 31% of breaches. The median time to fully fix a critical vulnerability rose to 43 days, and only 26% of actively exploited vulnerabilities were remediated at all. One legacy Telnet flaw alone generated 42.2 million detection events in this sector.

COMMON BARRIERS, OUR SOLUTIONS

| THE PROBLEM | HOW WE FIX IT |
|---|---|
| **Compliance Documentation Gaps** | Risk assessments, gap analysis, written security program and policy documentation |
| **Wire & Payment Fraud Exposure** | Email security, DMARC enforcement, MFA and out of band verification controls |
| **Backup Failures** | Automated cloud and local backups with daily verification and tested restores |
| **Security Vulnerabilities** | Endpoint protection, MFA, penetration testing and patch management |
| **Core System Outages** | Proactive monitoring, redundancy planning and same day response |

*Sources: Black Kite 2026 State of Financial Services Report. Verizon Data Breach Investigations Report 2026. IBM Cost of a Data Breach Report 2026. FBI Internet Crime Complaint Center 2025 Annual Report. SonicWall 2026 Financial Services Protect Brief. Federal Trade Commission civil penalty schedule, 16 CFR 1.98.*

WHY PRACTICE SIZE IS NO PROTECTION

# IT DOES NOT TAKE A WALL STREET BANK TO BE A TARGET

The figures on the previous pages are sector averages, pulled upward by very large incidents. Targeting has moved in the opposite direction. Attackers increasingly favour community institutions, independent advisory firms and small accounting practices, not because the payout is bigger, but because the defenses are thinner and the leverage is exactly the same.

## WHAT WE SEE IN FIRMS

Investment and advisory firms overtook banks as the most targeted segment of the sector, accounting for 41.6% of ransomware disclosures in 2025 while bank disclosures fell by half.

Almost none of it is sophisticated. Attacks arrive through email and unprotected remote access far more often than through anything exotic.

Nearly two thirds of breaches still involve the human element. Phishing was the top initial attack vector this year and led to the costliest breaches of all.

## THE RISK YOU DO NO CONTROL

In August 2025 attackers reached Marquis Software Solutions, a marketing and compliance vendor, through remote access on its firewall. The institutions it served did not find out until late October.

The final count: at least 823,548 consumers across at least 80 banks and credit unions. Names, addresses, Social Security numbers, taxpayer ID numbers and financial account details.

Not one of those institutions was breached. Every one of them still had to notify.

**The part firms miss.** Third party involvement now appears in 48% of all breaches, up 60% in a single year. A vendor breach can trigger your own notification obligations even when your own systems were never touched. Every core processor, clearinghouse, custodian, payroll provider, tax platform and cloud service that handles client data is part of your attack surface, and a current written agreement with each one is not paperwork. It is the only thing that defines who is responsible when something goes wrong.

## WHAT ACTUALLY PROTECTS A FIRM THIS SIZE

**Tested Backups**
The single biggest factor in how badly ransomware hurts. With a clean, verified backup, recovery is hours instead of weeks.

**Phishing Resistant MFA**
Marquis had MFA. Attackers got past it with stolen session data. Modern MFA on every system, not just email, is the control that decides this.

**Out of Band Verification**
No wire, no payment change, no banking detail update on the strength of an email alone. One phone call to a number you already had on file.

*Sources: Black Kite 2026 State of Financial Services Report. Verizon Data Breach Investigations Report 2026. IBM Cost of a Data Breach Report 2026. State attorney general breach filings in Maine, Iowa, Texas and other states, and American Banker analysis of public disclosures, on the Marquis Software Solutions incident.*

WHAT CHANG ED FO R FINANCIAL SERVICES SECURIT Y

# THE RULES STOPPED BEING OPTIONAL

Healthcare is still waiting on a proposed HIPAA rule. Financial services is not waiting on anything. Three separate regimes finished phasing in between June 2023 and June 2026, and each one converted safeguards that used to be judgment calls into hard requirements. There is no grace period left to lean on.

| | |
|---|---|
| **SEC Regulation S-P**<br>**Fully in force**<br>**June 3, 2026** | Applies to broker dealers, registered investment advisers, funds, funding portals and transfer agents. Requires a written incident response program, customer notification within 30 days, documented oversight of service providers, and records proving all of it. Larger firms hit the same wall on December 3, 2025. |
| **NYDFS Part 500**<br>**Fully phased in**<br>**November 1, 2025** | Multi factor authentication for virtually all remote access, including cloud applications and third party platforms, plus a documented asset inventory. The first annual certification covering these controls was due April 15, 2026. NYDFS has already issued a $2 million penalty under the amended rule. |
| **FTC Safeguards Rule**<br>**Enforceable**<br>**since June 9, 2023** | Under GLBA the FTC treats tax preparers, accountants, financial advisers, mortgage brokers and lenders as financial institutions, with no size exemption. Requires a written program, a named qualified individual, MFA, encryption, vendor oversight and breach reporting. Penalties reach $53,088 per violation, per day. |

## WHAT ENFORCEMENT ACT UALLY FINDS

> **No written program.** The requirement has existed since 2003. Enforcement still finds covered firms operating without one at all.

