PERSONAL IDENTITY INSURANCE: COVERAGE AND PRICING IN THE U.S.[1]

DANIEL W. WOODS | Lecturer in Cyber Security, School of Informatics, University of Edinburgh

ABSTRACT

Personal identity theft occurs when a criminal uses stolen personal identifiers to manipulate third parties into taking actions under the false belief they are communicating with the individual whose identity has been stolen. A typical example is the criminal taking a loan out under the stolen identity. A market for personal identity insurance has emerged to mitigate the associated harms. We extract 34 personal identity insurance products that were uniquely filed with regulators in the U.S. We conduct a content analysis on the policy wordings and actuarial tables. Analyzing the policy wordings reveals that personal identity theft causes a number of costs in terms of monitoring credit records, lost income and travel expenses, attorney fees, and even mental health counseling. Our analysis shows there are few exclusions related to moral hazard. This suggests identity theft is largely outside the control of individuals. We extract actuarial calculations, which reveal financial impacts ranging from a few hundred to a few thousand dollars. Finally, insurers provide support services that are believed to reduce out of pocket expenses by over 90 percent.

1. INTRODUCTION

There is a risk of identity theft whenever third parties use personal identifiers to decide who to send funds to. For example, loans are typically extended to a specific individual, but this assumes the loanee can be reliably authenticated. Historically debt was issued by a member of the local community who could authenticate an individual via natural identifiers like face, voice, gait, and so on [Graeber (2012)]. Such identifiers are not available for online banking in which credit is extended to individuals in distant parts of the country or even abroad.

To solve this problem, lenders authenticate applicants via personal identifiers like passport details, social security numbers, address, and so on. These identifiers are presumed to be known by the individual alone. This assumption is flawed because billions of personal records have been lost in corporate data breaches over the last three decades [Edwards et al. (2016), Maochao et al. (2018)]. Criminals can use the stolen data to trick lenders into sending the loan payment to the criminal. The individual whose data was stolen, still unaware the loan was taken out, will then be pursued by the bank for repayment and their credit score will be damaged by missed repayments. The impacts include psychological harms (stress and anxiety), time spent resolving the theft, financial costs (increased interest rates due to lowered credit score), and more.

The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center received over fifty thousand reports of identity theft in 2021, which is 300 percent higher than in 2019 [FBI (2021)]. The total economic cost in 2021 is estimated to be U.S.$278 million, which amounts to over $5000 per incident [FBI (2021)]. Typical individuals will suffer an identity theft every 10 to 100 years, with the exact estimate varying based on the crime survey's methodology and target population [Woods and Walter (2022), Figure 11].

[1] This project was supported by the Willis Towers Watson Research Network. This research is supported by REPHRAIN: The National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (UKRI grant: EP/V011189/1).

The economic costs of identity theft raise the possibility that individuals may wish to insure against the consequences of identity theft. We collect a sample of 34 policies from a regulatory database covering U.S. states. We conduct an inductive content analysis of the policy documents and pricing algorithms, which allows us to answer the following:

RQ1: Which harms are covered by personal identity insurance?

RQ2: What is the implied likelihood and severity of each harm?

RQ3: How do insurers justify the scope and pricing of coverage?

The insights could help individuals to manage privacy risk by evaluating the effectiveness of transferring the consequences to an insurer. Individuals may be further supported by the risk-reduction services that are often provided along-side insurance [Thoyts (2010)]. Thus, one could consider privacy insurance as a form of privacy enhancing technology (PET), despite being a financial product that diverges considerably from the usual technical approach (PETs) [Heurix et al. (2015)]. The study also sheds light on an emerging field of technology insurance that covers cyberattacks [Romanosky et al. (2019)], crypto assets [Zuckerman (2021)], cyber bullying [Kshetri and Voas (2019)] and artificial intelligence liability [Lior (2022)].

Section 2 describes how we collect and analyze the empirical data, Section 3 presents the results, Section 4 discusses how these relate to cyber risk and insurance, and Section 5 offers a conclusion.

