

Cybersecurity Law Update 2024

David G. Ries



March 5, 2024

© David G. Ries 2024. All rights reserved.



David G. Ries
Clark Hill PLC
dries@clarkhill.com

412.394.7787

The views and opinions expressed in this presentation represent the view of the author and not necessarily the official view of Clark Hill PLC. Nothing in this presentation constitutes professional legal advice nor is intended to be a substitute for professional legal advice.

Cybersecurity, Data Protection & Privacy

Leader

Melissa K. Ventrone

Director

Lara K. Forde

Connect with a professional →

For immediate assistance regarding a security incident, contact our 24/7 Breach Hotline at 877.912.9470.

www.clarkhill.com₃



Right To Know - February 2024, Vol. 14

February 12, 2024

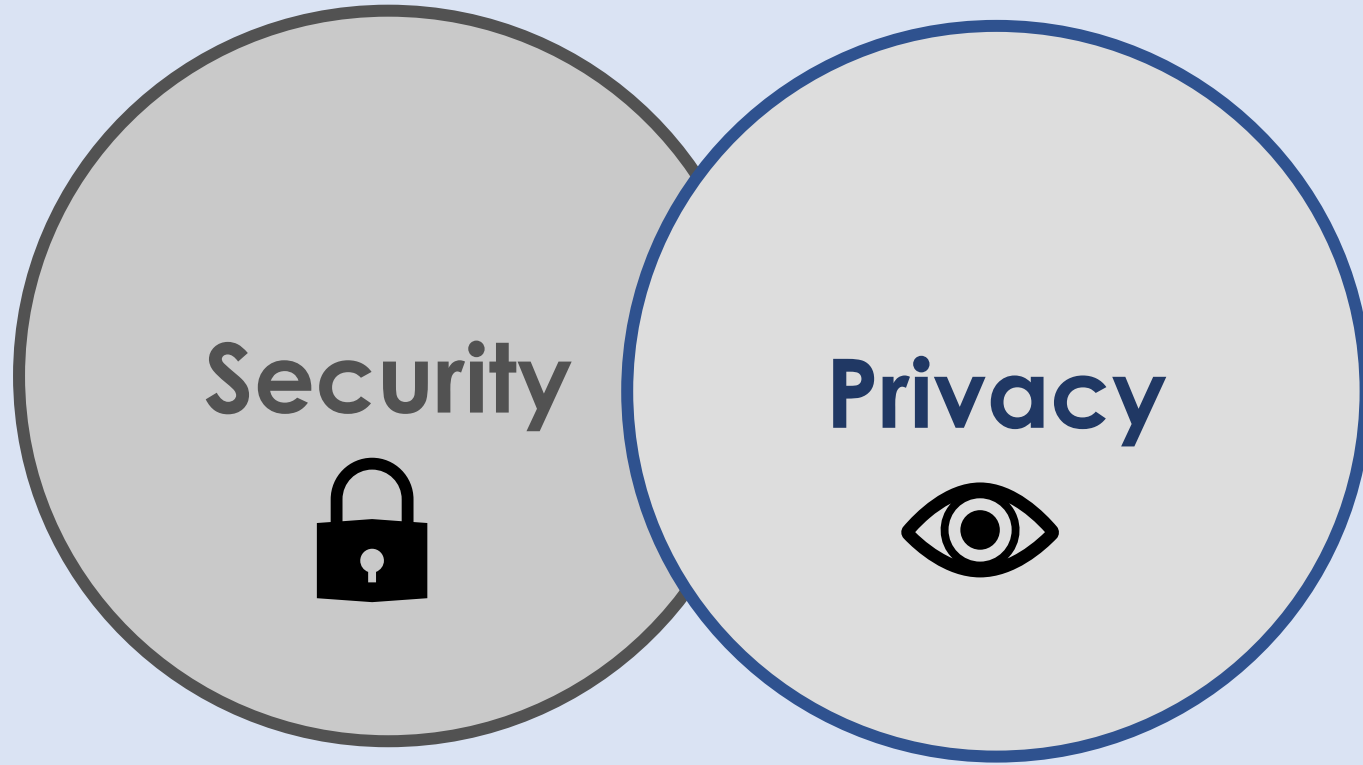
Cyber, Privacy, and Technology Report

Welcome to your monthly rundown of all things cyber, privacy, and technology, where we highlight all the happenings you may have missed.

[View previous issues and sign up to receive future newsletters by email here.](#)

State Actions:

- **New Jersey Enacts Consumer Data Protection Law:** New Jersey's consumer data protection law, [New Jersey Senate Bill – S332](#), was established on January 16, 2024, when it was signed into law by the governor. New Jersey is the first state to implement data privacy legislation in 2024. The NJDPA defines personal data as data that is “linked or reasonably linkable to an identified or identifiable individual.” The law applies to data controllers, who determine how data is processed, that are either (i) conducting business in New Jersey or (ii) that produce products or services targeted



Confidentiality
Integrity
Availability

Notice
Consent
Limited Collection
Restricted Access + Use
Integrity + Security

+

**U.S.
v.
Europe**



GENERATIVE AI REVOLUTION

Source: Shutterstock

Sanctions ordered for lawyers who relied on ChatGPT artificial intelligence to prepare court brief

A federal judge said the fines are meant to serve as deterrent in the era of artificial intelligence tools that are already giving way to legal fabrications.

JOSH RUSSELL / June 22, 2023



New York attorney Steven Schwartz leaves Manhattan Federal Court after a June 8, 2023, hearing in which he apologized for using the AI chatbot ChatGPT to generate bogus case citations for legal research. (Josh Russell/Courthouse News Service)

THE BIG FRAUD —

Deepfake scammer walks off with \$25 million in first-of-its-kind AI heist

Hong Kong firm reportedly tricked by simulation of multiple people in video chat.

BENJ EDWARDS - 2/5/2024, 10:54 AM



Getty Images / Benj Edwards

[Enlarge](#)

2017 FUTURES CONFERENCE

RUNNING *WITH THE* ***MACHINES***

ARTIFICIAL INTELLIGENCE IN THE PRACTICE OF LAW



October 26-27 | Georgia State University College of Law

Presented By The College Of Law Practice Management
In Partnership With Georgia State University College Of Law



2017 FUTURES CONFERENCE

ARTIFICIAL INTELLIGENCE

- Cybersecurity & Privacy
- Laws and Regulations
- Terms of Service
- Policies & Procedures
- Contracts
- Liability
- IP / Ownership / Attribution
- Deepfakes

Source: Shutterstock

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence



BRIEFING ROOM

PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to

Oct. 30, 2024

An official website of the United States government
[Here's how you know](#)

Information Technology

ARTIFICIAL INTELLIGENCE

Overview

Artificial Intelligence (AI) is rapidly transforming our world. Remarkable surges in AI capabilities have led to a wide range of innovations including autonomous vehicles and connected Internet of Things devices in our homes. AI is even contributing to the development of a brain-controlled robotic arm that can help a paralyzed person feel again through complex direct human-brain interfaces. These new AI-enabled systems are revolutionizing and benefitting nearly all aspects of our society and economy – everything from commerce and healthcare to transportation and cybersecurity. But the development and use of the new technologies it brings are not without technical challenges and risks.

On October 30, President Joseph R. Biden signed an Executive Order (EO) to build U.S. capacity to evaluate and mitigate the risks of Artificial Intelligence (AI) systems to ensure safety, security, and trust, while promoting an innovative, competitive AI ecosystem that supports workers and protects consumers. [Learn more about NIST's responsibilities in the EO](#) and the creation of the [U.S. Artificial Intelligence Safety Institute](#), including the new consortium that is being established.

