FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

FTC Report Number
202621072

Consumer Report To The FTC

The FTC cannot resolve individual complaints, but we can provide information about next steps to take. We share your report with local, state, federal, and foreign law enforcement partners. Your report might be used to investigate cases in a legal proceeding. Please read our Privacy Policy to learn how we protect your personal information, and when we share it outside the FTC.

About you

Name: Jacob Koch

Email: jako@easypcs.us

Address: 110 Stolze Dr

Phone: 618-567-8299

City: East Alton **State:** Illinois **Zip Code:** 62024--183

Country: USA

What happened

MISLEADING & DECEPTIVE ADVERTISING Submitted to: Federal Trade Commission, Bureau of Consumer Protection Category: Deceptive Practices → False Advertising / Material Omissions Primary Company: Amazon Web Services Additional Companies: Microsoft Azure, Google Cloud Platform, Yahoo, Oracle Cloud, IBM Cloud, Rackspace, VMware, Adobe Creative Cloud, Dropbox, Salesforce, Alibaba Cloud, Tencent Cloud COMPLAINT BODY SUBJECT: Industry-Wide Material Omission – Warrantless Government Access Under Section 702 of FISA STATEMENT OF FACTS Each of the above companies markets cloud services using terms like "secure," "enterprise-grade encryption," and "military-grade security." None discloses that Section 702 of FISA authorizes warrantless FBI/NSA searches of customer data stored by U.S. providers. A reasonable consumer hearing "secure" would not know their data can be searched without a warrant. This omission is material and deceptive under 15 U.S.C. § 45(a). These companies also market NIST-certified encryption (e.g., Dual_EC_DRBG) as a security feature, while failing to disclose that those standards contain an NSA-inserted backdoor – exploitable by both government agencies and criminal hackers. EVIDENCE OF A VIABLE ALTERNATIVE The undersigned developed Entangled Cyclical Encryption Architecture (ECEA) – Patent #63/716,466 – which has: No backdoors, no reliance on compromised NIST standards No statistical patterns (independently verified) Been submitted to the NSA and BIS (they have the source code) Over 2,000 independent challenge participants at 64-bit strength – zero breaks A public white paper ECEA proves backdoor-free encryption is possible. The industry's omission of Section 702 is not a technical necessity – it is a conscious choice to deceive. REQUESTED ACTION The FTC should: Investigate each company for deceptive practices under 15 U.S.C. § 45(a) regarding the omission of Section 702 access. Issue an industry-wide rule requiring any provider using the word "secure" to clearly disclose: warrantless search capability, inability to notify customers, and citation to 50 U.S.C. § 1881a. Promote backdoor-free architectures (like ECEA) as a benchmark for truthful "secure" claims. Impose retroactive penalties paid back to consumers for years of deceptive marketing. SUBMITTER CERTIFICATION I declare under penalty of perjury that the foregoing is true and correct. Supporting documentation available upon request. Signed, Jacob Koch, CEO – Perfect Computing Solutions, Inc. Date: 06/05/2026

How it started

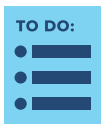
Date fraud began:	Amount I was asked for:	Amount I Paid:
Payment Used:		How I was contacted:
		Website or App

Details about the company, business, or individual

Company/Person		
Name: Listed in complaint above		
Address Line 1:	Address Line 2:	City:

Company/Person		
State:	Zip Code:	Country:
Email Address:		
Phone:		
Website:		
Name of Person You Dealt With:		

Your Next Steps



General Advice:

- You can find advice and learn more about bad business practices and scams at consumer.ftc.gov.
- If you're concerned that someone might misuse your information, like your Social Security, credit card, or bank account number, go to IdentityTheft.gov for specific steps you can take.
- Learn more about impersonation scams at ftc.gov/impersonators. If someone says they are with the FTC, know that the FTC will never demand money, make threats, tell you to transfer money, or promise you a prize.

What Happens Next

Thank you for reporting!

- We can't resolve your individual report, but we use reports to investigate and bring cases against fraud, scams, and bad business practices.
- Your report goes into the FTC's Consumer Sentinel database, which is available to federal, state, and local law enforcement across the country.
- We use reports to spot trends, educate the public, and share data about what is happening in your community. You can learn what other people in your state or metro area are reporting by visiting ftc.gov/exploredata.
- When the FTC brings cases, we try to get money back for people. At ftc.gov/refunds you can see recent FTC cases that resulted in refunds.

Want to learn more?

- Watch this video to learn about the importance of reporting.
- Sign up for FTC Consumer Alerts at ftc.gov/ConsumerAlerts to stay connected to the FTC and learn about new scams.