Testimony of the Identity Theft Resource Center
Before the United States Senate Committee on Commerce, Science, and Technology
Subcommittee on Consumer Protection, Product Safety and Data Security
2:30 pm May 8, 2024

Is this the Golden Age of Identity Crime

Delivered by James Everett Lee, ITRC Chief Operating Officer

Introduction

Good afternoon, Chair Hickenlooper, Ranking Member Blackburn and members of the Subcommittee. Thank you for the honor of speaking with you today. My name is James Everett Lee and I am the Chief Operating Officer of the non-profit Identity Theft Resource Center (ITRC) based in San Diego, California.

For 25 years the ITRC has offered free assistance to victims of identity crimes. In that time, our contact center staffed by trauma-informed advisors has helped hundreds of thousands of victims recover their identities that have been stolen, misused, or otherwise compromised.

Through our website and outreach programs, we have helped millions of individuals avoid becoming identity crime victims by teaching them how to protect their information. We also provide information about the latest scams that involve the theft or misuse of personal information.

Since 2005, the ITRC has compiled the largest repository of publicly reported data breaches and other forms of identity data compromises. What started with a single notice and a handful of data points nearly 20 years years ago has grown into a database of more than 20,000 data breaches with as many as 96 data points per event that is updated daily.

The ITRC publishes an annual data breach report and quarterly updates that analyze the trends reflected in the data breach notices mandated by state law and federal regulations. We make this information available for free to consumers in the form of a searchable database as well as a free alert service that informs them when an organization they enroll with the ITRC posts a data breach notice. A more robust version of the data and services are available to businesses, government agencies, and institutions for a nominal fee.

Today I'll touch on our findings related to the current trends in identity crimes based on first-hand reports from the new victims who reported more than 13,000 incidents to the ITRC in 2023. I will also touch on the impacts of identity crimes and cyberattacks on general consumers and small businesses. This information comes from our annual research reports which are attached to these remarks.

I will also reference two additional ITRC reports from 2023 that provide some context to the topic for today's hearing: Research of first impression on the impact of identity crimes in Black communities; and, a discussion paper on the challenges to verifying a person is who they claim to be in a time when key points of personal information has been compromised for most adults in the never-ending series of data breaches. These, too, are attached for your reference.

Finally, for the Subcommittee's awareness, the ITRC is a 501(c)3 non-profit funded primarily through grants from the U.S. Department of Justice, Office of Victims of Crime (DOJ-OVC) as well as private contributions, corporate sponsorships, and donations. We work closely with key federal agencies on issues that involve identity crime victims including the Federal Trade Commission (FTC), the Internal Revenue Service (IRS), the Department of Treasury (Treasury), the Federal Reserve, the Pandemic Response Accountability Committee (PRAC), and the Department of Homeland Security (DHS). We provide data breach information to many of these same agencies. We also offer online, Live Chat access to ITRC Advisors to state and local law enforcement agencies and other non-profit organizations under a DOJ grant. A full list of our financial supporters and partner organizations is available on our website.

The Golden Age of Identity Crime

A lot has transpired since the last time the ITRC was part of a full committee hearing on a similar topic in October 2021. On that day we coincidently published a quarterly data breach report that showed we had already passed the total number of compromises recorded in 2020 and were only 238 data events away from tying the all-time record set in 2017. In fact, we did set a record for publicly reported data breaches later in 2021 – 1,860.

We were still struggling at that time to understand the scope and scale of the identity fraud committed during the pandemic when identity criminals were able to use information stolen in data breaches to impersonate unwitting victims. That information was, and still is, used to open bank accounts, obtain loans, and trick innocent, trusting people into willingly sharing personal information with someone they thought they knew – often on a social media platform or as part of a romance scam.

Given the ITRC's role as a victim advocacy organization, we offered a singular prescription: To reduce the number of identity crime victims – and crimes – reduce the number of data breaches linked to cyberattacks. To do that, we discussed three needs:

- The need for better cybersecurity and data protection standards and practices
- The need for better enforcement of cybersecurity and data protection regulations
- The need to fix the data breach notice system

Fast forward to today and the needs are still the same. What has changed is the urgency required to address those needs along with the opportunity to devalue personal information stolen by identity criminals.

