IMPROVING PRIVATE SECTOR CYBER VICTIM NOTIFICATION AND SUPPORT

FURTHERING RECOMMENDATIONS FROM THE CYBER SAFETY REVIEW BOARD

ROB KNAKE

AUGUST 2025

IST Institute for SECURITY + TECHNOLOGY

Improving Private Sector Cyber Victim Notification and Support:
Furthering Recommendations from the Cyber Safety Review Board

August 2025

Author: Rob Knake

Design: Taylor White

About the Institute for Security and Technology

Uniting technology and policy leaders to create actionable solutions to emerging security challenges

Technology has the potential to unlock greater knowledge, enhance our collective capabilities, and create new opportunities for growth and innovation. However, insecure, negligent, or exploitative technological advancements can threaten global security and stability. Anticipating these issues and guiding the development of trustworthy technology is essential to preserve what we all value.

The Institute for Security and Technology (IST), the 501(c)(3) critical action think tank, stands at the forefront of this imperative, uniting policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

We work across three analytical pillars: the **Future of Digital Security**, examining the systemic security risks of societal dependence on digital technologies; **Geopolitics of Technology**, anticipating the positive and negative security effects of emerging, disruptive technologies on the international balance of power, within states, and between governments and industries; and **Innovation and Catastrophic Risk**, providing deep technical and analytical expertise on technology-derived existential threats to society.

Learn more: https://securityandtechnology.org/

Acknowlegments

The Institute for Security and Technology (IST) is grateful for the support of Microsoft, Inc., whose funding enabled us to pursue this line of research. We would especially like to thank Kevin Reifsteck and Gabrielle Gerecht for their invaluable feedback and expertise.

We are also grateful to the working group members who contributed their time, perspectives, and expertise. A special thanks to Jeremy Grant, Charley Snyder, Jim Lewis, and Elliott Phaup who gave generously of their time outside the working group meetings. Atul Tulshibagwale and Sean Odell at the OpenID Federation provided invaluable technical advice on the use of the Secured Signals Framework for incident notification, as did Maxmillian Groth at Decentriq on the emerging category of Data Clean Rooms.

This report reflects the judgments and recommendations of the author. It does not necessarily represent the views of members of the advisory committee, whose involvement should in no way be interpreted as an endorsement of the report by either themselves or the organizations with which they are affiliated.

Contents

Executive Summary

When cyber incidents occur, victims should be notified in a timely manner so they have the opportunity to assess and remediate any harm. However, providing notifications has proven a challenge across industry. When making notifications, companies often do not know the true identity of victims and may only have a single email address through which to provide the notification. Victims often do not trust these notifications, as cyber criminals often use the pretext of an account compromise as a phishing lure. The volume of messaging across digital platforms means that important messages are often simply overlooked. Even when victims do trust that a notification is real, they may simply not know what actions to take given a lack of context or the technical skills necessary to secure their accounts.

To address these challenges, the Cyber Safety Review Board of Directors (CSRB) made a series of recommendations for cloud service providers to improve the process for victim notification and support.[1] Chief among these recommendations was to encourage cloud service providers to work with major mobile device platform vendors to develop an "'amber alert' style victim notification mechanism for high-impact situations."

While there is merit in the CSRB's recommendation to develop a shared notification capability for cyber incidents, implementation would require overcoming significant technological and governance challenges. Overcoming these challenges would require considerable investment and willing partnership from multiple parties. Given these barriers, development of the system is unlikely to move forward to solve the relatively narrow problem the CSRB proposed to address – "high-impact situations" within the ecosystem of cloud service providers. However, expanding the purpose and reach of the system to address any account compromise within the broader technology ecosystem may increase stakeholder willingness to invest in overcoming the technological, governance, and viability challenges.

This report explores the challenges associated with developing the native-notification concept and lays out a roadmap for overcoming them. It also examines other opportunities for more narrow changes that could both increase the likelihood that victims will both receive and trust notifications and be able to access support resources.

[1] "Review of the Summer 2023 Microsoft Exchange Online Intrusion," Cyber Safety Review Board, March 20, 2024, https://www.cisa.gov/sites/default/files/2025-03/CSRBReviewOfTheSummer2023MEOIntrusion508.pdf.

The report concludes with three main recommendations for cloud service providers (CSPs) and other stakeholders:

Recommendations

1. **Improve existing notification processes and develop best practices for industry.**
2. **Support the development of "middleware" necessary to share notifications with victims privately, securely, and across multiple platforms including through native notifications.**
3. **Improve support for victims following notification.**

While further work remains to be done to develop and evaluate the CSRB's proposed native notification capability, much progress can be made by implementing better notification and support practices by cloud service providers and other stakeholders in the near term.

Introduction

> **“Cloud service providers should develop more effective victim notification and support mechanisms to drive information-sharing efforts and amplify pertinent information for investigating, remediating, and recovering from cybersecurity incidents.”**
>
> - The Cyber Safety Review Board, p. iv, March 2024

In its Review of the Summer of 2023 Microsoft Exchange Online Intrusion, the CSRB highlighted the need for cloud service providers to improve victim notification and support processes for cyber incidents.[2] The CSRB found that a significant number of victims who received notifications in that incident either did not see them or did not trust them, suspecting that the messages were malicious. Collaboration with Federal agencies was hampered by legal and contractual barriers that slowed the process for sharing victim information on compromised personal accounts with Federal agencies so that they could assist with notifications. Once a warrant was issued, Federal agencies were able to assist in the victim notification process both by notifying their own employees whose personal accounts were compromised and by deploying Federal law enforcement to make notifications through field offices. This process took over a month from when Microsoft began making notifications.

Based on these findings, the CSRB made a series of recommendations to improve victim notification processes including developing an “‘amber alert’ style” notification for “high-impact” situations (Recommendation 18), developing a process to identify and support victims that are targeted for national security purposes (Recommendation 19), and encouraging the U.S. government to address barriers to collaboration with victims (Recommendation 20). Other cloud service providers acknowledge similar challenges in delivering victim notifications in a timely manner that victims trust and act upon.

To address these challenges, the Institute for Security and Technology (IST) convened a working group of representatives from cloud service providers (CSPs) and other stakeholders to explore the CSRB’s recommendations. This report focuses on assessing the viability of implementing an “amber alert”-style notification system and, secondarily, assesses other options to improve the delivery of notifications and follow-on support.

[2] “Review of the Summer 2023 Microsoft Exchange Online Intrusion,” p. iv.