2. METHODS

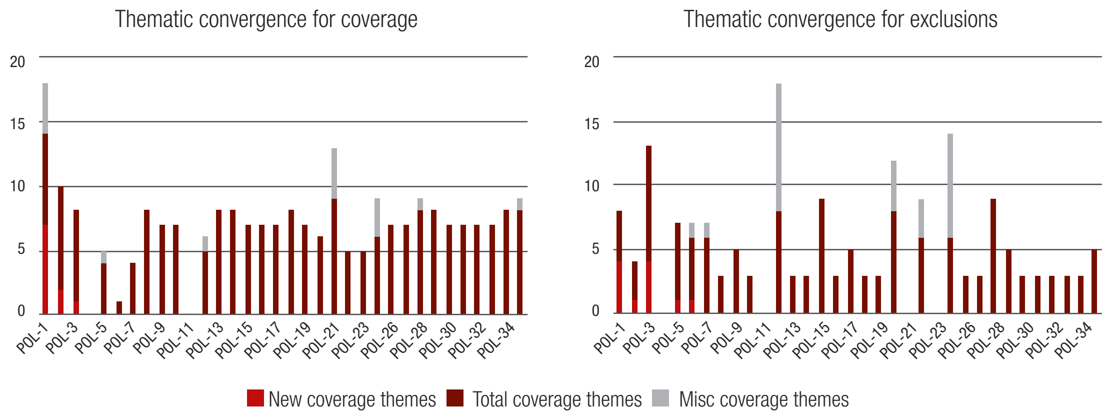
We adopt the high-level approach that was used by Romaonsky et al. (2019) to understand corporate cyber insurance. This involves sampling insurance regulatory filings from the SERFF database of the National Association of Insurance Commissioners (NAIC) until saturation is reached in terms of coverage [Campbell et al. (2020)]. Coverage themes are identified via an inductive content analysis [Elo and Kyngas (2008)]. We also map quantitative risk estimates to themes.

2.1 Sampling

We searched each state's filing system using the keyword "identity" and provided no further limitations on the search. We found identity insurance products filed under both commercial crime and homeowner insurance lines. Following the aforementioned study [Romanosky et al. (2019)], we only collected approved filings. We focused on the four largest states (California, Texas, Florida, and New York), as the greater market size provides more potential for thematic variation.

This resulted in 86 regulatory filings with meta-data including: state, submission date, companies, product name, and insurance line. We grouped filings to ensure each unit of analysis contained the policy wording, rating manual, and rating justification.[2] This resulted in 34 unique personal identity insurance filings. We did not double count when multiple insurance companies (often subsidiaries) filed together and did not count updated wordings as distinct insurance products, although we did track these changes. We stopped collecting policies when we stopped deriving new coverage themes [Campbell et al. (2020)].

Figure 1: The content analysis converged faster and more reliably for coverage than for exclusions, in part because some policies including long lists of seemingly irrelevant exclusions



Thematic convergence for coverage

Thematic convergence for exclusions

[2] Some companies filed these components in separately.

2.2 Analysis

We analyzed the policy wordings for RQ1 (i.e., which harms are covered by personal identity insurance?). We first read the document to identify high-level questions like who the policy was for and whether a help line was offered. We then extracted the sections describing what was covered and under which circumstances. These consisted of a list of contractual terms. We extracted each item as a unit of analysis.

We then mapped each unit of analysis to a theme. Themes had to be derived inductively due to the lack of prior research [Elo and Kyngas (2008)]. We created a theme for each unit that could not be classified under an existing theme. After analyzing 10 policies, we consolidated themes to ensure they were comprehensive and mutually exclusive [Stemler (2000)] and used the resulting codebook for the entire analysis. Figure 1 highlights how we quickly reached saturation in coverage but required more policies to do so for exclusions.

To answer RQ2 (i.e., what is the implied likelihood and severity of each harm?), we extracted all quantitative risk estimates from the rate schedules. Due to the simplicity of the pricing schemes, estimates can be classified into the following categories: likelihood and severity of the harm, pure premium (risk = likelihood severity), and market premium that includes the insurer's expenses and profit.

To understand how coverage and pricing were derived (RQ3), we read any documents that justified pricing algorithms. We also included selective quotes from insurer's justifications.

3. RESULTS

Section 3.1 describes what is covered and excluded by personal identity insurance. Section 3.2 identifies quantitative estimates and justifications.

