Data Security: Failure is Not an Option

July 20, 2022

OLA
Online Lenders Alliance

Threat Landscape

Online Lenders Alliance

External Threats are Increasing Year over Year

Global Ransomware Damage Costs*

- **2015: $325 Million**
- **2017: $5 Billion**
- **2021: $20 Billion**
- **2024: $42 Billion**
- **2026: $71.5 Billion**
- **2028: $157 Billion**
- **2031: $265 Billion**

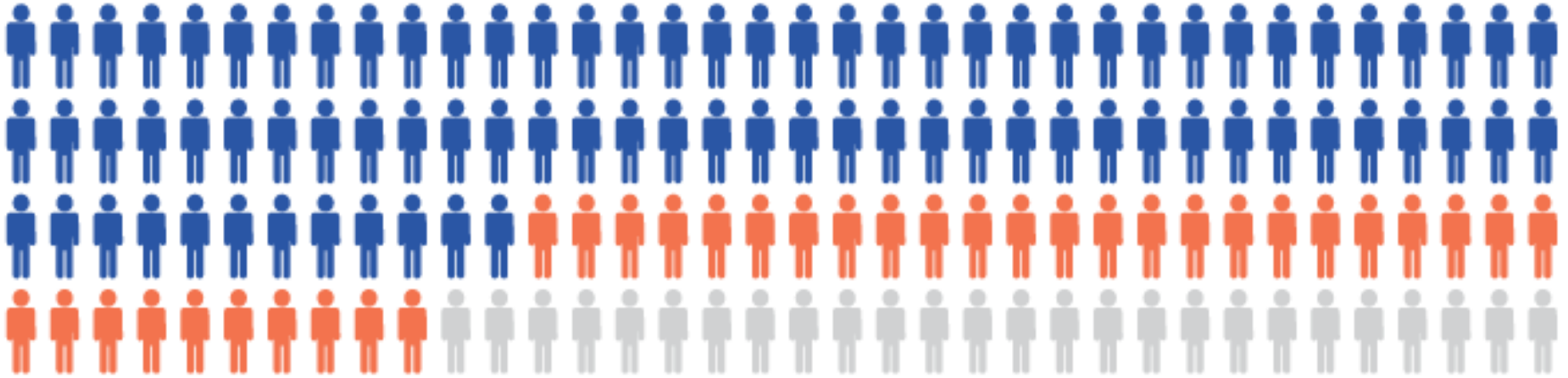
Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.

CYBERSECURITY VENTURES

* SOURCE: CYBERSECURITY VENTURES

OLA
Online Lenders Alliance

Internal Threats are Never Going Away



The negligent insider is the root cause of most incidents.

A total of 3,807 attacks, or 56%, were caused by employee or contractor negligence, costing on average $484,931 per incident. This could be the result of a variety of factors, including not ensuring their devices are secured, not following the company's security policy, or forgetting to patch and upgrade.

Malicious insiders caused 26% or 1,749 incidents at an average cost per incident of $648,062.

Malicious insiders are employees or authorized individuals who use their data access for harmful, unethical or illegal activities. Because employees are increasingly granted access to more information to enhance productivity in today's work-from-anywhere workforce, malicious insiders are harder to detect than external attackers or hackers.

Ponemon Institute 2022

Online Lenders Alliance

Data Security
Best Practices

Online Lenders Alliance

Cybersecurity and Infrastructure Security Agency Playbook

CISA Cybersecurity Incident & Vulnerability Response Playbooks (November 2021)