> **Selective MFA.** Turned on for email, but not the tax software, the accounting platform or the CRM. Partial deployment does not satisfy the rule.

> **Vendor agreements with no security language.** Long standing relationships where no contract ever set a security expectation.

> **A response plan nobody knows exists.** Written once to close an audit finding, never tested, never rehearsed with the people who would use it.

**Here is what matters for your firm.** Which rules apply depends on your charter, your registrations and your state, and most firms sit under two or three at once. But the underlying controls barely differ: written program, current risk assessment, MFA, encryption, vendor oversight and a tested response plan. Get those right and you are substantially compliant under all of them.

## START WITH THESE THREE

**A current risk assessment**
Written, dated and producible on request. It is the control cited cost often when a regulator comes looking.

**MFA everywhere client data lives.**
Not just email. Every system, every remote path, every cloud application, every seasonal staff account.

**Verified vendor agreements**
Current written security terms with every vendor that touches client financial data or your network.

*Sources: SEC amendments to Regulation S-P, adopted May 2024, compliance dates December 3, 2025 and June 3, 2026. NYDFS 23 NYCRR Part 500, second amendment final provisions effective November 1, 2025. FTC Safeguards Rule, 16 CFR Part 314. FTC civil penalty schedule, 16 CFR 1.98; no inflation adjustment was issued for 2026 under OMB Memorandum M-26-11, so the 2025 amount remains in effect. IRS Publications 4557 and 5708.*

A SIX QUESTION READINESS CHECK

# ANSWER THESE BEFORE SOMEONE ELSE DOES

These are the six questions we ask on every first visit to a financial services firm, and the six an examiner or an investigator would ask after an incident. Work through them honestly. Any one you cannot answer confidently is worth a conversation.

1. **When was your last written risk assessment, and could you produce it today?**
2. **Is multi factor authentication turned on for every system that touches client financial data,not just email?**
3. **Has anyone actually tested a restore from your backups in the last 90 days?**
4. **Do you have a current inventory of every device and application connected to your network?**
5. **Do you have current written security terms with every vendor that touches client data?**
6. **If a client emailed new wire instructions this afternoon, what would your team do before sending the money?**

Most firms are further along than they expect on two or three of these, and further behind on one. Knowing which is which is the entire point.

NO COST, NO OBLIGATION

## A free risk assessment for your practice

Every firm is set up differently. Before you decide anything, let one of our specialists take a free look at where your systems stand. In under an hour you will know where your risk sits and what it would take to close the gaps. Take the findings anywhere you like, including to your current IT provider. Our only goal is that you have a clear picture.

- Network and endpoint security review
- Regulatory gap check across GLBA, SEC and state rules
- Backup and recovery verification
- Core system and application compatibility review

# Ready to see where you stand?

Call (800) 307-1249 or visit topnotchcomputers.com

**Take Assessment**

WHY TOP NOTCH COMPUTERS

# LOCAL, INDEPENDENT, AND BUILT FOR PRACTICES

### Founded in 1999
Family owned and privately held. Free from private equity and outside interests. Our priority is your success.

### 5,000+ Clients
One of the largest managed IT client bases in the region. We bring enterprise resources with a small business feel.

### One Provider Model
Computers, networking, security, cloud and support all from one qualified team. No finger pointing between vendors.

### Industry Expertise
We actively support banks, credit unions, advisory firms and accounting practices, including core system integrations, secure document platforms and GLBA compliance.

"I've been using Top Notch for years in my business. They take care of everything – networking, cybersecurity, repairs to computers, and supply our equipment. We're relatively high-maintenance customers with compliance, but If there's ever an issue the gang takes care of it. Our client are high profile and the team Top Notch has no issue cross-collaborating and working with them as needed. 5*"

***— J.J. Goode, Top Notch Client***

# THANK YOU

**For considering Top Notch Computers. We hope this guide gives a better understanding of how important cybersecurity and technology services are for your firm.**




**Questions about anything in this guide?**
Call us. There is no charge for a conversation and no obligation to become a client.

(800) 307-1249

topnotchcomputers.com

Local IT Company serving Richmond, Charlottesville, & Falls Church Virginia