FEATURED CONTENT

- Executive Order on Safe, Secure, and Trustworthy AI
- U.S. Artificial Intelligence Safety Institute
- AI Risk Management Framework
- AI Resource Center
- Fundamental AI Research
- Applied AI Research
- AI Standards
- AI Measurement and Evaluation
- AI Policy Contributions
- AI Engagement
- Related Links

NIST AI 100-1


Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST

<https://www.nist.gov/artificial-intelligence>

An official website of the United States government [Here's how you know](#)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY  **AMERICA'S CYBER DEFENSE AGENCY**

Search

Topics ▾ Spotlight Resources & Tools ▾ News & Events ▾ Careers ▾ About ▾ [REPORT A CYBER ISSUE](#)

[Home](#) / [Topics](#) / [Cybersecurity Best Practices](#) SHARE: [f](#) [x](#) [in](#) [m](#)

Artificial Intelligence

The security challenges associated with AI parallel cybersecurity challenges associated with previous generations of software that manufacturers did not build to be [secure by design](#), putting the burden of security on the customer. Although AI software systems might differ from traditional forms of software, fundamental security practices still apply.

As noted in the landmark [Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence \(AI\),"](#) signed by the President on October 30, 2023, "AI must be safe and secure." As the nation's cyber defense agency and the national coordinator for critical infrastructure security and resilience, CISA will play a key role in addressing and managing risks at the nexus of AI, cybersecurity, and critical infrastructure.

CISA's Roadmap for Artificial Intelligence

CISA has developed a Roadmap for Artificial Intelligence, which is a whole-of-agency plan aligned with national AI strategy, to address our efforts to: promote the beneficial uses of AI to enhance cybersecurity capabilities, ensure AI systems are protected from cyber-based threats, and deter the malicious use of AI capabilities to threaten the critical infrastructure Americans rely on every day.

CISA will implement the Roadmap through five lines of effort:

WHITE HOUSE FACT SHEET

FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

[READ HERE](#) [↗](#)

LATEST NEWS

Director Easterly and CSE Director Khoury Discuss AI on CBC Power and Politics

[WATCH THE VIDEO](#) [↗](#)

DHS INFORMATION

DHS AI: [Artificial Intelligence at DHS | Homeland](#)

CISA

www.cisa.gov/ai

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC MAKES AI-GENERATED VOICES IN ROBOCALLS ILLEGAL

State AGs Will Now Have New Tools to Go After Voice Cloning Scams

WASHINGTON, February 8, 2024—Today the Federal Communications Commission announced the unanimous adoption of a Declaratory Ruling that recognizes calls made with AI-generated voices are “artificial” under the Telephone Consumer Protection Act (TCPA). The ruling, which takes effect immediately, makes voice cloning technology used in common robocall scams targeting consumers illegal. This would give State Attorneys General across the country new tools to go after bad actors behind these nefarious robocalls.

“Bad actors are using AI-generated voices in unsolicited robocalls to extort vulnerable family members, imitate celebrities, and misinform voters. We’re putting the fraudsters behind these robocalls on notice,” said **FCC Chairwoman Jessica Rosenworcel**. “State Attorneys General will now have new tools to crack down on these scams and ensure the public is protected from fraud and misinformation.”

The rise of these types of calls has escalated during the last few years as this technology now has the potential to confuse consumers with misinformation by imitating the voices of celebrities, political candidates, and close family members. While currently State Attorneys Generals can target the outcome of an unwanted AI-voice generated robocall—such as the scam or fraud they are seeking to perpetrate—this action now makes the act of using AI to generate the voice in these robocalls itself illegal, expanding the legal avenues through which state law enforcement agencies can hold these perpetrators accountable under the law.

In November of 2023, the FCC launched a Notice of Inquiry to build a record on how the agency can combat illegal robocalls and how AI might be involved. The agency asked questions on how AI might be used for scams that arise out of junk calls, by mimicking the voices of those we know, and whether this technology should be subject to oversight under the TCPA. Similarly, the FCC also asked about how AI can help us with pattern recognition so that we turn this technology into a force for good that can recognize illegal robocalls before they ever reach consumers on the phone.

The Telephone Consumer Protection Act is the primary law the FCC uses to help limit junk calls. It restricts the making of telemarketing calls and the use of automatic telephone dialing systems and artificial or prerecorded voice messages. Under FCC rules, it also requires telemarketers to obtain prior express written consent from consumers before robocalling them. This Declaratory Ruling ensures AI-generated voices in calls are also held to those same standards.

The TCPA gives the FCC civil enforcement authority to fine robocallers. The Commission can also take steps to block calls from telephone carriers facilitating illegal robocalls. In addition, the TCPA allows individual consumers or an organization to bring a lawsuit against robocallers in

FCC

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC MAKES AI-GENERATED VOICES IN ROBOCALLS ILLEGAL

State AGs Will Now Have New Tools to Go After Voice Cloning Scams

Feb. 8, 2024



[Home](#) / [News and Events](#) / [News](#) / [Press Releases](#)

For Release

FTC Proposes New Protections to Combat AI Impersonation of Individuals

Agency finalizes rule banning government and impersonation fraud and seeks to extend protections to individuals

February 15, 2024 | [f](#) [t](#) [in](#)

Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Imposter](#) | [government](#) | [deceptive/misleading conduct](#) | [Technology](#) | [Advertising and Marketing](#) | [Tech](#) | [Artificial Intelligence](#)

The Federal Trade Commission is seeking public comment on a [supplemental notice of proposed rulemaking](#) that would prohibit the impersonation of individuals. The proposed rule changes would extend protections of the [new rule on government and business impersonation](#) that is being

Related actions

[Proposed Amendments to Trade Regulation Rule on Impersonation of Government and Businesses](#)

[16 CFR Part 461: Trade Regulation Rule on Impersonation of Government](#)

FTC

Final Rule:
Prohibit impersonation of government and business

Proposed Rule:

- Prohibit impersonation of individuals**
- Provide for liability of AI platforms**

Feb. 15, 2024

USING AI RESPONSIBLY: U.S. LEADS EFFORTS TO DEVELOP ISO/IEC 42001, ARTIFICIAL INTELLIGENCE MANAGEMENT SYSTEM STANDARD

12/27/2023

NEW STANDARD NOW AVAILABLE FOR PURCHASE VIA ANSI WEBSTORE

A new international standard provides guidance for organizations of all kinds to use artificial intelligence (AI) systems responsibly: ISO/IEC 42001, *Artificial intelligence – Management system*, developed by the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) Joint Technical Committee (JTC) 1, *Information technology*, Subcommittee (SC) 42, *Artificial intelligence*. The U.S. has a leading role in JTC 1, with the [American National Standards Institute](https://www.ansi.org/) (ANSI), the U.S. member body to ISO, serving as secretariat.

Cloud Security Alliance



Membership ▼

STAR Program ▼

Certificates & Training ▼

Research ▼



Don't forget to register for [CSA's Virtual Cloud Threats & Vulnerabilities Summit 2024](#), March 26-27!

Working Group

AI Safety Initiative

"This coalition, and the guidelines emerging from it, will set standards that help ensure AI systems are built to be secure."
- Matt Knight, Head of Security at OpenAI



Security
Implications of
ChatGPT

Download



Artificial Intelligence (AI) Training and Resources

Equipping professionals with the right training and resources to mitigate the risks and vulnerabilities to the rapid introduction of machine learning and artificial intelligence in the world.

[Resources](#)[Training Courses](#)

Trending AI News & Updates



Webcast

SANS Cyber Defense Initiative 2023: SANS@Night - Leveraging AI: A Tutorial

ChatGPT, GPT-4, Llama 2, Bard, Minerva, Megatron, Claude, Chinchilla... What exactly are these "Large Language Models" that are in the news? What are they really good for? How do they work? What are the risks when we incorporate these into our business process?

This 90 minute presentation and tutorial will explain how these models work, what transformers are, how embeddings work, and how to build a question answering AI... the easy way and the hard way.. in addition to discussing the very real risks that come into play when we try to integrate these systems into a business process!