3.1 Coverage and exclusions

Our inductive analysis identified nine specific categories of coverage and classified the remaining 14 coverage items into a miscellaneous category. The resulting analysis is summarized in Table 1. The core coverage consists of different costs associated with correcting official records related to the policyholder's identity. The costs of credit services (Theme #1), like reports or monitoring, was mostly covered by the policies, with those offered in the early years limiting the number of reports. Almost all policies indemnify the cost of refiling loan applications (Theme #2) and communications costs (Theme #3), like long distance phone calls or notarizing documents incurred to "amend or rectify records as to your true name or identity". The costs of traveling to do so (Theme #4) was occasionally included. The time lost while traveling is commonly indemnified as lost income (Theme #5) and/or alternative care arrangements (Theme #6). Another common cost was attorney fees and court costs (Theme #7) resulting from the defense of a civil suit, civil judgment, or criminal charges brought against the policyholder.

Displaying the policies longitudinally captures how identity insurance expanded coverage over time. For example, mental health counseling (Theme #9) did not appear until 2014, after which it was included in the majority of policies. Policies also began to include clauses offering to cover all reasonable costs "to recover control over his or her personal identity" (Theme #10), although this clause usually explicitly excludes coverage for lost or stolen money. The only area of coverage retraction is the cost of hiring professionals to help investigate and manage personal identity thefts (Theme #8), which were only included in the early years. Such services may now be "free", meaning they do not count towards coverage limits.

It is worth unpacking the coverage items classified as miscellaneous. POL-1 and POL-21 were introduced by the same insurance company in different states and they included coverage for: liabilities resulting from fraudulent transactions using existing accounts or accounts opened in the policyholder's name, any costs "incurred by a financial institution or credit issuer," and the deductible payment for any other personal identity insurance. POL-12 and POL-25 included a clause covering "credit freeze, credit thaw costs, transcript costs, appeal bond, court filing fees, expert witness or courier fees." POL-25 also covered the costs of replacing "identification cards" and "ordering medical records" (as did POL-28), although both of these items likely overlap with the communication cost's theme. Finally, POL-35 explicitly included "costs approved by us, for providing periodic reports on changes to, and inquiries about the information contained in the insured's credit reports or public databases (including, but not limited to credit monitoring services)," which is likely to mainly consist of credit services (Theme #1).

Turning to the exclusions, Table 2 displays the exclusions discovered in the sample. All but one of the policies exclude losses due to business identity theft, which confirms these

Table 1: The coverage offered by each policy ordered by date of filing

DATE	POL	CREDIT SERVICES	APPLICATION COSTS	COMMUNICATION COSTS	TRAVEL COSTS	LOST INCOME	CARE EXPENSES	ATTORNEY FEES	PROFESSIONAL SERVICES	COUNSELING	REASONABLE COSTS	MISCELLANEOUS
11/07/05	5	6	✓	✓				✓				
06/21/06	7	12	✓	✓				✓				
03/26/07	6								✓			
01/08/08	20		✓	✓		✓	✓	✓	✓			
05/13/08	1	4	✓	✓		✓	✓	✓				4
08/24/08	21	4	✓	✓		✓	✓	✓	✓			4
04/20/10	29	✓	✓	✓		✓	✓	✓	✓		✓	
03/10/11	31	✓	✓	✓		✓	✓	✓			✓	
07/11/11	22	✓	✓	✓		✓		✓				
02/12/13	32	✓	✓	✓		✓	✓	✓			✓	
03/13/14	27	✓	✓	✓		✓	✓	✓			✓	
05/01/14	25	✓	✓	✓		✓	✓					3
05/16/14	14	✓	✓	✓		✓	✓	✓		✓	✓	
05/29/14	2	✓	✓	✓		✓	✓	✓		✓	✓	
07/01/14	26	✓	✓	✓		✓	✓	✓			✓	
09/24/14	35	✓	✓	✓	✓	✓	✓	✓				1
02/26/15	13	✓	✓	✓		✓	✓	✓		✓	✓	
03/06/15	8	✓	✓	✓		✓	✓	✓		✓	✓	
04/04/15	18	✓	✓	✓		✓	✓	✓		✓	✓	
06/30/15	34	✓	✓	✓		✓	✓	✓		✓	✓	
08/07/15	16	✓	✓	✓		✓	✓			✓	✓	
08/07/15	19	✓	✓	✓		✓	✓			✓	✓	
08/27/15	30	✓	✓	✓		✓	✓			✓	✓	
09/15/15	12		✓	✓		✓		✓				1
12/30/15	10	✓	✓	✓		✓	✓			✓	✓	
12/31/15	3		✓	✓	✓	✓	✓	✓		✓		
01/08/16	15		✓	✓	✓	✓	✓	✓		✓		
01/19/16	28		✓	✓	✓	✓	✓	✓		✓		1
09/09/16	33	✓	✓	✓		✓	✓	✓			✓	
09/15/16	23		✓	✓	✓	✓		✓				
02/03/20	9	12	✓	✓		✓	✓	✓			✓	
02/03/20	17	12	✓	✓		✓	✓	✓			✓	

