Testimony of the Identity Theft Resource Center
Before the United States Senate Committee on Commerce, Science, and Technology
10 am October 6, 2021

The connections between cybersecurity, data breaches, and identity crimes

Delivered by James Everett Lee, ITRC Chief Operating Officer

Introduction

Good morning, Chair Cantwell, Ranking Member Wicker and members of the Committee. 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 the past 21 years, the ITRC has offered free assistance to victims of identity crimes. Through our contact center staffed by trauma-informed advisors, about 11,000 times per year we directly help victims recover their identities that have been stolen or otherwise compromised and we help consumers who want to prepare for the day when their personal information is acquired or misused by identity criminals.

Through our website and outreach programs, we help educate an additional one million people around the world who hold U.S. identity credentials, including military personnel, on how to protect their identity 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 noticed data breaches and other forms of identity data compromises. What started as a handful of data points 16 years ago with a single company notice has grown into a database of more than 13,000 data breaches with as many as 90 data points per event that is updated daily.

We also publish an annual data breach report and quarterly updates that analyzes the trends reflected in the data breach notices mandated by state law and federal regulations. In fact, earlier today, we published our *Q3 Data Breach Analysis* which shows we have already surpassed the total number of U.S. data compromises reported in full-year 2020. We are only 238 data compromises from tying the all-time record set in 2017. You'll find the full report as an attachment to my written testimony. **Exhibit A: *Q3 2021 ITRC Data Breach Analysis - October 6, 2021***

I would like to briefly mention two additional reports that we publish. First, our Consumer Aftermath Report is the only comprehensive study on the total impact of identity crimes on consumers. I will reference our most recent findings report later in my remarks and the full report is attached as an exhibit. **Exhibit B: *2021 Consumer Aftermath Report, May 2021***

Later this month, which coincidently is Cybersecurity Awareness Month, we will publish our first report on the impacts of security and data breaches on small businesses and solopreneurs including gig workers. Our *Business Aftermath Report* is the first independent research of its kind that is based on information taken directly from small business owners and leaders.

Finally, as a non-profit, the ITRC is funded primarily through grants from the Department of Justice, Office of Victims of Crime as well as private contributions and corporate sponsorships. We work closely with key federal agencies on issues that involve identity crime victims including the Federal Trade Commission (FTC), the Internal Revenue Service's Security Summit, the Pandemic Response Accountability Committee (PRAC), the Department of Homeland Security (DHS), and numerous state and local law enforcement agencies. For example, the FTC has referred more than 20,000 victims of the most complex identity theft cases to us to provide the specialized support many ID crime victims require that government agencies and large for-profit companies are not equipped to address.

The connection between cybersecurity, data breaches, and identity crimes

Our job, every day, is to talk with victims of identity crimes. The information I'm going to share with you today is largely based on what we learn from people directly impacted by these crimes. These interactions also influence our advice to the Committee today.

When the ITRC was born two decades ago, the primary source of identity crimes was physical – stolen mail, a lost laptop, dumpster diving, shoulder surfing, a file folder left on a desk, or a filing cabinet left unlocked. The criminal was likely someone you knew or shared a connection.

Even when California passed the first data breach notice law, the first nationwide data breach notice didn't involve a cyberattack – it was the result of organized criminals setting up a legitimate-looking insurance business for the purpose of ordering paper copies of credit reports from a data broker. My how things have changed.

Today, the primary source of data compromises involving personal information is related to cyberattacks launched by professional criminals outside the US or by Nation/States. Of the 1,291 publicly reported data compromises so far in 2021, 1,111 are the result of a cyberattack. The number of ransomware-related data compromises reported so far in 2021 *exceed* the number of similar events in 2020 & 2019 *combined*. It should be noted that the 1,111 cyberattack-related data events reported so far this year is more than *all data compromises in full-year 2020*.

The chart below from the *Q3 Data Breach Analysis* shows the various ways data compromises occur and the most common attack vectors used by cybercriminals. Far and away phishing and related attacks followed by ransomware are the most common forms of cyberattacks that lead to data compromises.