Understanding the Problem: A Broken Chain of Trust

Generally, the American public has a high degree of trust in the tech industry and in CSPs specifically. Edelman's 2024 Trust Barometer finds that 60% of Americans trust the tech sector generally.[3] eMarketer's survey of technology company trust levels finds that 70% of Americans trust Amazon, 65% trust Google, 58% trust Microsoft, 55% trust Apple, and 36% trust Meta.[4] Other surveys show similar trends. Apple sits at 11th on Forbes' list of Most Trusted Companies.[5] Microsoft is at 33 and Google (Alphabet) is at 101 out of 300. Apple, Google, and Microsoft take the top three spots in the technology category for Clarify Capital's Most Trusted Brands survey.[6] Notably, trust in the technology sector is far higher than that of the government. On a similar polling question, the Pew Research Center finds that only 22% of the American public trust the Federal government to do what is right "just about always" or "most" of the time.[7]

These findings suggest that companies trying to make notifications are not untrusted actors – users and consumers generally expect these companies to protect their data and "do the right thing." A victim receiving a notification, at a minimum, does not think that these companies themselves are engaging in malicious activity or deceptive business practices when they send notifications, but they do not trust that the notifications are in fact from the company. The challenge therefore is not to "create trust" but to establish a chain of trust from the entity to the individual.

This challenge can be broken down into three phases:

1. **Getting Victim Attention**
2. **Gaining Victim Trust**
3. **Prompting Victim Action**

[3] Edelman, "2024 Edelman Trust Barometer: Supplemental Report Insights for the Tech Sector," March 2024, https://www.edelman.com/sites/g/files/aatuss191/files/2024-03/2024%20Edelman%20Trust%20Barometer%20Supplemental%20Report%20Insights%20for%20Tech.pdf.

[4] Meaghan Yuen, "More adults trust Big Tech and media companies than the US government," eMarketer, September 20, 2024, https://www.emarketer.com/content/more-adults-trust-big-tech-media-companies-than-us-government.

[5] Alan Schwarz, "Most Trusted Companies in America," Forbes, November 21, 2024, https://www.forbes.com/lists/most-trusted-companies/.

[6] "America's Most Trusted Business is Amazon," Clarify Capital, 2023, https://clarifycapital.com/most-trusted-businesses.

[7] Public Trust in Government: 1958-2024, Pew Research Center, June 24, 2024, https://www.pewresearch.org/politics/2024/06/24/public-trust-in-government-1958-2024/.

Getting Victim Attention

Working group members generally agreed that delivering notifications to victims is not difficult but getting victims to trust those notifications is difficult. Notifications can be sent through mobile apps, emails, text messages, phone calls, web portals, and letters. Yet many victims ignore messages delivered through these mechanisms. Likely, this is due to the volume of messages and notifications that individuals receive and due to fears that these messages are not authentic but instead fraudulent messages sent with the intention of compromising accounts. This fear is well founded. Criminals often send phishing emails that claim to be victim notifications and direct recipients to click URLs to secure their accounts that will instead deliver a malicious payload. That users are trained to be wary of these messages is a good thing – many decades of effort have gone into the education of end users on digital risks. Yet this wariness is making it difficult to deliver legitimate messages as users are not able to readily distinguish an alert from a phishing campaign.

Gaining Victim Trust

Gaining trust in the digital realm is not simple. User interface designers and developers have worked to develop various trust signifiers, but these often can be approximated by adversaries. Distinctions that may seem obvious to industry insiders are often overlooked by average users. Cybercriminals exploit small differences in domain names or use consumer accounts provided by CSPs to falsely generate trust when sending phishing messages. Given the emergence of “Smishing” and malicious robocalls, texts and phone calls are not more trusted than email.[8] Caller-ID is easily spoofed.[9] Even in-person “door knocks” by law enforcement are increasingly greeted with skepticism.[10] The emergence of voice and video deepfakes are only set to further undermine trust.[11]

For enterprise customers, many stakeholders have found that the person-to-person sales relationships can be an effective mechanism for making notifications. For small businesses, middle market companies, and individual consumers, however, those relationships often do not exist as services are purchased through web forms, through third-party resellers, or are free services.

[8] Proofpoint, “What is Smishing?,” last accessed June 2025, https://www.proofpoint.com/us/threat-reference/smishing.

[9] Federal Communications Commission, “Caller ID Spoofing,” last updated November 13, 2024, https://www.fcc.gov/consumers/guides/spoofing.

[10] Ellie Jo Pomerleau, “Police officer impersonation: what to look for and how to stay safe,” *WEAU 13 News*, June 18, 2025, https://www.weau.com/2025/06/18/police-officer-impersonation-what-look-how-stay-safe/.

[11] Nikki Main, “Man Scammed by Deepfake Video and Audio Imitating His Friend,” *Gizmodo*, May 22, 2023, https://gizmodo.com/deepfake-ai-scammer-money-wiring-china-1850461160; William McCurdy, “Deepfake fraud fears mount after Progress Corp hack,” *Biometric Update*, July 5, 2023, https://www.biometricupdate.com/202307/deepfake-fraud-fears-mount-after-progress-corp-hack.

Prompting Victim Action

Many stakeholders noted that even when notifications are sent successfully and victims do not believe that messages are SPAM or spearphishing, victims often still fail to take action based on the notification. Stakeholders generally agreed that many victims fail to take action because notifications often lack any context victims can use to determine what has been compromised and why or simply lack the necessary skills to take steps to secure themselves.

When CSPs have identified an adversary and conducted forensics that identifies what resources were compromised, they typically do not provide this information to individual users. Even if context were provided, many, if not most, victims are not IT or IT security professionals and will not know how to determine what is necessary to secure their accounts. Providing specific information on what actions victims should take could, in part, address this challenge. But for most victims, an offer of support service or, at a minimum, directing them to a trusted third party (or having that third party reach out), is likely necessary.

Additional Considerations in Protecting the Chain of Trust

Preventing Adversary Interdiction of Notifications

An important consideration for providing notifications is to take steps to reduce the risk that notifications will be intercepted by the threat actor. Thus, notifications should not be delivered to a compromised device or through a compromised account. The Department of Defense has implemented this policy in its Cyber Incident Handling Program. Under DOD policy, "Incident reporting will be conducted out of band from the involved network. Do not use assets on an information network that is (or potentially has been) compromised because an attacker may be monitoring the compromised network and could be warned of detection."[12] For the Department of Defense, meeting this requirement is typically accomplished by using the next highest classification network (ie Unclassified to Secret; Secret to Top Secret). While the civilian community does not have a similar tiered network, the principle holds that notifications should not be made to a device or account that is known to be compromised.