Integers denote the maximum number of credit reports in the credit services column and the number of coverage items in the miscellaneous column.

policies are intended to cover losses suffered by individuals. Most policies include reporting requirements, such as filing a police report or notifying within 30-120 days. Many of the exclusions are included in other insurance policies, such as not covering losses when the policyholder had prior knowledge of the loss or when the loss is incorrectly reported. The fraud exclusion denies coverage for events caused by the insured or an acquaintance with the insured's knowledge, but a handful of policies also excluded losses committed by close acquaintances without the insured's knowledge, a form of insider threat.

Some of the exclusions are unlikely to cause or constitute personal identity harms. For example, the conflict/political column includes exclusions for losses due to war and political actions, the disaster column includes both natural and nuclear incidents, and bodily injury covers physical harm to a person. Neither war, nuclear accidents, or bodily harm are likely causes of or outcomes from personal identity theft. The miscellaneous exclusions are similarly tenuous, such as "loss from games of chance" (POL-25) and "loss of valuable papers, valuable documents, jewelry, silverware and other personal property..." (POL-12). Corporate cyber insurance policies have been shown to also include a wide range of seemingly irrelevant excluded events [Woods and Weinkle (2020)].

Insurance theory predicts policies will exclude activities that increase risk, known as moral hazard [Baker (1996)]. In addition to not lying (Fraud theme) and reporting swiftly and to the police (Reporting theme), the computer security theme captures such exclusions. This typically covered voluntary disclosure, which POL-3 defined as "disclosure of any code or other security information that can be used to gain access to any of your accounts...this exclusion will not apply if such disclosure was made when you were under duress or the victim of fraud." Thus, the most salient moral hazard is that a policyholder willingly discloses information. Notably, only one of the policies (POL-7) from 2006 required the insured to maintain security software: "It is the responsibility of each "identity recovery insured" to use and maintain his or her computer system security, including personal firewalls, anti-virus software, and proper disposal of used hard drives."

One interpretation is that insurers learned that personal identity harm was rarely caused by the insured not following information security procedures.

3.2 Pricing and justifications

Table 3 displays our data about pricing and actuarial justifications. Notably, there is more missing data than in the previous section. Many of the filings missed actuarial justifications and some did not even report the premium. A study of corporate cyber insurance also found that policy wordings were more consistently included than pricing and actuarial data [Romanosky et al. (2019)].

The first column describes the annual price of personal identity insurance per insured entity, which ranges from U.S.$0.25 to over U.S.$100. This variance is not well explained by the amount of coverage, described in the next two columns displaying the associated limit (maximum insurance pay-out) and deductible (the first part of loss paid by the policyholder). Sometimes this was because the policy contained more coverage. For example, some of the higher prices result from bundling personal identity insurance with "$50,000 of Named Malware, and $5,000 of Public Relations Services" (e.g., POL-2, 14, and 26). Some of the lowest priced policies (e.g., POL-12 and 25) were intended to be sold in bulk (the bulk discount column) so that one organization purchases insurance for multiple individuals. The possibility that organizations purchase personal identity insurance on behalf of individuals explains the risk rated column, which contains a tick if different rates apply based on the insured's characteristics (e.g., the organization's industry).

The likelihood and impact column are purely based on actuarial expectations, unlike the premium that also reflects the insurer's business model, such as expense costs or investment income [Thoyts (2010)]. The estimates of frequency were more variable than the estimates of the impact. The lower frequency estimates resulted from normalizing the number of data fraud cases reported to the FBI by the U.S. population, whereas the higher values (e.g., 3.7 percent) came from normalizing the number of data fraud cases by the sample size of an FTC survey. Such disparities may result from the difficulties surveying rare and emotionally salient phenomena [Florencio and Herley (2013)].