Attack Vector 2021 YTD vs. Full Years 2020 & 2019

Attack Vector	2021 YTD	2020	2019
Cyberattacks	**1,111**	**878**	**928**
Phishing/smishing/BEC	370	383	490
Ransomware	244	158	83
Malware	103	104	112
Non-secured Cloud Environment	19	50	15
Credential Stuffing	12	17	3
Unpatched software flaw	2	3	3
Zero Day Attack	2	1	n/a
Other - not specified	359	162	222
System & Human Errors	**134**	**152**	**231**
Failure to configure cloud security	48	57	56
Correspondence (email/letter)	40	55	89
Misconfigured firewall	9	4	4
Lost device or document	7	5	19
Other - not specified	30	31	63
Physical Attacks	**35**	**78**	**118**
Document Theft	3	15	19
Device Theft	12	30	57
Improper Disposal	3	11	14
Skimming Device	n/a	5	4
Other - not specified	17	17	24
Unknown	**11**	**n/a**	**2**
TOTALS:	**1,291**	**1,108**	**1,279**

What has also changed over time is the type of data identity thieves want and how they acquire it. The last time we set an all-time high for data breaches in 2017, identity thieves wanted to Hoover up as much data as possible from as many sources as they could find.

Today, we see highly organized cybercriminals launching highly sophisticated attacks using automated tools. Data quantity is no longer the goal of an attack; data quality is. With the right information – primarily logins and passwords – cyberthieves do not need to engage in time consuming and risky attacks that exploit known, but unpatched software bugs. Using automated tools and data stolen in breaches, they can walk in the front door and have access to everything they need to extort an organization or take over the account of an individual.

As a result of this shift, we see more cyberattacks that impact fewer individuals in mass attacks. Make no mistake, though, individuals are still at-risk today.

We are moving from an era of identity theft where data is acquired and accumulated to a time of identity fraud where ID thieves monetize the data they've collected - with the occasional effort to refresh older information. The chart below shows the shift in terms of the number of data breach victims dating back to 2015.

Compromise Year-over-Year Totals		
Month	Compromises	Victims
2021 YTD*	1,291	281,451,400
2020	1,108	310,116,907
2019	1,279	883,558,186
2018	1,175	2,227,849,622
2017	1,529	1,827,986,798
2016	1,105	2,541,588,745
2015	785	318,276,407
*As of 9/30/2021		

Connecting the Dots

To connect the dots using a real-world example, let's discuss the dramatic rise in identity-related unemployment benefits fraud during the COVID-19 pandemic. Public and private sector estimates of the financial impacts vary from just short of $100B to nearly $400B in stolen benefits. The victims fall into two categories: those who needed benefits and were denied because a cybercriminal applied for the benefits first; and those who didn't lose their job, but someone applied for and received benefits in their name.

At the ITRC, we first noticed there was something unusual occurring when we began to receive phone calls from Washington State. In normal times, the ITRC receives fewer than 20 inquiries per year about identity-related unemployment fraud. Shortly after the federal unemployment subsidies went into effect, we began to see a call a day from the Seattle area. That soon increased to several a day, before leaping to more contacts in one month than we had seen from all 50 states in the previous two years. ***Exhibit C: Spreadsheet of 2020-21 ITRC Victim Stats by State***

In early 2020 Washington State had a robust unemployment benefits program and had recently upgraded its technology to a state-of-the-art system that allowed taxpayers to register for a single account to access all State services. The system included a credential verification process that relied on readily available information about a person – information that was available for sale in identity marketplaces along with known logins and passwords. It was very easy for cybercriminals to use stolen information to create a new State benefits account or redirect an existing account using data breach-fueled information.

The volume of applications overwhelmed the state teams responsible for auditing the applications for fraud, eventually leading to the decision to switch from identity verification before paying benefits to auditing for fraud after-the-fact. After one month, Washington state change their model and reports of fraudulent unemployment claims dropped dramatically, but not before more than $500M in fraud was identified in Washington State alone.

Since April 2020 through today, 98 Washington residents have sought the assistance of the ITRC to help them recover from government benefit related fraud. I've attached to these remarks a state-by-state breakout of residents who turned to the ITRC for assistance since 2019.