Since 2021, we've seen bad actors shift tactics, expand their reach, and accelerate the pace of innovation. The results of these actions are the highest number of data breaches we've ever seen, often with devasting financial and emotional impacts on the individuals caught in the crossfire between professional identity criminals and the business or data source they target.

Add to the mix the introduction of generative artificial intelligence, and you have a recipe for a prolonged period of identity crime - fueled by stolen personal data, made highly effective and efficient by AI, with individuals and many businesses all but helpless to defend themselves. What we now have is all the ingredients for a Golden Age of Identity Crime.

Today's Trends

Today's trend lines support the classic definition of a Golden Age: great wealth, growth, innovation, and a kind of stability that supports long-term achievement.

Beginning with data breaches – the fuel for virtually all identity crimes and a fair portion of cyberattacks. The number of data compromises reported in the United States surpassed two significant milestones in 2023: The highest number of data events reported in a single year and exceeding 2,000 (and ultimately 3,000) events in a single year.

The total number of data compromises reached 3,205, impacting an estimated 353 million victims, including those affected by multiple compromises. The 2023 compromises represent a 78-percentage point increase over the previous year and a 72-percentage point hike from the previous all-time high number of compromises set in 2021.

Total Compromises by Year

	Compromises	Victims
2023	3,205	353,027,892
2022	1,801	425,212,090
2021	1,860	300,607,163
2020	1,108	310,235,204
2019	1,279	883,558,186
2018	1,175	2,227,849,622

SOURCE: ITRC 2023 Data Breach Report, January, 2024

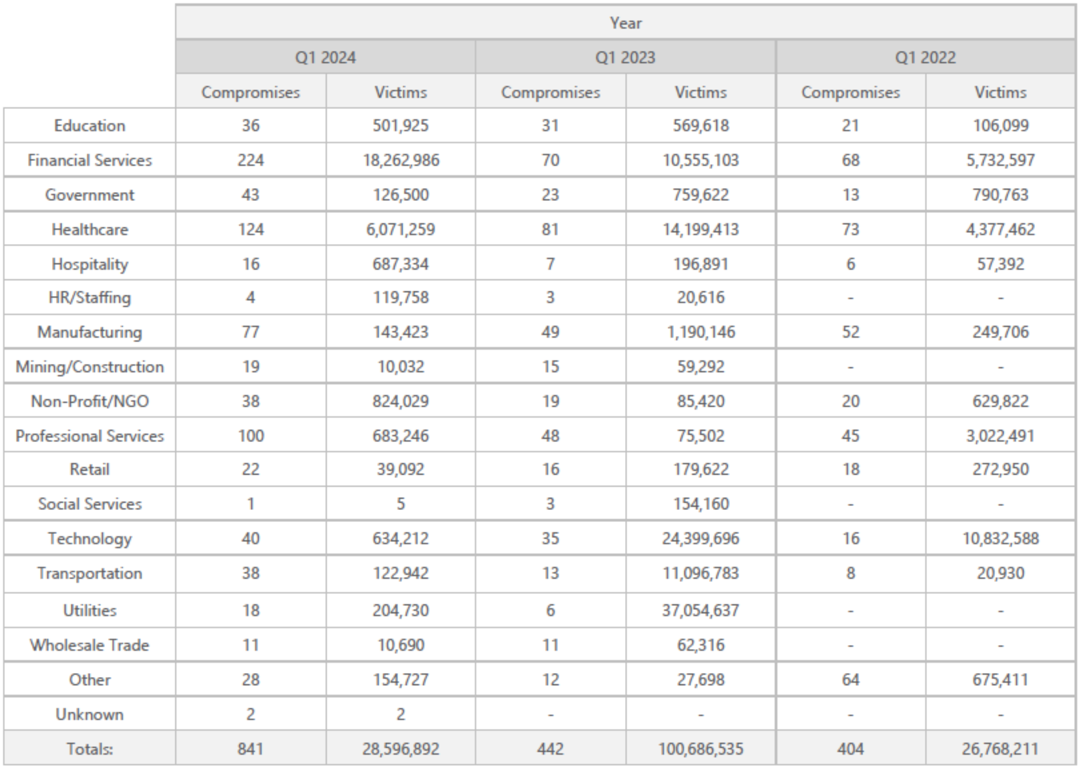
As of May 6, 2024, we have recorded 1,178 data breaches impacting an estimated 64 million people in 2024. Historically, Q1 is the lowest point in each year in terms of data breach notices, so we are already on a path for another record-setting year.