SANS Institute

www.sans.org/mlp/ai

[Justice.gov](#) > [U.S. Attorneys](#) > [Northern District of California](#) > [Press Releases](#) > [Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records](#)

PRESS RELEASE

Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records

Wednesday, October 5, 2022

Share



For Immediate Release

U.S. Attorney's Office, Northern District of California

Oct. 5, 2022



United States
Attorney's Office
Northern District of California

[About NDCA](#) | [Find Help](#) | [Contact Us](#)

Search



[About](#) ▾

[News](#)

[Notifications](#) ▾

[Programs](#) ▾

[Resources](#) ▾

[Employment](#)

[Contact Us](#) ▾

[Justice.gov](#) > [U.S. Attorneys](#) > [Northern District of California](#) > [Press Releases](#) > [Former Chief Security Officer Of Uber Sentenced To Three Years' Probation For Covering Up Data Breach Involving Millions Of Uber User Records](#)

PRESS RELEASE

Former Chief Security Officer Of Uber Sentenced To Three Years' Probation For Covering Up Data Breach

+ \$50,000 fine

May 5, 2023

Press Release

SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

Complaint alleges software company misled investors about its cybersecurity practices and known risks

FOR IMMEDIATE RELEASE
2023-227

Washington D.C., Oct. 30, 2023 — The Securities and Exchange Commission today announced charges against Austin, Texas-based software company SolarWinds Corporation and its chief information security officer, Timothy G. Brown, for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. The complaint alleges that, from at least its October 2019 initial public offering through the end of the period ending December 31, 2022, the company misled investors about its cybersecurity practices and known risks.

Oct. 30, 2023



Laws and Regulations

Statutes

Regulations

Guidance

Executive Orders

Federal + State

Selected Federal Laws

- **Federal Information Security Management Act (FISMA)**
Federal Information Security Modernization Act
- **Financial Industries Modernization Act (Gramm-Leach-Bliley)**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **Strengthening American Security Act of 2022**

Strengthening American Cybersecurity Act of 2022

**TITLE I—FEDERAL INFORMATION SECURITY
MODERNIZATION ACT OF 2022**

**TITLE II—CYBER INCIDENT REPORTING FOR
CRITICAL INFRASTRUCTURE ACT OF 2022**

**TITLE III—FEDERAL SECURE CLOUD
IMPROVEMENT AND JOBS ACT OF 2022**

Strengthening American Cybersecurity Act of 2022

SEC. 2242. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS

“A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.”

“A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made.”

CISA Critical Infrastructure



Chemical Sector

The Department of Homeland Security is designated as the Sector Risk Management Agency for the Chemical Sector.



Communications Sector

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. The Department of Homeland Security is the Sector Risk Management Agency for the Communications Sector.



Dams Sector

The Department of Homeland Security is designated as the Sector Risk Management Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.



Emergency Services Sector

The Department of Homeland Security is designated as the Sector Risk Management Agency for the Emergency Services Sector. The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.



Financial Services Sector

The Department of the Treasury is designated as the Sector Risk Management Agency for the Financial Services Sector.



Government Facilities Sector

The Department of Homeland Security and the General Services Administration are designated as the Co-Sector Risk Management Agencies for the Government Facilities Sector.



Information Technology Sector

The Department of Homeland Security is designated as the Sector Risk Management Agency for the Information Technology Sector.



Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.



Commercial Facilities Sector

The Department of Homeland Security is designated as the Sector Risk Management Agency for the Commercial Facilities Sector, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.



Critical Manufacturing Sector

The Department of Homeland Security is designated as the Sector Risk Management Agency for the Critical Manufacturing Sector.



Defense Industrial Base Sector

The U.S. Department of Defense is the Sector Risk Management Agency for the Defense Industrial Base Sector. The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.



Energy Sector

The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector Risk Management Agency for the Energy Sector.



Food and Agriculture Sector

The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Risk Management Agencies for the Food and Agriculture Sector.



Healthcare and Public Health Sector

The Department of Health and Human Services is designated as the Sector Risk Management Agency for the Healthcare and Public Health Sector.



Nuclear Reactors, Materials, and Waste Sector

The Department of Homeland Security is designated as the Sector Risk Management Agency for the Nuclear Reactors, Materials, and Waste Sector.



Water and Wastewater Systems Sector

The Environmental Protection Agency is designated as the Sector Risk Management Agency for the Water and Wastewater Systems Sector.

Last Updated Date: October 21, 2020



Press Release



SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

FOR IMMEDIATE RELEASE
2023-139

Washington D.C., July 26, 2023 — The Securities and Exchange Commission today adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. The Commission also adopted rules requiring foreign private issuers to make comparable disclosures.

"Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors," said SEC Chair Gary Gensler. "Currently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules will benefit investors, companies, and the markets connecting them."

The new rules will require registrants to disclose on the new Item 1.05 of Form 8-K any cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the registrant. An Item 1.05 Form 8-K will generally be due four business days after a registrant determines that a cybersecurity incident is material. The disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing.

The new rules also add Regulation S-K Item 106, which will require registrants to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats,

Related Materials


- [Final Rule](#)
- [Fact Sheet](#)

July 26, 2023

Disclose:
"material cybersecurity incident"

Within:
4 business days of determining
that the incident is material

Docket (FAR-2021-0017) / Document

 PROPOSED RULE

Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing

Posted by the **Federal Acquisition Regulation** on Oct 3, 2023


View More Documents 4


View Related Comments 81

 Share ▾

 Document Details

 Browse Posted Comments 81

 Document ID
FAR-2021-0017-0001

 Comments Received
81
[More Details ▾](#)

Content

Action

Proposed rule.

Summary

DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to partially implement an Executive order on cyber threats and incident reporting and information sharing for Federal contractors and to implement related cybersecurity policies.



[Home](#) / [News and Events](#) / [News](#) / [Press Releases](#)

For Release

FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches

Amendment will require non-bank financial institutions to report when they discover that information affecting 500 or more people has been acquired without authorization

October 27, 2023 | [f](#) [t](#) [in](#)

Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Privacy and Security](#) | [Data Security](#) | [Gramm-Leach-Bliley Act](#)

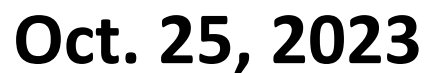
The Federal Trade Commission has approved an amendment to the Safeguards Rule that would require non-banking institutions to report certain data breaches and other security events to the agency.

Oct. 27, 2023

Related actions

[16 CFR Part 314: Standards for Safeguarding Customer Information](#)

Topics



Laws and Regulations

Federal

- Breach Notice
- Reasonable Security
- FTC Act
- Privacy

State

- Breach Notice
- Reasonable Security
- Privacy

International

- GDPR +



Source: Shutterstock

State Reasonable Security (PII)

24 states

General “reasonable security” v. detailed requirements

**MA Standards for the Protection of Personal Information
(201 CMR 17)**

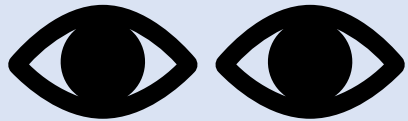
NY Stop Hacks and Improve Electronic Data Security (SHIELD) Act

State Breach Notice (PII)

50 states + DC, PR, USVI

- **Information covered**
- **Entities covered**
- **Definition of “breach”**
- **Who must be notified**
- **Risk of harm**
- **Time of notice**
- **Form or method of notice**
- **Credit monitoring**
- **Exceptions**
 - **Safe Harbor**
 - **Encryption**

Rights-Based Privacy Laws



CA Consumer Privacy Act (CCPA) + CA Consumer Privacy Rights Act (CPRA) (in effect)

VA Consumer Privacy Act (in effect)

CT Data Privacy Act (in effect)

CO Privacy Act (in effect)

UT Consumer Privacy Act (in effect)

TN Information Protection Act (effective July 1, 2024)

OR Consumer Privacy Act (effective July 1, 2024)

TX Data Privacy and Security Act (effective July 1, 2024)

MT Consumer Data Privacy Act (effective Oct. 1, 2024)

IA Consumer Data Protection Act (effective Jan. 1, 2025)

DE Personal Data Privacy Act (effective Jan. 1, 2025)

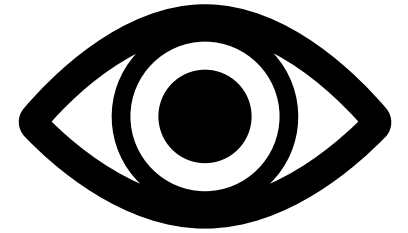
NJ (effective Jan. 15, 2025)

IN Consumer Data Protection Act (effective Jan. 1, 2026)

Biometric Privacy Laws

IL Biometric Privacy Act (BIPA)
(includes private right of action)

TX + WA
(no private right of action)



LEGISLATORS & STAFF

NCSL Is at Your Service

Your NCSL state liaison is ready for all your policy questions.