Addressing the International Dimension

Most CSPs have significant operations outside the United States and thus many victims of cyber incidents will be foreign persons living and working in foreign jurisdictions. Moreover, the threat actor targeting an individual or an enterprise may very well be a government agency in the jurisdiction where a company operates or a person lives or works. Asking a government agency to provide assistance could simply mean informing the adversary that their campaign

[12] Chairman of the Joint Chiefs of Staff Manual, "Cyber Incident Handling Program," CJCSM 6510.01B, July 10, 2012, p. B-16, https://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-02-05-175710-897.

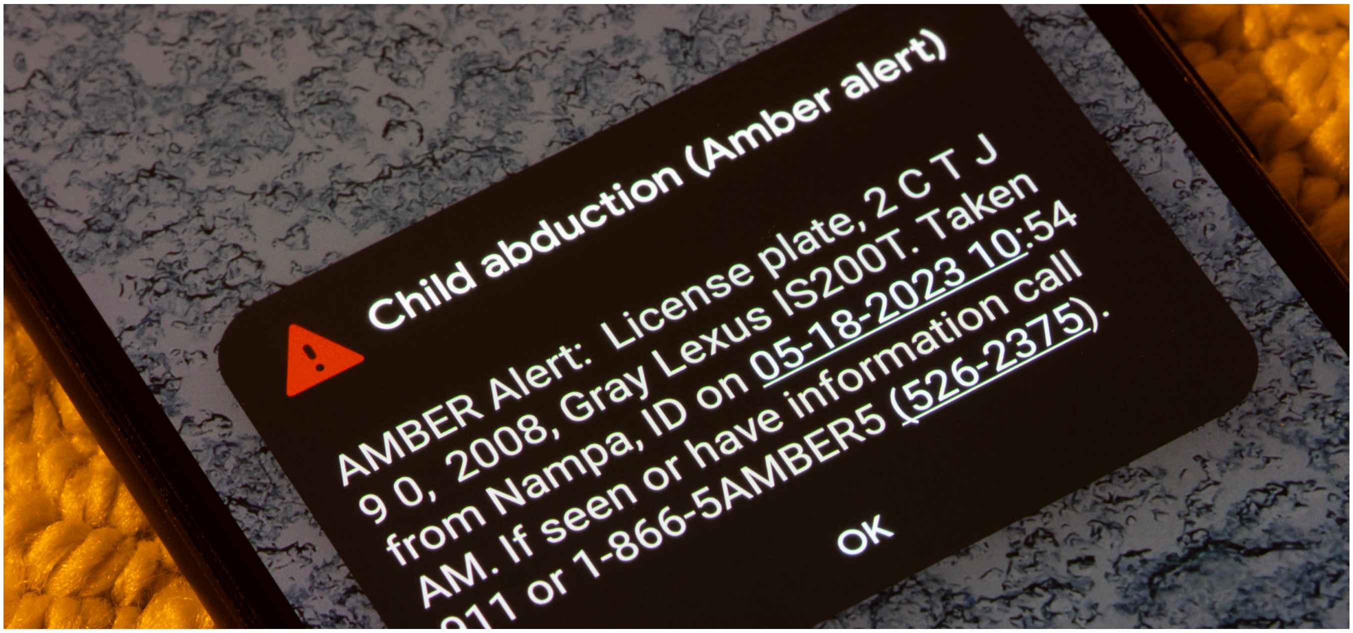
has been discovered. Thus, any solutions to address these problems should be made in an international context in which governments may be unable, unwilling, or adverse to supporting the notification process.

Developing Notification Solutions

> **"CSPs and the U.S. government, in conjunction with major mobile device platform vendors, should develop a targeted, quickly recognizable "amber alert" style victim notification mechanism for high-impact situations. The alert should be more readily distinguishable from notification emails, which are frequently mistaken by victims for phishing, building on some existing mechanisms for NSNs within platform providers' ecosystems where the mobile device operating system can send a native system alert about the compromise of an end user's CSP account, such as a push notification."**
>
> \- The Cyber Safety Review Board, p. 23, March 2024

Given documented challenges with distributing notifications that are both trusted and acted upon, solutions for delivering native notification capabilities may prove most effective. Actual use of the Amber Alert system and the underlying systems for victim notifications is not likely a viable option (and was not recommended by the CSRB). Amber Alerts are broadcast to all cellular devices in a specific geography – the system is not designed to target alerts to individuals and the identity of recipients is not known nor relevant. In contrast, victim notifications must be specifically targeted to the individual victim while protecting the privacy of their information. Thus, a separate system would need to be developed to achieve the outcome of delivering an Amber Alert-style notification natively to a victim.

Figure 1: An amber alert displayed on an iPhone



Child abduction (Amber alert)

AMBER Alert: License plate, 2 C T J 9 0, 2008, Gray Lexus IS200T. Taken from Nampa, ID on 05-18-2023 10:54 AM. If seen or have information call 911 or 1-866-5AMBER5 (526-2375).

(SOURCE: ADOBE STOCK)

Background: Amber Alerts and the Wireless Alert System

While the CSRB flagged the Amber Alert as an example of a high priority and trusted notification delivered to a mobile phone, the underlying Wireless Emergency Alert (WEA) system is not capable of delivering a targeted message to an individual user but instead provides warning to all cell users in a specific geographic area.[13] Amber Alerts are broadcast based on location to all members of the public using “cell broadcast” (“Short Message Service-Cell Broadcast” in the relevant standards). Yet lessons can be drawn from understanding the Amber Alert process.

Building the chain of trust to place an Amber Alert on an individual’s phone required authorizing legislation, creation of a national coordinator to oversee the system, the development and implementation of technical standards, a process for authenticating valid users, standards for issuing an alert, and annual funding for the operation and expansion of the system.[14]

Legal Authorization

While the Amber Alert program began as a private initiative between local area radio broadcasters and Dallas-Fort Worth police agencies in 1996, growth of the program did

[13] “Wireless Emergency Alerts,” FEMA, last updated October 18, 2023, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public/wireless-emergency-alerts,

[14] “Guidelines for Issuing AMBER Alerts,” U.S. Department of Justice Office of Justice Programs, last accessed June 2025, https://amberalert.ojp.gov/about/guidelines-for-issuing-alerts.

not occur until Congress passed legislation that provided the program a legal foundation. The "Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003" (the PROTECT Act)[15] established the National Coordinator of the AMBER Alert Communications Network within the Department of Justice, the development of standards for issuing alerts, and provided both core and grant funding for the program.

As the program grew, it began to draw in partners outside of government agencies to distribute notifications beyond local radio stations. With the growth of the Internet and social media, the importance of "secondary alerts" grew. Individuals could sign up for alerting through opt-in provisions with their cellular carriers and social media sites.