The steady downward drift in terms of the estimated number of individual victims may appear to be a positive trend, but is in fact an illusion. The number of victims impacted in 2023 represents a 16-percentage point reduction from 2022 when more than half of the total annual victim count was related to three breaches announced late in the previous year. By any measure, there are simply too many victims.

A single or series of small events can also rapidly reverse a downward victim trend. Through Q1 2024, the number of victims reported by compromised organizations dropped 81 percent (81%) from the last Quarter of 2023. However, a series of breaches in April this year has already more than doubled the victim count for the year.

That number does not include the ransomware-related breach at United Healthcare's Change subsidiary which will significantly increase the number of victims. Based on company comments, the number of victims could exceed one-third of U.S. residents given United Healthcare’s market share. To date, United Healthcare has not offered a specific victim estimate.

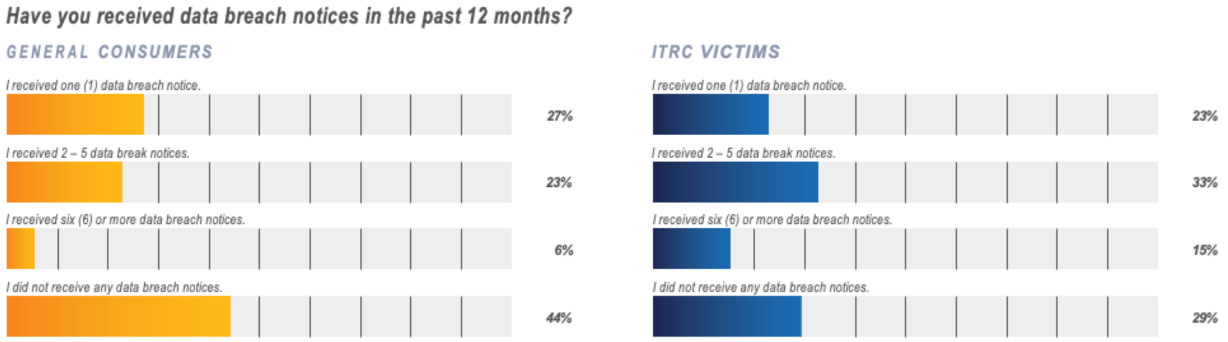
United Healthcare aside, the decline in the number of individual victims is largely attributed to the fact that organized cyber and identity criminals do not need to acquire personal and business information on the scale they once did. The kinds of attacks that lead to data breaches today are more targeted in terms of the organization that is attacked, the information sought, and the goal of the attack (financial or intelligence). The result is more attacks against a broader set of businesses, but a smaller footprint in terms of individual victims in any single attack. For example, in Q1 2024 attacks increased in 15 of 17 industries year over year, but the overall victim count decreased.



	Year					
	Q1 2024		Q1 2023		Q1 2022	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	36	501,925	31	569,618	21	106,099
Financial Services	224	18,262,986	70	10,555,103	68	5,732,597
Government	43	126,500	23	759,622	13	790,763
Healthcare	124	6,071,259	81	14,199,413	73	4,377,462
Hospitality	16	687,334	7	196,891	6	57,392
HR/Staffing	4	119,758	3	20,616	-	-
Manufacturing	77	143,423	49	1,190,146	52	249,706
Mining/Construction	19	10,032	15	59,292	-	-
Non-Profit/NGO	38	824,029	19	85,420	20	629,822
Professional Services	100	683,246	48	75,502	45	3,022,491
Retail	22	39,092	16	179,622	18	272,950
Social Services	1	5	3	154,160	-	-
Technology	40	634,212	35	24,399,696	16	10,832,588
Transportation	38	122,942	13	11,096,783	8	20,930
Utilities	18	204,730	6	37,054,637	-	-
Wholesale Trade	11	10,690	11	62,316	-	-
Other	28	154,727	12	27,698	64	675,411
Unknown	2	2	-	-	-	-
Totals:	841	28,596,892	442	100,686,535	404	26,768,211