TABLE OF CONTENTS

Security Breach Laws

Additional Resources

CONTACT

Pam Greenberg

Telecommunications and
Information Technology

All Documents 

Crime

Security Breach Notification Laws

1/17/2022

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have laws requiring private businesses, and in most states, governmental entities as well, to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data or information brokers, government entities, etc.); definitions of “personal information” (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

PLEASE NOTE: NCSL serves state legislators and their staff. This site provides general comparative information only and should not be relied upon or construed as legal advice.

TABLE OF CONTENTS

Introduction

2021 Overview

2021 Consumer Data Privacy Legislation

Explanation of Categories

Additional Resources

CONTACT

Pam Greenberg

Telecommunications and Information Technology

All Documents 

Crime

Telecommunications Technology and Regulation

Privacy and Security

Information Technology and Management

2021 Consumer Data Privacy Legislation

12/27/2021



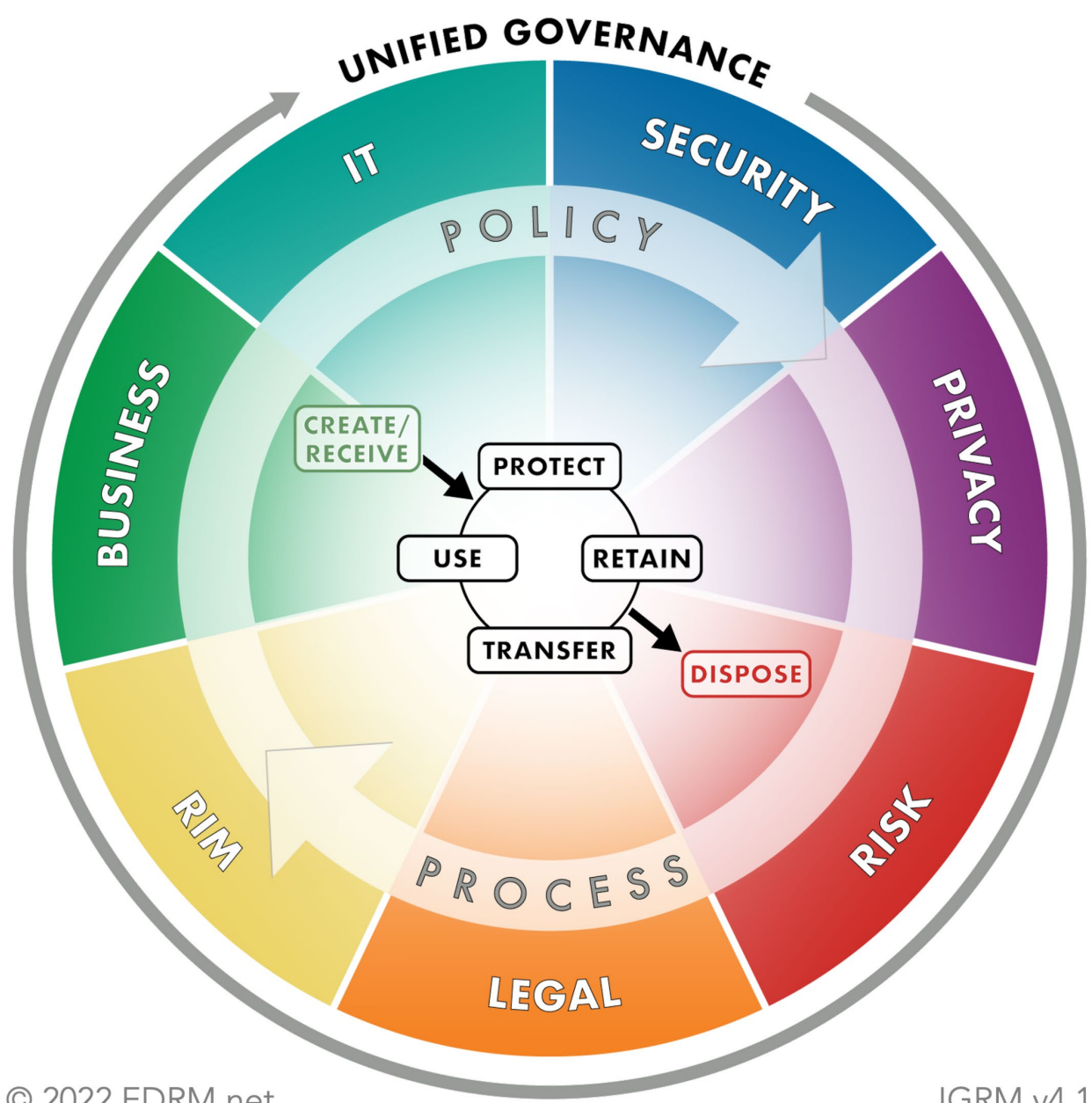
Introduction

States have long been involved in passing privacy-related laws directed at specific sectors or services, and [several states](#) have constitutional privacy provisions that give citizens greater privacy protections than the U.S. Constitution. In recent years, however, information privacy has gained momentum as a significant issue in state legislatures.

Online commerce sites, social media, and mobile devices and apps are becoming an integral part of consumers' lives. They improve consumer access to information and make shopping and purchases faster and easier. Smart

Information Governance Reference Model (IGRM)