Some policies even delimit the frequency and impact estimate for coverage themes identified in the previous sub-section. For example, POL-3 references data obtained from their reinsurer to estimate the frequency of: replacement of documents (0.05 percent), travel expenses (0.035 percent), loss of income (0.035 percent), child and elderly care

Table 2: The exclusions included in each policy ordered by date of filing

DATE	POL	BUSINESS IDENTITY	BODILY INJURY	CONFLICT/POLITICAL	FRAUD	PRIOR KNOWLEDGE	REPORTING	DISASTER	NON-IDENTITY	INSIDER THREAT	COMPUTER SECURITY	MISCELLANEOUS
11/07/05	5	✓			✓	✓	✓		✓	✓		
06/21/06	7	✓			✓	✓	✓		✓		✓	
03/26/07	6	✓			✓	✓	✓					1
01/08/08	20	✓	✓		✓	✓			✓	✓	✓	4
05/13/08	1	✓	✓	✓	✓							
04/20/10	29	✓		✓	✓		✓	✓				
03/10/11	31	✓			✓		✓					
07/11/11	22	✓			✓	✓			✓	✓		3
02/12/13	32	✓			✓		✓					
03/13/14	27	✓			✓		✓					
05/01/14	25	✓	✓		✓	✓		✓	✓		✓	8
05/16/14	14	✓			✓		✓					
05/29/14	2	✓			✓		✓					
07/01/14	26	✓			✓		✓					
09/24/14	35		✓	✓	✓		✓	✓				
02/26/15	13	✓			✓		✓					
03/06/15	8	✓			✓		✓					
04/04/15	18	✓			✓		✓					
06/30/15	34	✓			✓		✓					
08/07/15	16	✓			✓		✓					
08/07/15	19	✓			✓		✓					
08/27/15	30	✓			✓		✓					
09/15/15	12	✓	✓		✓	✓		✓	✓		✓	10
12/30/15	10	✓			✓		✓					
12/31/15	3	✓	✓	✓	✓	✓	✓	✓		✓	✓	
01/08/16	15	✓	✓	✓	✓	✓	✓	✓		✓	✓	
01/19/16	28	✓	✓	✓	✓	✓	✓	✓		✓	✓	
09/09/16	33	✓			✓		✓					
02/03/20	9	✓		✓			✓	✓			✓	
02/03/20	17	✓		✓			✓	✓			✓	

The final column displays the number of coverage items classified as miscellaneous.

Table 3: Pricing and actuarial information available for each regulatory filing

DATE	POL	PREMIUM ($)	LIMIT ($)	DEDUCTIBLE ($)	RISK RATED	BULK DISCOUNT	FREQUENCY	IMPACT ($)
11/07/05	5		15000					
06/21/06	7	100					1%	3000
03/26/07	6							
01/08/08	20	126.25						
05/13/08	1	60	15000				2%	1369
08/24/08	21	126	20000					422
09/30/09	4	15	10000			✓		
04/20/10	29							
03/10/11	31	19	25000	100				
07/11/11	22							
08/24/11	11							
02/12/13	32	20	15000	250				
03/13/14	27	28	15000				0.05%	1603
05/01/14	25	1.08	10000			✓		
05/16/14	14	81-299*	50000	2500	✓			
05/29/14	2	81-299*	50000	2500	✓			
07/01/14	26	81-299*	50000	2500	✓			
09/24/14	35							
02/26/15	13							
03/06/15	8	10	15000					
04/04/15	18	10	15000	100				
06/30/15	34	10	15000	100			0.01%	3015
08/07/15	16	10	15000	100			3.70%	1200
08/07/15	19	10	15000	100				
08/27/15	30	10	15000	100				
09/15/15	12	0.24	25000		✓	✓		
12/30/15	10	10	15000	100			3.70%	1200
12/31/15	3	1.54	25000				0.05%	1603
01/08/16	15							
01/19/16	28	2.93	25000					
09/09/16	33	16						
09/15/16	23	2.44	1000000				0.05%	3541
02/03/20	9	15	25000		✓	✓		
02/03/20	17	15	25000		✓	✓	3.81%	365

Empty fields should not be interpreted as anything other than missing data.