Soon, this scenario played-out in every state to one degree or another. Ironically, the states with technology dating back to the 1960s faired the best. And at least one state that upgraded mid-pandemic saw their cyber-related fraud increase AFTER they implemented a state-of-the-art system. From March 2020 to the end of September 2021, we logged 2,112 cases of unemployment identity fraud in all 50 states and the District of Columbia.

Behind all these numbers, though, are victims. Real people who were – and in some cases still are – suffering.

The ITRC's *Consumer Aftermath Report* from May of this year illustrates the impacts of this fraud on two distinct groups. However, as you will see, the impacts are not proportionate.

Victims whose identities were used to apply for benefits they didn't need were largely only inconvenienced. They are still at risk of future attacks, however, because their information has been compromised and is in the hands of known criminals who can use that information at any time.

Of course, they may not have known their identities were being misused until a debit card arrived in the mail loaded with unemployment benefits. Often-times the letter was followed by a call from someone claiming to be a representative of the State or issuing bank saying there had been a mistake and to send the card to a "special" address.

Or a victim or mail carrier would find someone trying to collect mail from their mailbox. In some incidents reported to the ITRC, as many as 50 debit cards per day would arrive by mail – each addressed to a different person. Others didn't learn their identities had been compromised until they received a 1099 form saying they owed taxes on benefits they did request or receive.

For the victims who needed those benefits but were denied the resources they were due, the impacts could be devasting. In following up directly with victims, we learned that:

- 40 percent were unable to pay their routine bills
- 14 percent were evicted for non-payment of rent or mortgage
- 33 percent did not have enough money to buy food or pay for utilities

- 13 percent were unable to get a temp or permanent job as a result of identity misuse

As of April 2021 when this survey of victims was conducted:

- 69 percent of victims denied benefits said their issues were still unresolved from 2020
- 75 percent of victims whose identities were used to apply for PPP loans had unresolved issues
- 82 percent of people who were the victims of benefits scams where they unknowingly paid a criminal to expedite their benefit payments had not resolved the issues from 2020.

And, the fraud continues to this day. A local television station here in Washington, DC reports that one local Virginia business continues to receive requests to verify unemployment claims – none of which are for actual employees of the company. In 2020 we opened 802 unemployment ID fraud cases. To date in 2021, the count stands at 1,296. In 2019, the count was 14.

All of these issues are directly linked to identity thieves stealing personal information. While it's not possible to always draw a direct line to a specific data breach, the broad-based attacks that impacted every state utilized data available in illicit identity marketplaces. Information placed there as a result of an organizational failure to prevent unauthorized access to consumer information, most often because of poor cybersecurity practices, procedures, or execution.

All of this begs a simple question with a complex answer: What can, and should, we do?

In the ITRC's view, all potential solutions begin from the same place: The status quo is broken. From there, we believe policymakers and industry leaders need to focus on three key areas to achieve the ultimate goal of any public policy: Protect our citizens and protect the homeland. Specifically, we recommend intense focus on three areas:

We need better cybersecurity standards and practices.
The cyberattacks against known, but unpatched flaws and the data breaches that result from them are largely preventable.

NIST has set a record each year since 2016 for the number of known software flaws that are assigned a risk rating in the National Vulnerability Database. We will set another record this year, too, most likely in excess of 19,000 known software bugs. There have already been 33 Zero Day attacks – cyberattacks exploiting a previously unknown software flaw - in calendar year 2021. That's 11 more than 2020.

Meanwhile, the average time to patch a known software bug in enterprise software or web applications is measured in months or years depending on the sector – while attackers can exploit a new flaw in a matter of hours or minutes. Without enforceable minimum standards, there is no incentive beyond headline avoidance and fear of post-breach litigation to motivate most organizations. The "it's cheaper to pay the fine" mentality is alive and well when it comes to cybersecurity.

There is an even more basic step that can be highly effective at keeping personal information out of the hands of criminals: don't collect the information in the first place. You cannot breach what you do not have. Americans have made it pretty clear when given a choice about opting in or out of data collection or sharing, most people will say "no thanks." An estimated six percent (6%) of US iPhone users opted-in to data tracking when given the opportunity to choose earlier this year. That's six percent of an estimated 116M people in the U.S.