Balancing Value, Risk and Cost

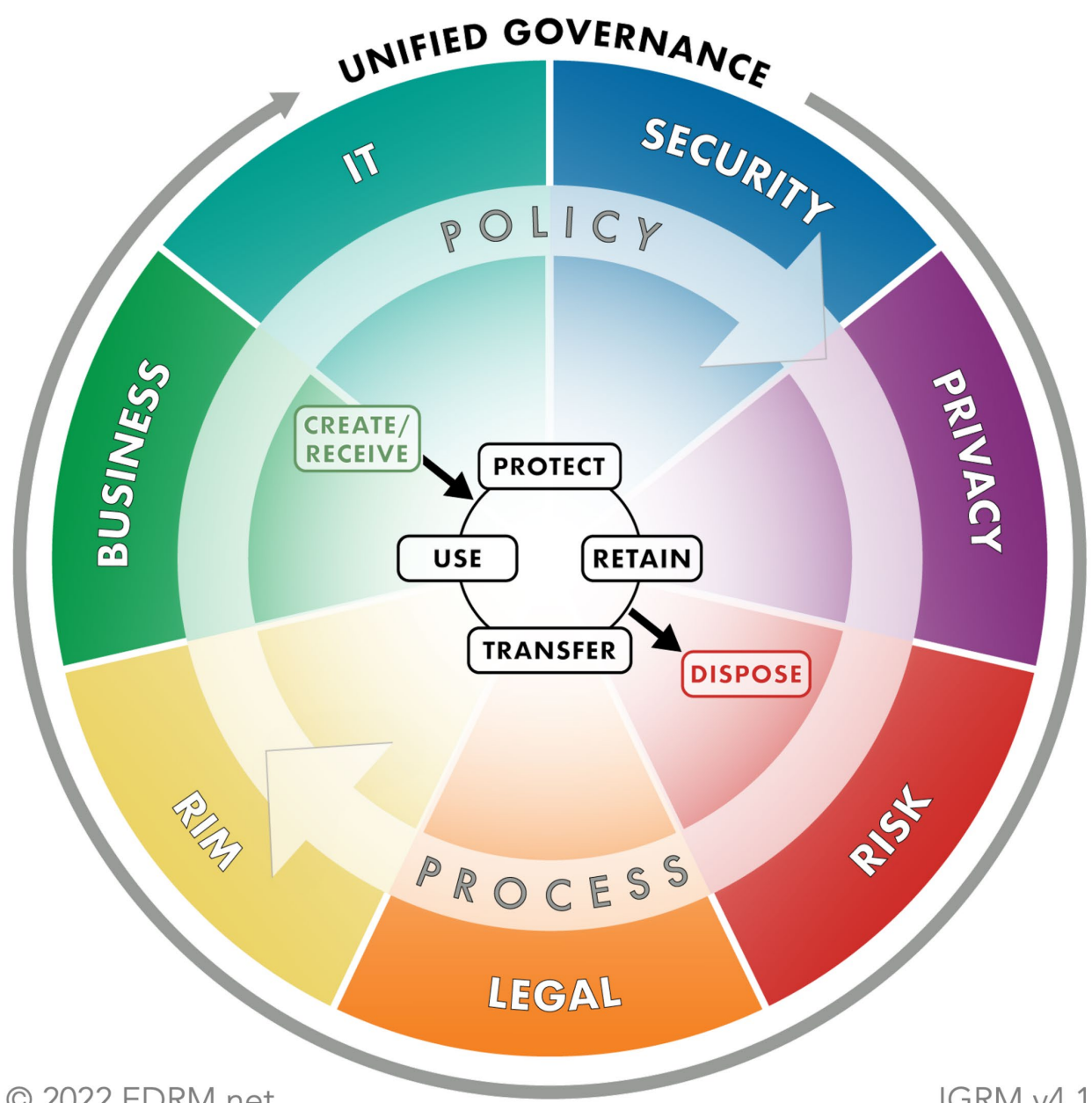


Information Governance

Manage life cycle of information from creation or receipt through final disposition

Information Governance Reference Model (IGRM)

Balancing Value, Risk and Cost



Manage and Minimize Data

Inventory of Technology and Data
- Data Map

Classify Data

Minimize Collection and Retention

Secure Disposal

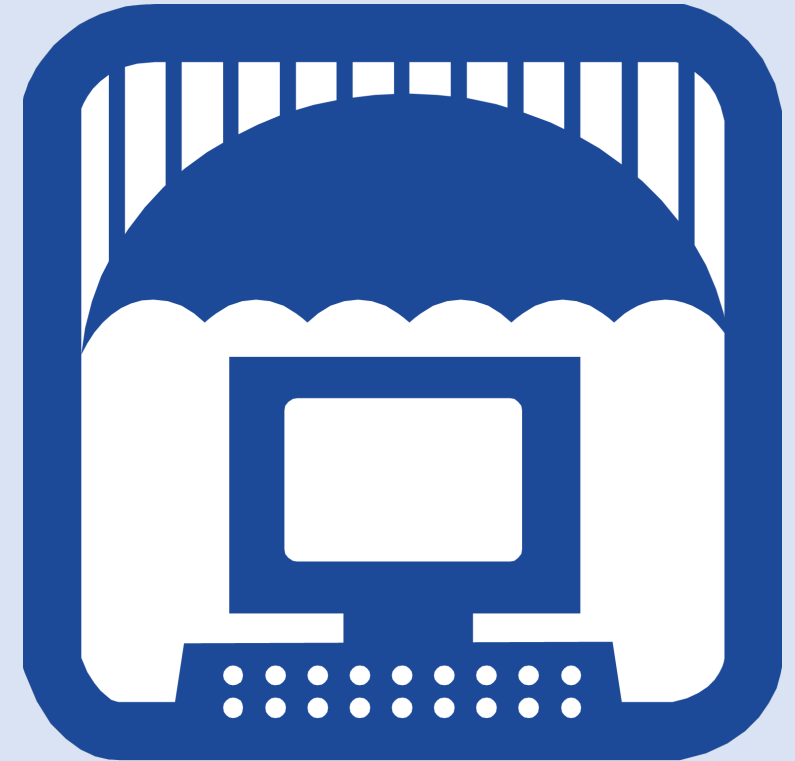
Risk-based

Policies

Training

Review and update

Constant security awareness



Comprehensive Cybersecurity Program



What is “Reasonable Security”?

Source: Shutterstock

Standards / Frameworks / Controls



NIST Cybersecurity Framework

NIST Special Publication 800-53, Rev 5
+ numerous additional standards

ISO 27000 series standards:



Information Security Management Systems

Center for Internet Security
CIS Controls, Version 8

NEWS

NIST Releases Version 2.0 of Landmark Cybersecurity Framework

The agency has finalized the framework's first major update since its creation in 2014.

February 26, 2024

- NIST's cybersecurity framework (CSF) now explicitly aims to help all organizations — not just those in critical infrastructure, its original target audience — to manage and reduce risks.
- NIST has updated the CSF's core guidance and created a suite of resources to help all organizations achieve their cybersecurity goals, with added emphasis on governance as well as supply chains.
- This update is the outcome of a multiyear process of discussions and public comments aimed at making the framework more effective.



More roads lead to NIST's updated cybersecurity framework, which now features quick-start guides aimed at specific audiences, success stories outlining other organizations' implementations, and a searchable catalog of informative references that allows users to cross-reference the framework's guidance to more than 50 other cybersecurity documents.

Credit: N. Hanacek/NIST

👤 MEDIA CONTACT

Chad Boutin
charles.boutin@nist.gov 📧
(301) 975-4261

🏢 ORGANIZATIONS

Information Technology Laboratory
Applied Cybersecurity Division
Applied Cybersecurity - HQ