With the passage of the "Warning, Alert, and Response Network Act," (the WARN Act)[16] in 2008 and the operationalization of the WEA system in 2012, wireless notifications became the most important means for distribution of Amber Alerts. While participation remains voluntary under the law, almost all mobile carriers participate in it and few end users choose to not receive the notifications. Under the WARN Act, a carrier that chooses not to participate must notify their customers, and users are opted into receiving Amber Alert and other notifications by default.

Technical Standards and Guidelines

The National Coordinator is responsible for the development of technical standards and guidelines to implement the Amber Alert program.[17] These standards are maintained as part of the Department of Justice's National Information Sharing Standard (NISS) program.[18] The Amber Alert Information Exchange Package Documentation (IEPD) and the associated XML schema is available in a separate section of the Department of Justice website.[19]

Also relevant are the technical standards for the WEA system over which Amber Alerts are distributed. FEMA and the FCC are responsible for the development and maintenance of WEA standards including the Common Alerting Protocol (CAP).[20,21] The Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry

[15] "An Act to prevent child abduction and the sexual exploitation of children, and for other purposes," Public Law 108–21, April 30, 2003, https://amberalert.ojp.gov/sites/g/files/xyckuh201/files/media/document/protect_act.pdf.

[16] "Warning, Alert, and Response Network Act," H.R. 4954—53, Title VI-Commercial Mobile Service Alerts, December 8, 2005, https://transition.fcc.gov/pshs/docs/emergency-information/cmas-warn-act.pdf.

[17] "NISS Knowledge Base: Justice Information Sharing," U.S. Department of Justice Office of Justice Programs, November 2, 2020, https://bja.ojp.gov/program/it/niss/kb.

[18] "National Information Sharing Standards (NISS): Information Exchange Package Documentation (IEPD) and Justice Standards Clearinghouse," U.S. Department of Justice, Office of Justice Programs, last accessed June 2025, https://bja.ojp.gov/program/it/niss.

[19] "Information Exchange Package Documentation (IEPD)," U.S. Department of Justice, Office of Justice Programs, https://bja.ojp.gov/program/it/niss/iepd.

[20] "Wireless Emergency Alerts," Federal Communications Commission, last updated February 28, 2025, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/alerting/general/wireless

[21] "Common Alerting Protocol," FEMA, last updated January 6, 2021, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/technology-developers/common-alerting-protocol.

Association (TIA) have jointly issued most of the relevant standards. OASIS is responsible for CAP.[22]

FEMA and the FCC do not approve messages before they are sent but do provide guidance on alert issuance. Misuse of the system can result in revocation of alerting authority status.[23]

Validation of Alerting Authorities

In order to issue an Amber Alert or other Wireless Emergency Alert, public safety agencies must apply to FEMA to become an alert-originating authority (also known as a Collaborative Operating Group or COG) under the overarching Integrated Public Alert and Warning System (IPAWS).[24,25] There are 1600 Alerting Authorities approved to issue alerts today. The approval process requires:

- Completing IPAWS Training
- Purchasing IPAWS Compatible Software
- Completing a Memorandum of Agreement with FEMA
- Securing Public Alerting Permissions

Authentication is carried out through IPAWS Compatible Software.[26] Contrary to claims made by some vendors, there is no certification requirement for this software. At the other end of the pipeline, Commercial Mobile Service Providers (carriers like AT&T, T-Mobile, and Verizon) connect to the IPAWS through the Federal Alert Gateway through a CMSP Gateway that meets ATIS standards.[27]

Coordination

The Office of Justice Programs (OJP) at the Department of Justice serves as the National Amber Alert Coordinator. Under a grant from OJP, the National Criminal Justice Training Center (NCJTC) at Fox Valley Technical College operates the Amber Alert Training and Technical Assistance Program (AATTAP).[28] The AATTAP provides training to state and local government agencies on Amber Alert planning and implementation. In addition, the National

[22] OASIS, "Common Alerting Protocol Version 1.2," July 1, 2010, https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf.

[23] "Best Practices for Alerting Authorities using Wireless Emergency Alerts," FEMA, last updated March 24, 2023, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/alerting-authorities/best-practices.

[24] Alerting Authorities," FEMA, last updated April 29, 2025, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/alerting-authorities.

[25] "Integrated Public Alert & Warning System," FEMA, last updated April 29, 2025, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system.

[26] "Demonstrated IPAWS Capabilities–Alert Origination Software Providers," FEMA, fact sheet, September 2022, https://www.fema.gov/sites/default/files/documents/fema_alert-origination-software-providers-ipaws_102022.pdf.

[27] "Commercial Mobile Service Providers," FEMA, last updated October 27, 2023, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/broadcasters-wireless/commercial-mobile-service-providers.

[28] "About Amber Alert," The Amber Advocate, last accessed June 2025, https://amberadvocate.org/about/.

Center for Missing & Exploited Children, a non-profit corporation established by Congress in 1983, manages the Amber Alert Secondary Distribution Program, including distribution through WEA.[29] NCMEC contracts with OnSolve for the authentication and distribution system.[30] The IPAWS Technical Support Services Facility provides 24/7 technical support to IPAWS alerting authorities and is a component of FEMA.[31]

Funding

The PROTECT Act authorized $10 million in funding for the first fiscal year of the program. NCMEC received $48.9 million in 2023 from government grants and $1.1 million in contracts; however, only a portion of this funding goes to its role as manager of the Amber Alert Secondary Distribution Program.[32] In 2022, OJP awarded The Amber Alert Training and Technical Assistance Program a $4.4 million grant.

[29] National Center for Missing and Exploited Children, last accessed June 2025, https://www.missingkids.org/home.

[30] "OnSolve to Serve as Primary Mass Notification System for the National Center for Missing & Exploited Children (NCMEC)," OnSolve, press release, December 2, 2020, https://www.onsolve.com/latest-news/onsolve-mass-notification-system-for-the-ncmec/.

[31] "The IPAWS Technical Support Services Facility," FEMA, last updated May 16, 2025, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/ipaws-technical-support-services-facility.

[32] "Form 990: National Center for Exploited and Missing Children," Internal Revenue Service, 2023, https://www.missingkids.org/content/dam/missingkids/pdfs/NCMEC-2023-Form-990-Public-Disclosure.pdf.

Developing the Native Notification for Victim Notification Concept

Drawing lessons learned from how the Amber Alert system has been developed, implementing a native notification system for cyber incidents could follow a parallel path. This section outlines potential requirements for governance, standards, authorizing participants, distributing notifications, and funding the system.