We need better enforcement.
Victims deserve better enforcement mechanisms and we believe victims are best served when there are options for redress. Clearly, the sticking points here in Washington and the states that have considered their own privacy & security laws are the issues of private right of action and federal pre-emption. When regulators have the tools they need to fully enforce strong laws, everyone wins. However, in the environment where we operate today, some states are more aggressive in protecting their citizens than others, resulting in disparate impacts for the same crime based on where you live. Victims and businesses alike are well served when everyone knows the rules and faces the same consequences. And just like in other areas of public policy, a system where the government and the aggrieved share the ability to seek redress provides the options that helps everyone.

The current California privacy law – the CCPA - is an example of that shared authority. Only the California Attorney General may take an enforcement action under most provisions of the law – the exception being if a data breach is caused by a failure to provide adequate cyber security. Then the law sets a procedure by which an individual can seek a statutorily set level of damages. This limited right of action is included in the new privacy law overwhelming approved by voters in 2020 that will take effect in 2023. The new CPRA also allows a slightly expanded private right of action if an email address and password are compromised in a data breach.

As for federal pre-emption, again we believe victims are best served by options. While we need minimum standards, technology moves faster than government. Giving state and local jurisdictions the ability to be responsive to new threats and technologies while maintaining a base of strong security and privacy is the kind of flexibility we believe helps victims and organizations, too.

Lastly on this point, our partners at the FTC are best equipped to be the enforcement agency for enhanced privacy and protection standards – if they are given the proper tools, mechanisms, and Congressional mandate.

Our victim notification system is wholly inadequate.
Please understand that what I'm about to say is not a rousing endorsement of the European Union's General Data Protection Regulation (GDPR). But, one area where the GDPR seems to be working is the breach notification system wherein organizations are required to provide notice to regulators and, ultimately, citizens if appropriate.

Why do I say this is a model worthy of exploration? The concept of a U.S. data breach notice law was first proposed in 2003 by a certain senator from Washington. Congress did not adopt the law, but California lawmakers took notice and passed the world's first data breach notice law that same year. It became effective in 2004. In 2005, "data breach" entered the popular lexicon for the first time when a company where I was an executive issued the first nationwide breach notice under the theory that data doesn't respect dotted lines on a map…and with a little friendly persuasion from Sens. Markey and Blumenthal in their previous roles.

By the way, that breach was quaint by today's standards - 156,000 potential victims, as Ms. Rich may remember - and would not even meet the threshold for issuing a data breach in some states today. Over the next 13 years, 90 other countries adopted data breach laws before the final two states required breach notifications in the wake of the Equifax compromise in late 2017.

I already mentioned that the ITRC database reflects some 13,000+ data breach notices accumulated over 16 years. The current average number of breaches reported in the US is about 5 per day. The average number of data breaches reported in the EU under the GDPR is 331 per day as of January 2021. Couple that with the estimated 15B stolen logins and passwords available for sale in identity marketplaces and it's obvious the number of US data breaches are being under reported.

When they are reported, the notices are largely meaningless with little transparency or actionable information. A recent study by the University of Michigan and a second by Carnegie Melon University both show that we simply are not equipping victims with enough information about what happened and how to protect themselves. The vast majority of breach victims simply do nothing.

The Michigan study concluded that even after receiving a breach notice, most people in the study did not know their information had been compromised at least three times. The Carnegie Melon study showed that most people who receive a data breach notice do not take even the basic step of changing the password on a compromised account; and if they do, it's generally months after receiving the breach notice and the replacement password is weaker than the original.

Mandatory reporting with strong penalties for failing to comply with both the required form and substance of a notice along with a bias toward more transparency will make a difference in terms of equipping victims with the knowledge needed to protect themselves and their loved ones from future data compromises.

Conclusion

In our view, today's hearing is ultimately about how we reduce the number of identity crime victims. Yet, there is a separate conversation needed about how we support people when they are victimized. The victim support system we have today is just as inadequate as our cybersecurity standards, our enforcement structure, and our system of victim notification. The ITRC would love to engage with you on this topic, too.

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