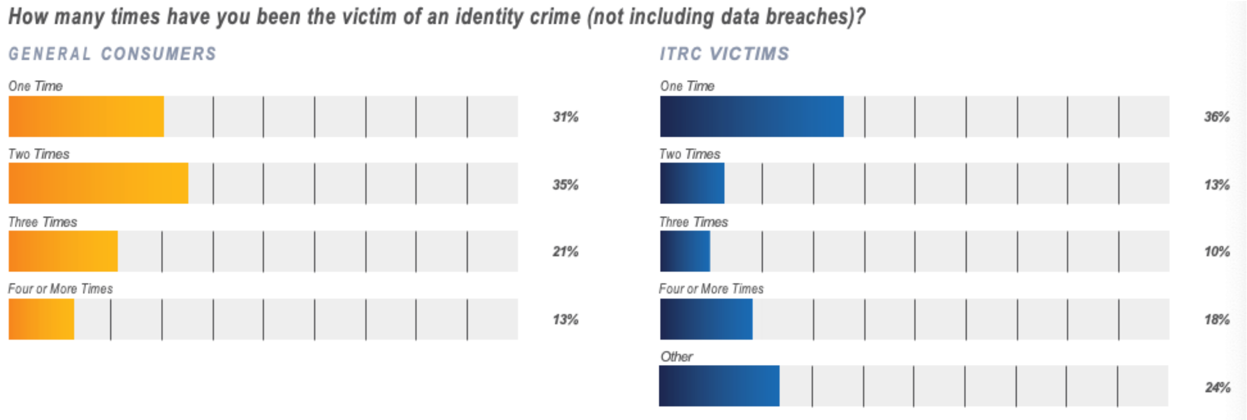
SOURCE: ITRC Q1 2024 Data Breach Analysis, April 2024

The trend of fewer individuals being impacted is somewhat offset by the fact individuals were likely to be the victim of multiple data breaches in 2023. Breach victims are also more likely to be the victims of identity misuse.



SOURCE: ITRC Consumer Impact Report, August 2023

In fact, there is a general victim impact trend where more individuals are reporting multiple instances of identity misuse as part of a single event in addition to being victimized multiple times. In 2021, 29 percent of victims who contacted the ITRC reported being the victim of previous identity misuse. By 2023 that number was 41 percent. The number is even higher among the general population who do not contact the ITRC for help – 69 percent (69%):



SOURCE: ITRC Consumer Impact Report, August 2023

From a financial standpoint, in 2021 only nine percent (9%) of victims of identity crimes lost more than $10,000, with 35 percent of victims losing less than $500. Today, nearly two-thirds of victims report losing more than $500 with 30 percent (30%) reporting losses of $10,000 or more. For the first time in the ITRC's 25-year history, we now routinely receive reports of six and seven-figure losses due to identity-related scams.

The most troubling trend, though, is the dramatic rise in the number of individuals who contemplate self-harm as a result of being the victim of an identity crime.
When we discussed the wide range of identity crime impacts during the 2021 committee hearing, the number of victims who contemplated suicide had jumped from a 20-year norm of two to four percent (2-4%) to eight percent (8%) during the pandemic.

Today that number stands at 16 percent (16%) with no sign of slowing. And, unlike past years, we now regularly receive phone calls from grieving family members whose loved one took their own life - and are still being attacked by the same identity criminals seeking to keep the scam alive. From fake go-fund-me campaigns to raise money for funeral expenses to continuing to post from the deceased person's social media account to draw other people into the scam, victims are losing their life savings and their lives at the hands of identity criminals. Here's an example.

All of these impacts bring us back to the topic at hand: Can we reduce the number of identity crimes and crime victims with better cybersecurity and data protections?

The short answer is yes.

First, let me make it clear that the ITRC does not advocate for or against any particular legislation or regulation. We do, however, provide objective information on the underlying issues prompting a proposed or active policy. With that in mind, the ITRC continues to believe that the best way to help identity crime victims is to prevent victimization in the first place.

And, the best way to prevent victimization is to prevent the loss of personal information in data breaches in conjunction with making stolen personal information less valuable to criminals. To do that we still believe we need:

- Minimum cybersecurity and data protection standards, including regular risk assessments
- Enforcement of cybersecurity and data protection laws and regulations backed by audits
- A new way of addressing data breach notices

And I'll add a fourth item: Protect the appropriate uses of information and enhance anti-fraud and identity verification with the responsible use of biometrics to devalue stolen personal information.