* = price for a bundle including additional coverage

(0.011 percent), reimbursement of fraudulent withdrawals (0.0250 percent), legal costs (0.03 percent), remediation service costs (0.05 percent), and case management service costs (0.075 percent). We advise that the relative frequencies are perhaps the main takeaway. For example, the child and elderly care costs are incurred less frequently than those to hire response services.

To provide a flavor of the actuarial reasoning, we quote the following from POL-10 extract in full: "According to a recent study commissioned by the Federal Trade Commission, 90% of "All ID Theft" out of pocket expenses are $1,200 or less. While we do not have significant experience with this coverage, we believe that the availability of case management restoration services will reduce this severity to approximately $81. The same FTC-commissioned report suggests a frequency of 3.7 percent. Thus, our loss content is expected to be approximately $3.00. Loss-related expenses (toll-free help-line and case management service) are expected to be $3.50. Thus our total loss cost is $6.50."

The most notable aspect is that case management services reduce out of pocket expenses by over 90 percent. Other data sources for actuarial justifications include: the Bureau of Labor Statistics, Ponemon group, Javelin's surveys, competitor analysis, and the FBI.

4. DISCUSSION

This section discusses the implications of our results, and then links these to related work.

4.1 Implications

The existence of personal identity insurance suggests individuals anticipate privacy harms that are not sufficiently remedied by the legal system. The following, which was included in multiple insurer's filings, summarizes the gap: "While many financial institutions provide protections to consumers for the actual fraud loss, most individuals have no help for the time and expense required to restore their personal identities."

The impact column of Table 3 suggests actuaries estimate the associated time and expenses to be around U.S.$3,000.

Interestingly, POL-10 believed post-theft services paid by the insurer could reduce such expenses by over 90 percent. This mirrors corporate cyber insurance in which policies pay for a team of consultants spanning law, IT, and public relations to respond to cyber incidents [Franke (2017), Woods and Bohme (2021a)]. More generally, scholars have observed insurers positively influencing risk management practices of insureds across a range of insurance lines, known as insurance as governance [Ericson et al. (2003), Ben-Shahar and Logue (2012)].

A provocative question to ask is whether governments could do more to help individuals recover from identity theft, after all, many thefts exploit state provided identifiers like social security numbers that cannot be easily replaced due to the government's architectural design choices. The bulk discounts in some policies suggests that these costs display considerable economies of scale. The equivalent post-incident services are provided publicly for fire, and were originally provided by insurers [Carlson (2005)].

In terms of the identifying new harms, the costs covered in Table 1 are driven by the complexity of bureaucracies. Coverage items include re-filing applications that were rejected due to identity theft, the cost of notarizing documents, lost income, or additional care expenses due to the time invested that individuals are normally expected to cover. A different kind of cost is mental health counseling, which was not offered until 2014 after which it was included in the majority of policies. Its inclusion suggests the insurance industry recognizes the psychological harm of victims of identity theft. It seems reasonable that anticipation of a U.S.$3,000 impact following a data breach might lead to anxiety, as argued by privacy scholars [Solove and Citron (2017)].

The actuarial estimates confirm that the impact of identity theft is relatively low but also relatively common. This diffuseness of harm has been identified as a reason why courts dismiss data breach lawsuits [Calo (2014), Citron and Solove (2022)]. The source of quantitative estimates is interesting in that actuarial justifications relied on public data collection (e.g., FTC surveys or FBI crime reports). One might ask whether governments collecting and releasing similar aggregate data for other privacy harms could help bootstrap private insurance markets. Or perhaps academics could reflect on what would be required for their surveys to be used for the same purpose.

More generally, our search was relatively narrow in that we used a small number of search terms. Future work could explore other lines of insurance related to privacy harms. It could also expand our analysis beyond the four largest states. We suspect the results will be similar as we detected few differences across states in terms of the content of policies or actuarial estimates, although the regulatory reports did differ.

4.2 Related work

The study also contributes to an emerging body of work investigating technology insurance products that cover cyber-attacks against firms [Romanosky et al. (2019)] and individuals, crypto assets [Zuckerman (2021)], cyber bullying [Kshetri and Voas (2019)] and artificial intelligence liability [Lior (2022)]. So far, corporate cyber insurance is the only technology insurance product with a developed body of literature.