SIGN UP FOR UPDATES FROM NIST

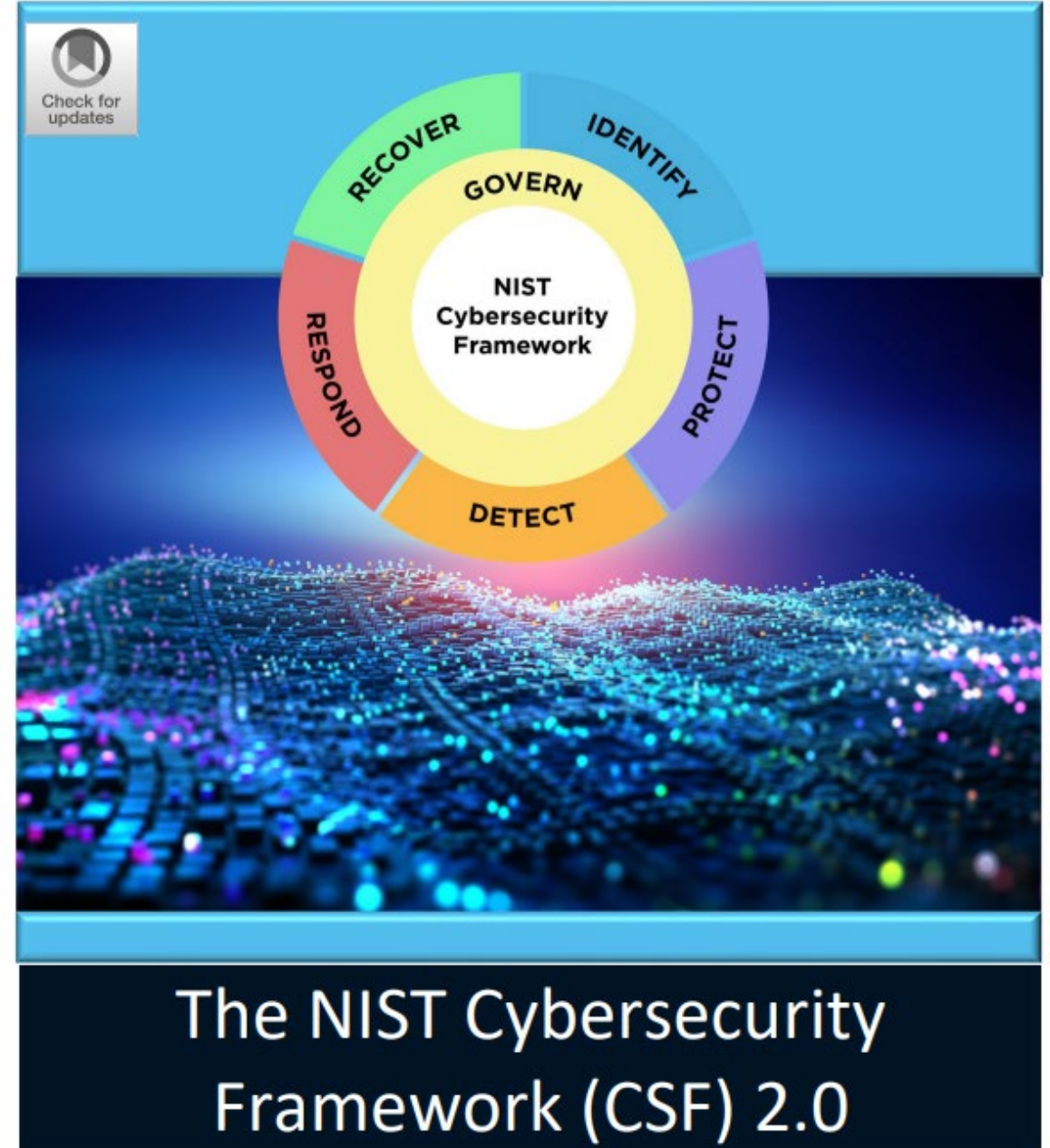
Enter Email Address

Sign up

Feb. 26, 2024



Fig. 2. Framework Functions



The Numbers

“Over 90% of successful cyber attacks start with a phishing email.”



CISA Oct. 2021

Verizon 2023



74% of breaches included a human element.

Basic security hygiene still protects against

98%
of attacks



Require phishing-resistant multifactor authentication (MFA)



Apply Zero Trust principles



Use modern anti-malware




Keep up to date on software



Protect data

Microsoft
Sept. 2023

Multifactor Authentication

 Microsoft

Microsoft Security

Solutions ▾

Products ▾


Services ▾

Partners


Resources ▾


Contact Sales


Start free trial




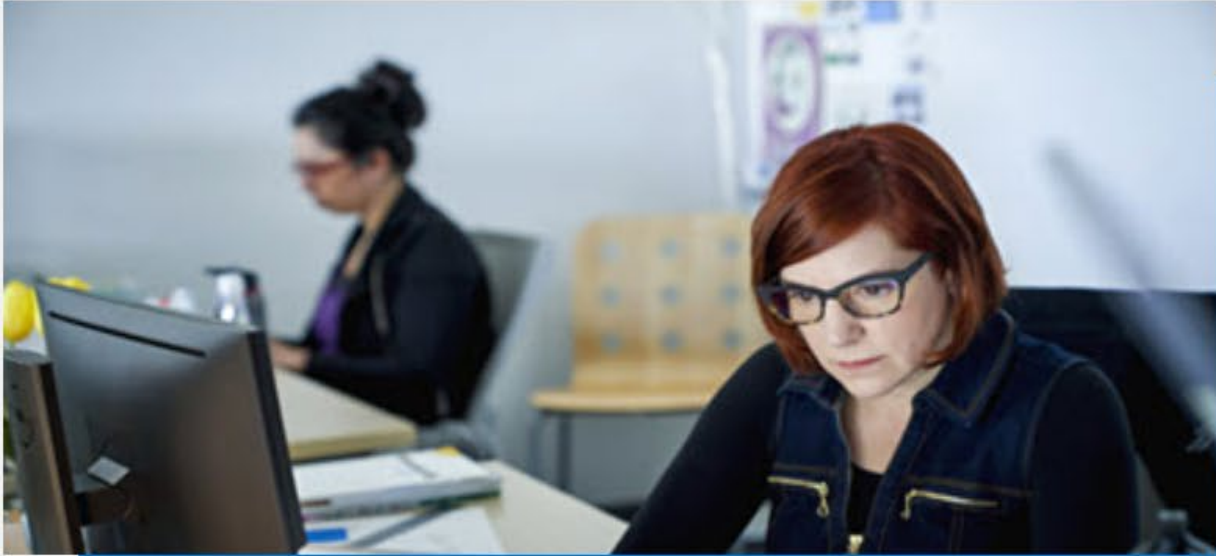
All Microsoft ▾

Search 

Light  Dark

 [Blog home](#) / Identity and access management

Search the blog 



[News](#) [Identity and access management](#) [Threat actors](#) · 2 min read

One simple action you can take to prevent 99.9 percent of attacks on your accounts

By [Melanie Maynes](#), Senior Product Marketing Manager, Microsoft Security

Microsoft (Aug. 2019)



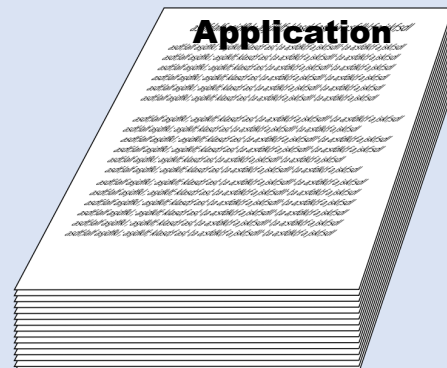
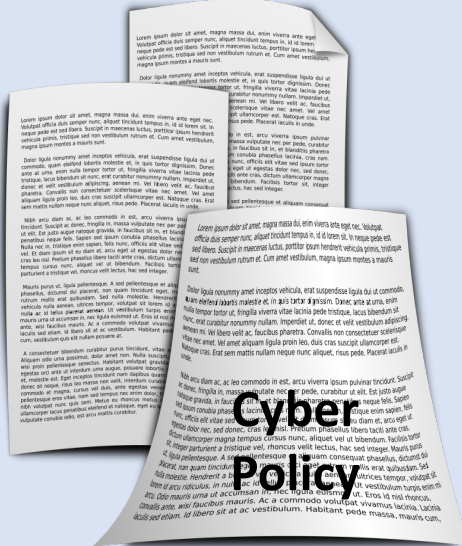
Source: Shutterstock

Risk Management Process

- Assess the risks.
- Manage the risks:
 - Eliminate the risk.
 - Control the risk with appropriate administrative, technical and physical safeguards.
 - Transfer the risk (insurance, indemnity, etc.).
 - Accept the risk.
- Often a combination of approaches.

Cyber Insurance

Source: Shutterstock



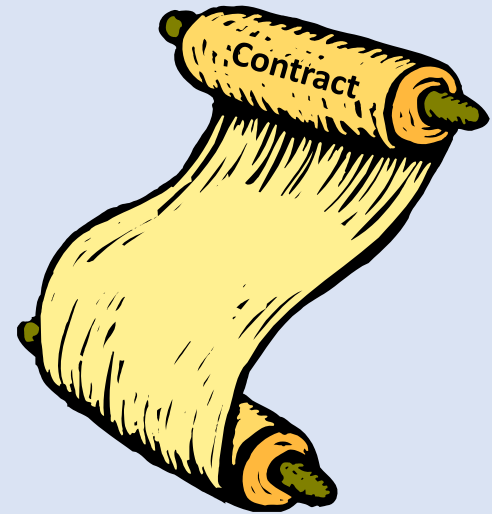
Contracting for Security

“Reasonable security”

Detailed requirements

Incorporate standards or frameworks

Include third-party / supply chain



OFAC Sanctions



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹

Date: September 21, 2021



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.²

Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.