Let me take these one by one:

Having uniform minimum standards for data security and protection that can be routinely measured is the price of entry to a world where software is part of every aspect of our lives. Our cars are computers on wheels. Our phones aren't just used for talking. The toothbrush I just bought is software-driven and I paid for it with a credit card that has a chip in it.
We've seen the tragic results of poor software in the aviation industry, and we know the risks if a rogue actor or Nation/State exploits critical infrastructure.

It's not just software that runs things that benefits from minimum standards and data protection practices. So can the information that makes up each and every person's identity today.

In 2019, the ITRC did not track a single data breach attributed to a Zero Day[1] software flaw.
By 2021, there were 4; in 2022 there were 8. In 2023 there were more than 100 data breaches caused by a bad actor exploiting a software bug the developer or security professionals did not

know existed. Once considered rare, advanced tech like AI is making Zero Day attacks easy to plan and execute.

Once a software flaw is known, it can take months to apply a patch to enterprise software used to operate every aspect of businesses. The larger the company, the longer it takes to patch a known flaw, all the while hoping a bad actor does not discover an unpatched bug.

The ITRC and other security researchers have all identified a steep rise in data breaches from unpatched software. If the worst-case scenario does occur and a flaw is exploited, security teams likely won't know about the attack until it's been underway for an average of 204 days, according to IBM. It will still take another 73 days to contain the attack.

With the advent of AI, defenders have the tools to help find bugs and resolve attacks faster. But technology is agnostic – users are not. Bad actors also have tools to help find and exploit the inevitable bugs that make their way into production versions of software. Just last month (April 2024), the University of Illinois announced a discovery that allows generative AI to develop malware to take advantage of a software flaw just by reading the public alert used to notify software users of the vulnerability.

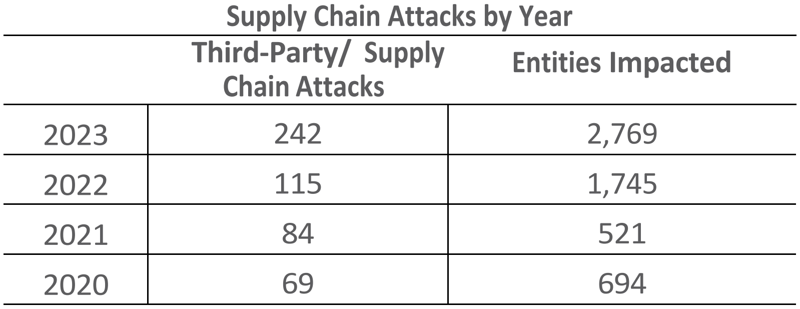
Minimum standards may also help reduce the number of so-called Supply Chain Attacks against third-party organizations that store or have access to the data of customers or partners. These smaller organizations tend to have fewer security resources and protections, but access to personal information from large and/or multiple entities.

From an identity criminal's perspective, a supply chain is Nirvana. Why risk getting caught or expend the time and energy to attack a large, well-defended organization when you can attack a vendor with fewer protections and the data of hundreds of organizations?

In the most recent ITRC data breach report from January 2024, we noted a steady increase in Supply Chain attacks over time.

[1] A Zero Day software vulnerability is one that is discovered after software has been released into production. The term is commonly associated with cyberattacks.

Since 2020, the number of organizations impacted has surged by nearly 300 percent (300%)



Supply Chain Attacks by Year

	Third-Party/ Supply Chain Attacks	Entities Impacted
2023	242	2,769
2022	115	1,745
2021	84	521
2020	69	694

SOURCE: ITRC 2023 Data Breach Report, January 2024

The chart illustrating the growth in Supply Chain Attacks includes organizations impacted by one of the largest third-party vendor attacks ever – a 2023 attack against the company that offers the MOVEit file transfer software and service. Cybercriminals exploited previously unknown flaws in software and cloud versions of MOVEit used by businesses, governments, schools, hospitals and other organizations around the world to securely share documents and information.

In Q1 2024, the number of organizations impacted by Supply Chain Attacks more than tripled compared to the same period in 2023. Fifty (50) new attacks in the Quarter impacted 243 organizations compared to 73 entities in Q1 in the previous year.