Governance Entity

If developed by a consortium of private companies for voluntary participation, no legislation would be required; however, an open and transparent governance structure will be necessary to build trust among all parties and address antitrust concerns. A new or existing non-profit organization would be the most appropriate governance entity to manage the system. The consortium could consider an open application process to solicit proposals by organizations to fulfill this function.

Standards Organization and Standards Development

The governance entity should be responsible for developing standards and guidelines for use of the system. The development of these standards should be outsourced to an appropriate standards organization. Ideally, existing standards could be used or augmented for this purpose.

The most promising existing standard is the Risk Incident Sharing and Coordination (RISC) standard.[33] RISC is based on the Shared Signals Framework (SSF) that is sponsored by the OpenID Foundation and specifies a series of event types that can be exchanged between authentication systems.[34] RISC events can be used to share information about accounts for logging in across multiple platforms such as whether a credential has been compromised, disabled, or an identifier recycled. These events are used by platforms to make authentication determinations but the standard could be extended to provide notice to account holders that one of their accounts has been compromised and direct them to resources. The FIDO Alliance, which promotes standards for passwordless authentication, and OASIS, which is responsible

[33] M. Scurtescu, A. Backman, P. Hunt, J. Bradley, S. Bounev, A. Tulshibagwale, “OpenID RISC Profile Specification 1.0 - draft 04,” Shared Signals, Github, https://openid.github.io/sharedsignals/openid-risc-1_0.html.

[34] “Shared Signals Working Group - Overview,” OpenID, last accessed June 2025, https://openid.net/wg/sharedsignals/.

for many of the standards for Amber Alerts, could also be viable standards entities for this purpose.[35]

Notification Authorities

The governance entity will need to establish a process for approving organizations to issue notifications. An important factor will be addressing antitrust concerns given that the proposed system requires cooperation between industry competitors. Eligibility standards for membership will need to be clear and applications will need to be open.

Membership should be divided into two categories: **First Party Notifiers** and **Third-Party Notifiers**. First Party Notifiers would include founding Consortium Members and other entities that would issue notifications to their users over the system. First Party Notifiers would most likely be the large consumer service providers that will make the most frequent use of the system and wish to have a voice (and vote) in the governance and the development of the organization. Third Party Notifiers would include cyber incident responders, insurance companies, or industry consortiums that would issue notifications on behalf of their clients, customers, or members through devices, websites, and apps of First Party Notifiers. For instance, a company like Netflix that has a large user base might join as a First Party Notifier, distributing notifications on compromised Netflix accounts to devices and other platforms that are part of the system as well as delivering notifications for other participating companies through the Netflix app and web portal. A credit reporting agency like Equifax or an incident response firm might join as a Third-Party Notifier, using the system to distribute notifications on behalf of smaller customers that would not otherwise have access to the system.

Validating Notifications and Matching Victims to Distribution Mechanisms

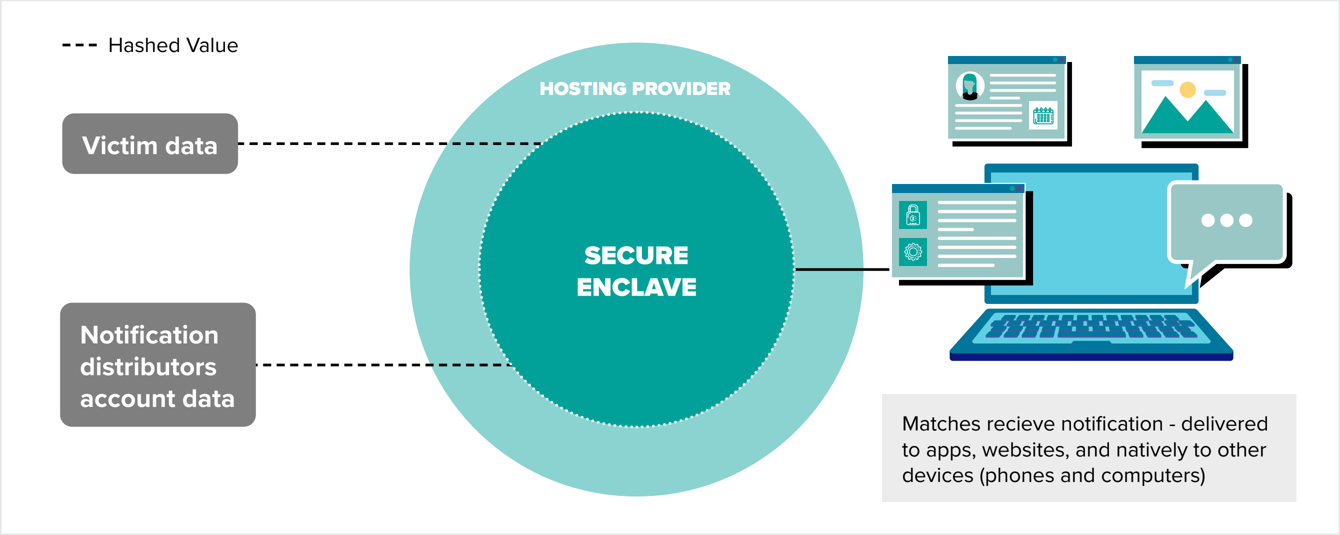
The system must be able to validate the right to send notifications and to match identifiers on victims such as an email address with phone numbers and accounts at distribution mechanisms. For native notifications, it will require the ability to match a victim's compromised account with their mobile phone. It will need to do this with close to 100% accuracy as a delivery to the wrong individual would constitute an additional incident.

In some cases, a company that needs to make a notification will only have an email address. In other cases, it may have a name and phone number and secondary email address. These may have been validated as tied to the owner of the account. The company may also have information on the victim's mobile device, though OS developers have worked to limit this information. Companies may have carrier information and device type. This information will need to be matched with subscriber information at distribution mechanisms.

[35] FIDO Alliance, last accessed June 2025, https://fidoalliance.org/.

Assembling a database of all global account holders is a non-starter given security, privacy, and business interests. Instead, the system should operate through a Data Clean Room.[36] Data Clean Rooms allow two or more parties to combine proprietary or sensitive data without ever revealing the underlying data to the other parties. For this purpose, the Data Clean Room would be set up as a "black box" matching schema where victim account information would be submitted as hashed values and matched to hashed values of account data held by distributors. Matches would result in the distribution of the message and confirmation of the match back to the distributor.