This advisory describes the potential sanctions risks associated with making and facilitating ransomware payments and provides information for contacting relevant U.S. government agencies, including OFAC if there is any reason to suspect the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.³

Background on Ransomware Attacks

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims' sensitive files. The cyber actors then demand a

¹ This advisory is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive, or as imposing requirements under U.S. law, or otherwise addressing any requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

² This advisory updates and supersedes OFAC's *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* of October 1, 2020.

³ This advisory is limited to sanctions risks related to ransomware and is not intended to address issues related to information security practitioners' cyber threat intelligence-gathering efforts more broadly. For guidance related to those activities, see guidance from the U.S. Department of Justice, *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources* (February 2020), available at <https://www.justice.gov/criminal-ccips/page/file/1252341/download>.



U.S. DEPARTMENT OF THE TREASURY

ABOUT TREASURY POLICY ISSUES DATA SERVICES **NEWS**

HOME > NEWS > PRESS RELEASES

NEWS

Press Releases

Statements & Remarks

Readouts

Testimonies

Featured Stories

Webcasts

Press Contacts

PRESS RELEASES

United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group

February 20, 2024

The United States imposes sanctions on affiliates of group responsible for ransomware attacks on the U.S. financial sector

WASHINGTON — Today, the United States is designating two individuals who are affiliates of the Russia-based ransomware group LockBit. This action is the first in an ongoing collaborative effort with the U.S. Department of Justice, Federal Bureau of Investigation, and our international partners targeting LockBit.

“The United States will not tolerate attempts to extort and steal from our citizens and institutions,” said Deputy Secretary of the Treasury Wally Adeyemo. “We will continue our whole-of-government approach to defend against malicious cyber activities, and will use all available tools to hold the actors that enable these threats accountable.”

Russia continues to offer safe harbor for cybercriminals where groups such as LockBit are free to launch ransomware attacks against the United States, its allies, and partners. These ransomware attacks have targeted critical infrastructure, including hospitals, schools, and financial institutions. Notably, LockBit was responsible for the November 2023 ransomware attack against the Industrial and Commercial Bank of China's (ICBC) U.S. broker-dealer. The United States is a global leader in the fight against cybercrime and is committed to using all available authorities and tools to defend Americans from cyber threats. In addition to the actions announced today, the U.S. government provides critical resources to support potential victims in protecting against and responding to ransomware attacks. For example, last year, the Cybersecurity & Infrastructure Security Agency in conjunction with other U.S. Departments and Agencies and foreign partners published two cybersecurity advisories, “[Understanding Ransomware Threat Actors: LockBit](#)” and “[LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability](#).” These



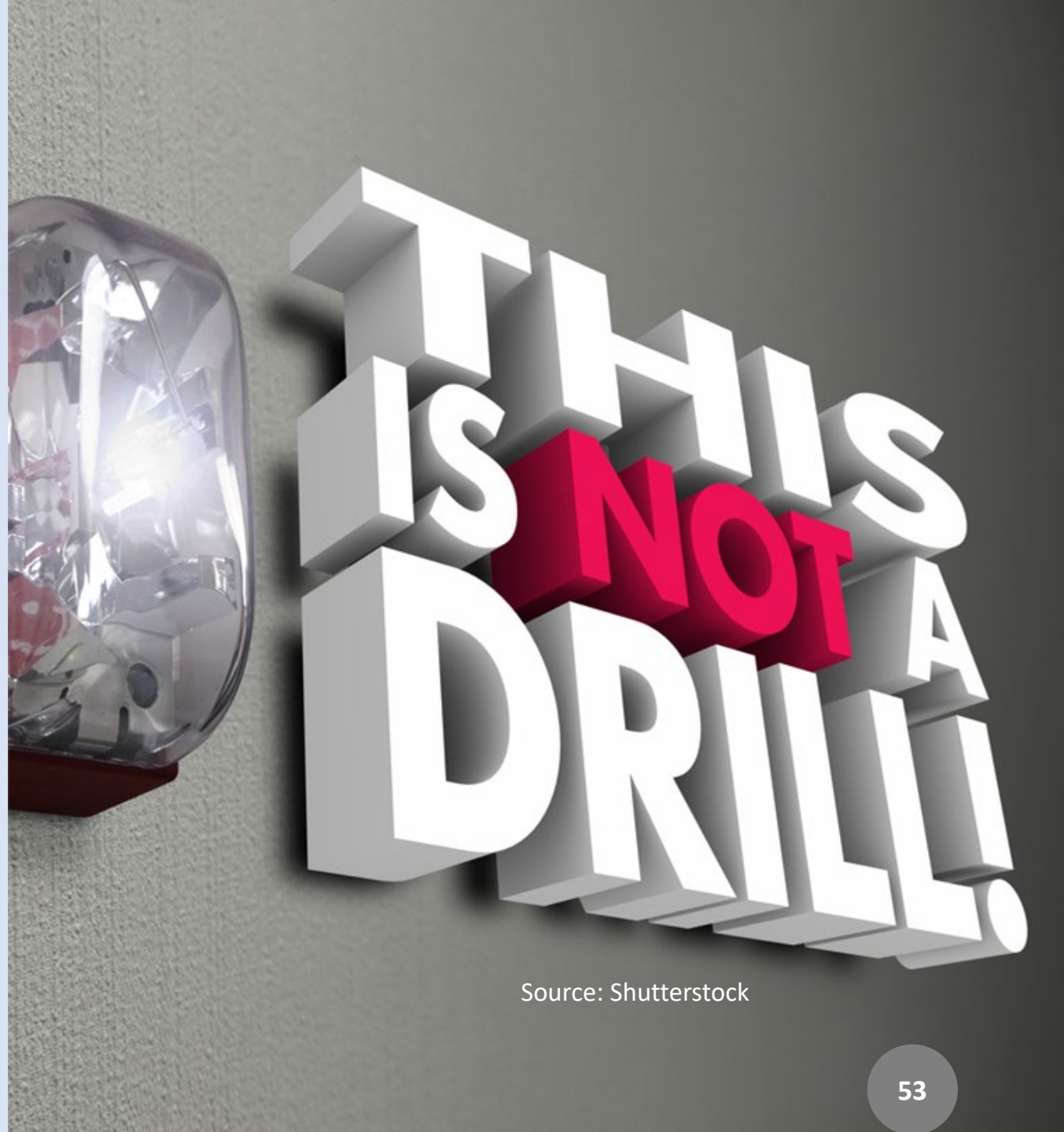
Feb. 20, 2024

Incident Response Plans

Preparing for when a business will be breached, not if it may be breached

The new mantra in security:

Identify & Protect + Detect,
Respond & Recover



Source: Shutterstock

Is it a “Data Breach”?

“event”

“incident”

“major incident”

“data breach”



Source: Shutterstock

HIPAA: “The acquisition, access, use, or disclosure of protected health information in a manner not permitted which compromises the security or privacy of the protected health information.”

Who You Gonna Call?

FBI

IC3

Secret Service

CISA

State & Local Police



Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to



A
PLAINT

CONSUMER
ALERTS

INDUSTRY
ALERTS

BEC

RANSOMWARE

ELDER
FRAUD

SCAMS



FEDERAL BUREAU OF INVESTIGATION

Internet Crime Complaint Center IC3



Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant.

[File a Complaint](#)



Internet Crime Complaint Center (IC3)

What is BEC?

Business Email Compromise is a sophisticated scam targeting both businesses and individuals performing a transfer of funds. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques resulting in an unauthorized transfer of funds.