The United Healthcare/Change data breach will most likely turn out to be the largest Supply Chain attack we've ever seen just due to the sheer number of organizations in the Change supply chain and the number of individuals served by them.

These are examples of what happens when we do not have uniform, minimum standard for collecting, processing, and storing personal information. The recent discussion draft of the proposed American Privacy Rights Act (APRA) includes concepts already in place around the world and in some state laws and regulations. In particular, data minimization, risk assessments and routine audits to ensure organizations are continually adapting to ever-changing risks.

Data minimization is predicated on a simple truth: you cannot lose control of information you don't have or haven't secured. The logic is not complicated. If you don't need the information to complete a business transaction, don't collect it. If you need it, delete it as soon as the transaction is completed unless you are required to keep it. If you must keep the information, make sure it is secure and encrypted.

Routine risk assessments help ensure information and systems are secured in a manner equal to the risk an organization faces. Add two other complementary concepts - privacy by design and security by default – to help keep privacy and security at the forefront of every stage of the product lifecycle.

An organization that embraces these actions also has the foundation to build a company culture that ensures Security and Data Protections are not just departments, but integral parts of every team member's job.

This leads to the second and third points: To be effective in reducing identity crimes, uniform standards need strong enforcement backed by routine audits. Cybersecurity is a race between attackers and defenders. Defenders must continually measure their progress and constantly adjust to the new risks at hand. An audit becomes part of the roadmap for building the defenses needed to keep pace with aggressive attackers.

The need for strong enforcement actions also applies to data breach notices which are increasingly ineffective.

Today, data security regulations are limited, compliance is weak and enforcement is spotty. Whether there are consequences for non-compliance written into regulations or disciplinary actions taken by regulators depends almost exclusively on geography and/or industry.

There are fines in the healthcare industry because HIPAA includes the ability to assess penalties when cyberattacks or data breaches result in personal health information being exposed. The Securities and Exchange Commission can, and does, take enforcement actions for failing to adequately secure data and systems that have a material impact on investors. The Federal Communications Commission also has a set of enforceable cybersecurity and data protection regulations.

Individuals and groups of state attorneys general also litigate following major data breaches. A few states have also adopted separate health and biometric data protection laws.

There is ample evidence to support the conclusion that the vast majority of breaches may go unreported; there are few if any consequences for non-compliance; and, breach notices increasingly contain little to no help helpful information for victims and other organizations seeking to avoid a similar attack. For example:

- From 2018 until 2021, 100 percent (100%) of data breach notices tracked by the ITRC included information about the root cause of the attack and a majority also included the number of victims impacted. Since Q4 2021, that number has dropped to the point where in Q1 2024, only 32 percent (32%) of data breach notices linked to cyberattacks contained information about the cause of the attack.

- In late 2023, following an SEC investigation and litigation by state attorneys general, tech services provider Blackbaud admitted that client information of more than 13,000 organizations had been compromised, but only 604 data breach notices were tracked by the ITRC. (Blackbaud was also fined for making false statements about the type of information exposed in the data breach, for making misleading statements about when they knew the information to be false, and for failing to secure sensitive personal information which it had earlier denied).

- An average of nine (9) new data breach notices were issued each day in 2023 in the United States. In the European Union in 2023, the daily rate of new data breach notices was 335 due to the uniform requirements of the General Data Protection Regulation (GDPR).

I would offer one final thought. Adopting data minimization and giving consumers more access and control over their personal information for certain uses are vitally important parts of data protection. These practices can significantly reduce the amount of unnecessary personal information at risk of a data breach and misuse by criminals.

However, there are also important uses of personal information that help ensure identity information is only used by the true person who owns that identity. Personal information, used responsibly and transparently, is important for proving a person is who they claim to be in a wide variety of transactions – from opening bank accounts to applying for government benefits, as examples.

Restricting the use of personal information for identity verification and fraud prevention would have the unintended effect of aiding identity criminals and negatively impacting communities that already are disproportionately affected by identity crimes. A two-year study by the ITRC revealed the challenges facing Black communities that would be made worse if the tools needed to accurately identify a person were restricted.

Data enhanced with tools such as biometric verification (not recognition) have the potential to reduce the value of stolen identity information. That, in turn, would reduce the incentive for criminals to steal the information in the first place and render already stolen information useless in verification processes.

Thank you for your time and attention. I look forward to answering your questions.