Figure 2: Applying Data Clean Rooms to victim notification


--- Hashed Value
Victim data
Notification distributors account data
HOSTING PROVIDER
SECURE ENCLAVE
Matches recieve notification - delivered to apps, websites, and natively to other devices (phones and computers)

Funding

Startup costs will need to be covered by the initial consortium of backers. Once operational, fees from Notification Authorities should be set to fund the organization on an ongoing basis. Because the level of system usage will be determined by the extent of discovered adversary activity, fees should not be based on utilization but organization size and industry. Additional services supporting victims could be charged to members for specific incidents. Based on available budget data for the Amber Alert ecosystem and other organizations within the IT security ecosystem, founding consortium members should commit to at least $10 million in initial funding.

[36] "Data Clean Room," Databricks, last accessed June 2025, https://www.databricks.com/discover/enterprise-data-platform/clean-room#clean-rooms.

Assessing the Native Notification Concept

There is merit in further exploring the native notification concept as part of a larger ecosystem to deliver notifications that users will trust through multiple means. Gaining the support of all the parties in the ecosystem that would be required for native notification to mobile devices is likely to be a significant undertaking. Yet building out the governance and technical system to deliver native notifications can also deliver notifications effectively across multiple systems and platforms. App-based notifications and web portal notifications may be as effective as native messages, but a system that uses multiple channels to deliver a coordinated message to users is likely necessary to engender trust.

While the concept of native notifications has intuitive logic and appeal, there is no data to support the contention that these notifications would necessarily be more trusted than other forms of notification — as well as some evidence that Amber Alerts and other native notifications are not always trusted. FEMA, which is responsible for managing the underlying system that delivers Amber Alerts, maintains a Myths vs. Facts website about the process.[37] The webpage provides responses to many commonly voiced concerns about the agency's alerting programs. These include addressing whether the WEA system "sounds will activate vaccines, nanoparticles and graphene oxide" and addresses claims that "WEA installs malware on my phone." Thus, the end state of native notifications may not alone address the broken chain of trust.

[37] "IPAWS Myths vs. Facts," FEMA, last updated April 4, 2024, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public/myths-facts.

Improving Existing Notification Programs

Given the identified challenges in implementing the native notification concept, CSPs and other stakeholders should examine lessons learned from existing victim notification programs and from government notification programs to improve the efficacy of current delivery methods. While the CSRB recommended the development of native notification to address "high-impact" victims, developing such a program is likely only viable if established to reach a broader audience. For high-impact victims like in the 2023 incident, existing notification programs that focus on existing delivery mechanisms and provide "concierge" support can likely address identified challenges. Lessons can be drawn from Apple, which has developed a strong program for notifying victims of mercenary spyware using zero click exploits on iOS. Federal law enforcement guidelines also suggest that multiple notification channels and creative use of those channels is both permissible and effective. Finally, the use of third parties should also be considered.

Coordinated Notifications Through Existing Channels

When Apple identifies evidence that an individual may have been the victim of zero-click spyware on an iOS device, it sends a notification through its customer portal, through email, and via Apple messages.[38] In April of 2024, Apple sent notifications to victims in 92 countries.[39] Apple recommends that users verify that Apple sent the notification by logging in to their customer portal where the threat notification will be displayed.[40]

The notification directs the victim to seek assistance from a non-profit organization equipped to provide support such as Access Now.[41] Access Now operates its Digital Security Helpline for "Civil Society Groups and Activists; Media Organizations, Journalists and Bloggers; and Human Rights Defenders."[42] The organization operates a vetting process before providing assistance. In its explainer, Access Now notes that it will not provide support to an individual or

[38] "About Apple threat notifications and protecting against mercenary spyware," Apple, April 25, 2025, https://support.apple.com/en-in/102174.

[39] Manish Singh, "Apple alerts users in 92 nations to mercenary spyware attacks," TechCrunch, April 10, 2024, https://techcrunch.com/2024/04/10/apple-warning-mercenary-spyware-attacks/.

[40] For example, see: Shashi Tharoor, @ShashiTharoor, "Received from an Apple ID, threat-notifications@apple.com, which I have verified. Authenticity confirmed. Glad to keep underemployed officials busy at the expenses of taxpayers like me! Nothing more important to do?" Twitter, October 31, 2023, https://x.com/ShashiTharoor/status/1719226802609307839.

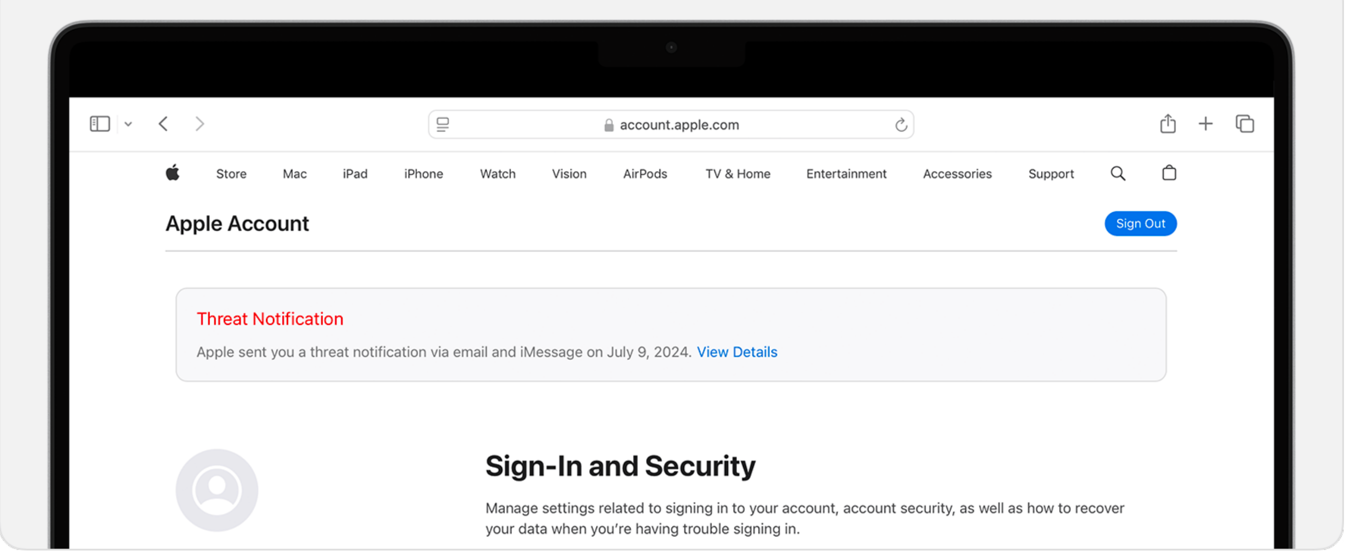
[41] Access Now, last accessed June 2025, https://www.accessnow.org/.