1. Contact the originating Financial Institution as soon as fraud is recognized to request a recall or reversal as well as a Hold Harmless Letter or Letter of Indemnity.
2. File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
3. Visit www.ic3.gov for updated PSAs regarding BEC trends as well as other fraud schemes targeting specific populations (real estate, pre-paid cards, W-2, etc.).
4. Never make any payment changes without verifying with the intended recipient; verify email addresses are accurate when checking mail on a cell phone or other mobile device.

[File a BEC Complaint](#)

[File a BEC Complaint](#)

RAT SUCCESSES⁶

Success to Date

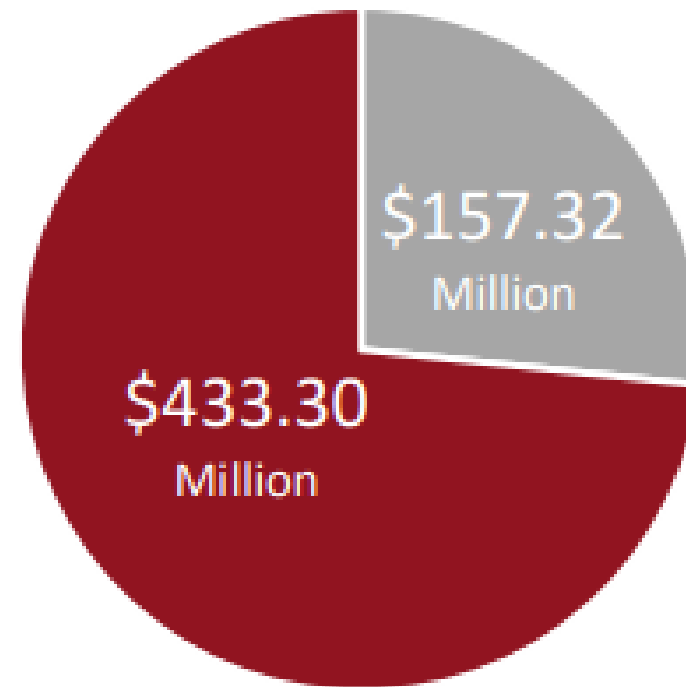
73% Success Rate

2,838 Incidents

\$590.62 Million Losses

\$433.30 Million Frozen

■ Remaining Losses ■ Frozen Funds



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**

Search

us-cert.cisa.gov[Report Cyber Issue](#)

CYBERSECURITY

INFRASTRUCTURE
SECURITYEMERGENCY
COMMUNICATIONSNATIONAL RISK
MANAGEMENTABOUT
CISA

MEDIA

[Cybersecurity](#) > [Cyber Incident Response](#)

Cybersecurity

[Cybersecurity Training & Exercises](#)[Cybersecurity Summit 2020](#)[Cyber QSMO Marketplace](#)[Combating Cyber Crime](#)[Securing Federal Networks](#)[Protecting Critical Infrastructure](#)[Cyber Incident Response](#)[Cyber Safety](#)[Cybersecurity Assessments](#)[Cybersecurity Governance](#)[Cybersecurity Insurance](#)[Detection and Prevention](#)[Information Sharing](#)

CYBER INCIDENT RESPONSE

When cyber incidents occur, the Department of Homeland Security (DHS) provides assistance to potentially impacted entities, analyzes the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the [national response to significant cyber incidents](#). The Department works in close coordination with other agencies with complementary cyber missions, as well as private sector and other non-federal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents.

[Expand All Sections](#)

CISA Central



Reporting Cyber Incidents to the Federal Government



National Cyber Incident Response Plan (NCIRP)



Incident Response Training



Last Updated Date: November 1, 2021

Was this webpage helpful? Yes | Somewhat | No



Letitia James

New York State Attorney General

Search ag.ny.gov

How can we help you?

I Want To...

[About](#) | [Resources](#) | [Libraries & Documents](#) | [News & Media](#) | [Contact](#)

[Home](#) | [Press Releases](#) | Attorney General James Secures \$200,000 From Law Firm For Failing To Protect New Yorkers' Personal Data

Attorney General James Secures \$200,000 from Law Firm for Failing to Protect New Yorkers' Personal Data

March 27, 2023

HPMB Law Firm Failed to Implement Data Security Measures to Protect New Yorkers' Health Information from Data Breaches



[Home](#) / [News and Events](#) / [News](#) / [Press Releases](#)

For Release

FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising

Under proposed order, GoodRx will pay a \$1.5 million civil penalty for failing to report its unauthorized disclosure of consumer health data to Facebook, Google, and other companies

February 1, 2023



Tags: [Consumer Protection](#) | [Regional Offices](#) | [Bureau of Consumer Protection](#) | [Western Region San Francisco](#) | [Health](#) | [Advertising and Marketing](#) | [Online Advertising and Marketing](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Health Privacy](#)

The Federal Trade Commission has taken enforcement action for the first time under its Health Breach Notification Rule against the telehealth and prescription drug discount provider GoodRx

Related Cases

[GoodRx Holdings, Inc.](#)

Related actions

Feb. 1, 2024

Feb. 4, 2024



For Release

FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach

FTC says company's poor security allowed hacker to steal sensitive data of millions of consumers, go undetected for months

February 1, 2024



Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#)

South Carolina-based Blackbaud Inc. will be required to delete personal data that it doesn't need to retain as part of a settlement with the Federal Trade Commission over charges that the company's lax security allowed a hacker to breach the company's network and access the personal data of millions of consumers including Social Security and bank account numbers.

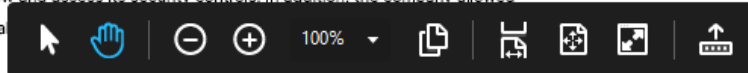
In its [complaint](#), the FTC says that Blackbaud, which provides data services and financial, fundraising, and administrative software services to companies, nonprofits, healthcare organizations, and others, failed to implement appropriate safeguards to secure and protect the vast amounts of personal data it maintains as part of the services it provides to its clients.

"Blackbaud's shoddy security and data retention practices allowed a hacker to obtain sensitive personal data about millions of consumers," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "Companies have a responsibility to secure data they maintain and to delete data they no longer need."

The FTC says that, despite promising customers that it takes "appropriate physical, electronic and procedural safeguards to protect your personal information," Blackbaud deceived users by failing to put in place such safeguards. For example, the company failed to monitor attempts by hackers to breach its networks, segment data to prevent hackers from easily accessing its networks and databases, ensure data that is no longer needed is deleted, adequately implement multifactor authentication, and test, review and assess its security controls. In addition, the company allowed employees to use default, weak passwords.

As a result of these failures, a hacker in early 2020 accessed a customer's Blackbaud-hosted database, according to the complaint. One of the data items accessed by the hacker was a list of

Give Feedback



FOR IMMEDIATE RELEASE

February 21, 2024

Contact: HHS Press Office

202-690-6343

media@hhs.gov

HHS' Office for Civil Rights Settles Second Ever Ransomware Cyber-Attack

OCR settles a ransomware investigation that affected over 14,000 individuals

Today, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), announced a settlement under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) with Green Ridge Behavioral Health, LLC, a Maryland-based practice that provides psychiatric evaluations, medication management, and psychotherapy. OCR enforces the HIPAA Privacy, Security, and Breach Notification Rules

<https://www.hhs.gov/hipaa/for-professionals/index.html>, which sets forth the requirements that HIPAA covered entities (most health care providers, health plans, and health care clearinghouses) and their business associates must follow to protect the privacy and security of protected health information. The settlement resolves an investigation following a ransomware attack that affected the protected health information of more than 14,000 individuals. Ransomware is a type of malware (malicious software) designed to deny access to a user's data, usually by encrypting the data with a

Feb. 21, 2024



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement ▾ Policy ▾ Advice and Guidance ▾ News and Events ▾ Ab

www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over

For Release

FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay \$16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking

FTC says despite its promises to protect consumers from online tracking, Avast sold consumers' browsing data to third parties

February 22, 2024



Feb. 22, 2024

Cybersecurity Law Update 2024

Thanks for Attending

David G. Ries



March 5, 2024