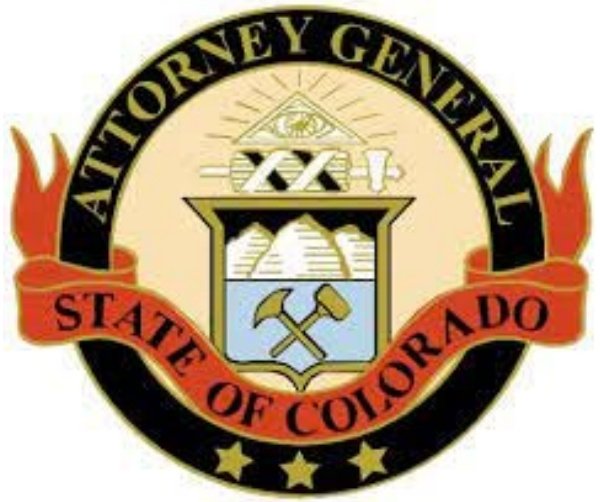
- Preparation
- Detection & Analysis
- Containment
- Eradication & Recovery
- Post-Incident Activities
- Coordination

Online Lenders Alliance

Colorado Attorney General Guidance

Data Security Best Practices (January 2022)

- Inventory the types of data collected and establish a system for how to store and manage that data.
- Develop a written information security policy.
- Adopt a written data incident response plan.
- Manage the security of vendors.
- Train your employees to prevent and respond to cybersecurity incidents.
- Follow the Department of Law's ransomware guidance to improve your cybersecurity and resilience against ransomware and other attacks.
- Timely notify victims and the Department of Law/Attorney General (when required) in the event of a security breach.
- Protect affected individuals from identity theft and other harms.
- Regularly review and update your security policies.



Data Breach / Security Incident Response

Online Lenders Alliance

UPDATED FTC GLBA Safeguards Rule

In December 2021, the Federal Trade Commission issued a final rule amending the Standards for Safeguarding Customer Information (Safeguards Rule) under the Gramm-Leach-Bliley Act.

- Requires a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in the financial institution's control. The plan must address the following:
  - (1) The goals of the incident response plan;
  - (2) The internal processes for responding to a security event;
  - (3) The definition of clear roles, responsibilities and levels of decision-making authority;
  - (4) External and internal communications and information sharing;
  - (5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
  - (6) Documentation and reporting regarding security events and related incident response activities; and
  - (7) The evaluation and revision as necessary of the incident response plan following a security event.
- Effective date: December 9, 2022

The FTC is also considering an additional rulemaking to require financial institutions to report to the FTC any security event where the financial institutions have determined misuse of customer information has occurred or is reasonably likely and at least 1,000 consumers have been affected or reasonably may be affected.

Online Lenders Alliance

State Data Breach Notification Laws

- Arizona
  - New notification requirement to state Department of Homeland Security.
- Connecticut:
  - Expanded data elements (e.g., taxpayer identification number, passport, medical, biometrics, usernames and passwords, etc.).
  - Timing requirement shortened from 90 days to 60 days.
  - New requirements for breaches of login credentials (e.g., electronic notification or to another uncompromised method, password reset, etc.).
- Maryland
  - Reasonableness standard for harm trigger.
  - 45-day notification deadline begins at discovery, not when the investigation concludes.
  - 10-day notification deadline for service providers.
  - 7-day notification deadline following a law enforcement delay.
  - New content requirements for notice to the Attorney General: number of affected individuals, a description of the breach, steps taken, and a sample consumer notice.

Online Lenders Alliance

Litigation / Enforcement Actions

Online Lenders Alliance

FTC Consent orders

In the past year, the FTC has brought numerous privacy and data security enforcement actions, including against a retail company, social media platform, and a mortgage analytics firm.

Lessons learned from these consent orders:

- Do not store Social Security numbers, passwords, or other sensitive information in clear, readable text.
- Do not retain data longer than necessary.
- Do not use data collected for security purposes for any other purposes, such as marketing.
- Utilize readily available, industry-standard security tools.
- Implement mult-factor authentication.
- Use independent third parties to assess your information security controls and data breach response plan.

Online Lenders Alliance

Questions/Discussion

If you would like to ask a question, you can ASK or type your question into the CHAT feature NOW.

Online Lenders Alliance