[42] "Digital Security Helpline," Access Now, last accessed June 2025, https://www.accessnow.org/help/.

organization if they are “affiliated with… current holders of political office.”[43] Access Now says that it received 4,337 requests for assistance through its helpline in 2024.[44] Apple provided grants totaling $525,000 to Access Now between January and September 2024.[45] $250,000 was specified for the Digital Security Helpline. Okta, the David and Lucile Packard Foundation, Democracy Funders Network, NordVPN, and the Ford Foundation also provided grants directed at the Digital Security Helpline.

Working group members generally agreed that if a victim can be driven to log in to their user portal where a notification banner can be displayed, the victims will trust the notification. A victim might not initially trust an email message and users have grown wary of notifications delivered over messaging platforms, but sustained and coordinated efforts that direct users to login to a web portal that they are familiar with may convince them to go directly to that website. Savvy web users will likely not click on any links delivered as part of notifications and notification campaigns should account for this user behavior.

Figure 3: Apple web portal notification



Apple Account

Threat Notification

Apple sent you a threat notification via email and iMessage on July 9, 2024. View Details

Sign-In and Security

Manage settings related to signing in to your account, account security, as well as how to recover your data when you’re having trouble signing in.

(SOURCE: APPLE)

[43] “Digital Security Helpline: About Our Mandate and the Support We Provide,” Access Now, last accessed June 2025, https://www.accessnow.org/helpline-mandate/.

[44] Lorenzo Franceschi-Bicchierai, “Apple sends spyware victims to this nonprofit security lab,” TechCrunch, December 20, 2024, https://techcrunch.com/2024/12/20/why-apple-sends-spyware-victims-to-this-nonprofit-security-lab/.

[45] “Funding,” AccessNow, last accessed June 2025, https://www.accessnow.org/financials/.

Borrowing Best Practices from Law Enforcement

The Attorney General Guidelines for Victim and Witness Assistance encourages law enforcement to "use technology and be creative" to reach victims, particularly when incidents require large numbers of notifications.[46] The guidance specifically calls out the use of "website, email, and call center capabilities" and can include public notice that a notification campaign is underway through news outlets and social media.[47] When incidents are made public, CSPs should provide public guidance on how to confirm that a notification is authentic and not malicious. As the guidelines call out, notifiers should "carefully evaluate the type of information relayed and the method of communication to minimize the risk that investigations are compromised and the victims' privacy interests are inadvertently invaded."[48]

Making Use of Proxies and Representative Organizations

The Attorney General Guidelines specifically encourage law enforcement to make use of proxies to disseminate notices to large numbers of victims. Such notifications can include "… proxy notification to a person or entity that can disseminate notice to other victims, such as banks, internet service providers, community organizations, corporate entities, or counsel for a class of victims."[49] CSPs can likely borrow these best practices recognizing, as the guidelines do, that the benefits of notifying victims outweigh potential risks to privacy from taking such an approach. The National Cyber Security Centre (NCSC) in the UK has taken steps to formalize such an approach by developing a registry for UK companies to register for "Early Warning" alerts.[50] Companies create an account and provide: 1) their organization name; 2) their public IP addresses and domain names; and 3) point of contact information for security events. Former NCSC officials noted that the NCSC was considering allowing cyber insurers to enroll their customers as well.

[46] U.S. Department of Justice, "The Attorney General Guidelines for Victim and Witness Assistance," 2022 edition, March 31, 2023, https://www.justice.gov/d9/pages/attachments/2022/10/21/new_ag_guidlines_for_vwa.pdf.

[47] "The Attorney General Guidelines," p. 59.

[48] "The Attorney General Guidelines," p. 60.

[49] "The Attorney General Guidelines," p. 60.

[50] National Cyber Security Centre, "Active Cyber Defense: Early Warning," last accessed June 2025, https://www.ncsc.gov.uk/section/active-cyber-defence/early-warning.

Summary Recommendations

Improving the victim notification process should be a priority for CSPs and the broader cybersecurity community. To realize the CSRB's vision for native notification requires both developing a mechanism to securely exchange victim identifiers and gaining the support of mobile device makers and carriers to deliver these notifications. Given these challenges, CSPs should first work to improve existing notification processes by adopting best practices and implementing lessons learned through a process of continual improvement. While making these improvements, CSPs and other stakeholders should begin working to develop a shared notification system. Finally, CSPs and other relevant stakeholders should take steps to improve the support that they provide to victims once a notification has been delivered.

Recommendation 1:
Improve existing notification processes and develop best practices for industry.

Lessons learned from the 2023 CSRB report and other CSPs notification programs suggest that a series of improvements could make existing notifications programs function better.

Cloud Service Providers should use multiple channels to drive victims to log in to their customer portals to receive detailed notifications and support. Several CSPs have established processes with the goal of getting victims to login to their customer portals to receive notifications. Focused messaging to encourage users to log in to a familiar web address even if they are wary of clicking on a link is a proven effective model. Consistent messaging across multiple email accounts, text messages, and phone numbers can convince even the most wary or dismissive users to log in. Should these attempts fail, CSPs should consider disabling accounts to force a login to the user portal where the notification can be shared (particularly for email providers where users may use IMAP to access messages through an email client). Even if passwords are not compromised, forcing a password reset or breaking service provision to prompt a login to a web portal is the most effective way to deliver a notification. In this approach, CSPs force a password reset for their service (including app specific passwords) so that their service is no longer available without verification. They then send notifications through secondary email, text, apps or automated phone calls. Because these messages demonstrate awareness of the current state of the account (that it is not functional), they are far more likely to be trusted. Even if these messages are not delivered, forcing the password reset or otherwise breaking authentication will drive most users to the login portal on their own.

Notifiers should share available context with victims. Stakeholders are likely overstating the impact on sources and methods from disclosing the details of intrusions to victims. While companies should remain wary of sharing such information over compromised channels, the government's experience over the last decade is that concerns with sharing the context around incidents were largely overstated. Where context is available, it should be shared with victims so that they can conduct their own assessment of residual risk.

NIST should update Special Publication 800-61 to include recommendations on victim notification. NIST Special Publication 800-61 – Incident Response Recommendations and Considerations for Cybersecurity Risk Management should be revised to provide guidance on how companies should make and prepare to receive security notifications based on the Attorney General Guidelines for Victim and Witness Assistance.[51] Specifically, 800-61 should:

» Provide guidance that strongly recommends providing notifications out of the compromised channel

» Encourage notifiers to creatively use technology to reach victims

» Use proxies such as banks, ISPs, ISACs while protecting the privacy rights of victims

Stakeholders should pursue an opt-in notification program similar to the UK's Early Warning System with cyber insurers and other interested parties. While opt-in solutions will only reach a small minority of potential victims, those persons and companies most motivated to receive notifications should have an avenue to do so. Cyber insurers have a financial motivation for their covered entities to receive timely notifications of incidents and exposures. Notifications can reduce the likelihood and amount for incident claims. Insurance providers can act as a bridge between CSPs, security researchers, and other entities that have information on security events to share with businesses at any scale.

[51] Alex Nelson, Sanjay Rekhi, Murugiah Souppaya, and Karen Scarfone, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management," NIST, Special Publication 800-61r3, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

Recommendation 2:
Support the development of "middleware" necessary to share notifications with victims privately, securely, and across multiple platforms including through native notifications.

Regardless of whether the final notification is delivered in a native message on a mobile device or through multiple other means, "middleware" is necessary to privately and securely match a victim's account at one organization with the victim's account on a different network or system. Developing this system is the crucial next step to implement the CSRB recommendation.

Create a consortium of CSPs and other stakeholders to further develop an infrastructure for shared notifications. Stakeholders should convene a consortium of relevant parties to continue work on this topic. Such a consortium could be a new organization or sponsored by an existing organization with relevant experience.

Support a standards organization to develop a data exchange model for victim notifications. The OpenID Foundation's RISC standard and Secure Signals Framework are likely the most amenable to meeting the requirements of the envisioned notification system. The FIDO alliance, OASIS, and other organizations could also be augmented to address victim notification. The model will need to address whether a distributed system is possible or whether a centralized entity is necessary to match data on victims and notifiers.

Develop a Data Clean Room Proof of Concept and Seek to Pilot It. Development of a proof of concept would confirm or negate the barriers identified to realizing the vision articulated by the CSRB. Crucially, a proof of concept must address: 1) how victim data will be protected and 2) how notifiers will be incentivized. Likely, a viable system will require the use of black box technology to match encrypted identifiers from participating companies.

Recommendation 3:
Improve support to victims following notification.

Improving the provision of support to victims of account compromise is at least as important as improving the delivery of notifications to inform the victim of the compromise. The CSRB report explicitly called for improving support to victims, not just improving notifications.

Cloud providers that do not already have them should develop secure configuration programs to protect against advanced persistent threats. Google has developed its Advanced Protection program and Apple has developed Lock Down Mode for iPhone and Advanced Data Protection for iCloud.[52] Microsoft has created its AccountGuard program as a free service to support high-risk organizations as part of its Democracy Forward Initiative.[53] Each of these offerings addresses some aspects of a holistic program, yet no vendor has developed a complete offering. Secure configuration programs for consumer services should ensure they have multiple means to provide victim notifications for these users. Programs that do not already should require registrants to provide physical addresses, additional email addresses, phone number, and third-party trusted contacts.

Companies should engineer systems to automatically enroll targeted individuals in secure configuration programs. When a company detects that an individual has been targeted or victimized, it should push a secure default configuration but allow victims to revert back to baseline configurations if they so choose. Once they have regained access, the CSP should provide a dialogue with relevant context that takes them through the process to secure their account or explains that default security features have been enabled but can be disabled if they so choose.

Federal agencies should strongly encourage or require government leaders to enroll their personal accounts in secure configuration programs. The process for enrollment should be included in orientation for new political appointees and Senior Executive Service (SES) with national security responsibilities.

CSPs and other stakeholders should support the development of the consumer incident response market. When an individual consumer's accounts are compromised, there are few options on the market to support remediation. Companies like BlackCloak cater to executives;[54] however, as with Uber, what begins as a niche offering to high net worth individuals, can very quickly be scaled to meet mass demand. What the market requires in short is UberX for incident response. As one working group participant noted, such a service would be a natural extension of services like LifeLock or GeekSquad.[55] When a company is responsible for a breach, it should provide these services or outsource the provision of these services in partnership with trusted non-profits or other third parties.

[52] "Advanced Protection Program," Google, last accessed June 2025, https://landing.google.com/intl/en_in/advancedprotection/; "About Lockdown Mode," Apple, April 9, 2025, https://support.apple.com/en-us/105120; Android Lockdown Mode is judged to be targeted against physical threats and not designed for regular use. See: Alex Vakulov, "How To Use Lockdown Mode To Secure Your Android Smartphone," Forbes, November 15, 2024, https://www.forbes.com/sites/alexvakulov/2024/11/15/how-to-use-lockdown-mode-to-secure-your-android-smartphone/.

[53] "Microsoft AccountGuard," Democracy Forward Initiative, last accessed June 2025, https://accountguard.microsoft.com/.

[54] BlackCloak, "Private Client Services," last accessed June 2025, https://blackcloak.io/private-client-services/.

[55] LifeLock, "Homepage," last accessed June 2025, https://lifelock.norton.com/; "Geek Squad Protection," Best Buy, last accessed June 2025, https://www.bestbuy.com/site/geek-squad/geek-squad-protection/pcmcat159800050001.c?id=pcmcat159800050001.

Conclusion

The problems that the CSRB identified with cyber victim notification and support processes remain unsolved today. These challenges exist across all service providers and among other stakeholders in the digital ecosystem. There are significant challenges that must be overcome to realize the vision for native notification that the CSRB set out, including building a governance mechanism to oversee the process and a system to securely exchange sensitive information among participants. Given these challenges, the scope of any solution should be broadened to any incident that impacts user security and not just to “high-impact” victims. Given the relatively small number of high-impact victims, improvements to existing notification processes are likely sufficient for this narrower problem.

Further exploration of the concept is merited on the governance and technical design, which should be addressed in tandem. Most crucially, for this system to become a reality, proponents must develop a set of incentives for companies that will distribute notifications to participate. Regardless of whether proponents of native notification support further work on the concept, there are improvements that CSPs and other stakeholders can make to existing notification and support processes. Making these improvements and exercising these processes should move forward in the near term.

Working Group Participants

Name	Company
Chris Boyer	AT&T
Kathryn Condello	Lumen
Jeremy Grant	Venable
Margie Graves	IBM
Rob Joyce	Joyce Cyber LLC
Steve Kelly	IST
Michael Klein	IST
Jim Lewis	Project on Technology and National Security
Eugenia Lostri	Google
Priscilla Moriuchi	Apple
Robert Novy	Oracle
Elliott Phaup	National Security Institute
Kevin Reifsteck	Microsoft
Adam Shostack	Shostack Associates
Jordana Siegel	AWS
Charley Snyder	Google
Megan Stifel	IST
Bridgette Walsh	FS-ISAC
Evan Wolff	Akin

INSTITUTE FOR SECURITY AND TECHNOLOGY

www.securityandtechnology.org

info@securityandtechnology.org