Research into corporate cyber insurance has studied the processes to assess and manage cyber risk. Insurers collect information about the security practices of applicants for corporate cyber insurance [Woods et al. (2017), Nurse (2020)], (inconsistently) incorporate information into pricing [Romanosky et al. (2019), Talesh and Cunningham (2021)], and provide a range of post-incident support services [Wolff and Lehr (2018), Woods and Bohme (2021b)]. For comparison, identity insurance applicants are not required to reveal security practices. However, it does provide access to post-incident services, which this study did not explore.

Research into cyber insurance has also considered whether it improves social welfare and how this motivates different regulatory strategies [Lemnitzer (2021), Baker and Shortland (2022)]. These questions typically turn on whether insurers improve risk management processes. More research is required to answer whether personal identity insurance does so, although we have argued identity theft is largely outside the individuals' control. Another question is how insurance products evolve over time [Baker (2019)]. Identity insurance has broadened to include psychological support, but it does not cover many types of cybercrime identified in surveys [Woods and Walter (2022)]. It is unclear whether it will absorb such crimes in the future, or whether a novel insurance product will displace identity insurance.

5. CONCLUSION

The following extract, which was included word-for-word in multiple regulatory filings, provides a concise summary of our study: "While there are ways to reduce one's exposure to identity theft, it is a crime that can strike anyone. Those who are victims of this crime need to make identity recovery a top priority, because otherwise:

- Credit rating can be ruined
- Arrest warrants can be issued against the victim
- Liens can be applied against the victim's assets

While many financial institutions provide protections to consumers for the actual fraud loss, most individuals have no help for the time and expense required to restore their personal identities."

While the extract suggests there are "ways" of reducing exposure, Table 2 shows insurers do not push policyholders towards implementing them. One explanation is that identity theft risk reduction is too ineffective or too onerous to ask of policyholders. This supports a narrative in which consumers are powerless to prevent privacy harms resulting from personal identity theft. The corresponding insurance coverage reflects a need for ex-post response solutions to both reduce privacy harms and indemnify the financial cost.

Our study confirms one aspect of the privacy harm literature. Legal systems fail to recognize and remedy privacy harms [Citron and Solove (2022)] as evidenced by the emergence of a private market covering the harms associated with identity theft incidents. We provide an additional contribution, namely that the lack of support services leads individuals to suffer more harm. For example, one insurer anticipates case management services to lead to a 90 percent reduction in the cost of an identity theft incident. Thus, policymakers could reflect on whether the impacts of identity theft and the expertise to remedy are fairly distributed across society. The status quo in which financial smoothing and risk reduction services are privately provided undoubtedly skews towards affluent consumers.

REFERENCES

Baker, B., 1996, "On the genealogy of moral hazard," Texas Law Review, 75:2, 237

Baker, T., 2019, "Back to the future of cyber insurance," Professional Liability Underwriting Society 3:1, 5-6

Baker, B., and A. Shortland, 2022, "The government behind insurance governance: lessons for ransomware," Regulation & Governance

Ben-Shahar, O., and K. D. Logue, 2012, "Outsourcing regulation: how insurance reduces moral hazard," Michigan Law Review 111, 197

Calo, R., 2014, "Privacy harm exceptionalism," Colorado Technology Law Journal 12, 361

Campbell, S., M. Greenwood, S. Prior, T. Shearer, K. Walkem, S. Young, D. Bywaters, and K. Walker, 2020, "Purposive sampling: complex or simple? research case examples," Journal of Research in Nursing 25:8, 652-661

Carlson, J. A., 2005, "The economics of re protection: from the Great Fire of London to Rural/ Metro 1," Economic Affairs 25:3, 39-44

Citron, D. K., and D. J. Solove, 2022, "Privacy harms," Boston University Law Review, 102

Edwards, B., S. Hofmeyr, and S. Forrest, 2016, "Hype and heavy tails: A closer look at data breaches," Journal of Cybersecurity 2:1, 3-14

Elo, S., and H. Kyngas, 2008, "The qualitative content analysis process," Journal of Advanced Nursing 62:1, 107-115

Ericson, R. V., A. Doyle, and D. Barry, 2003, Insurance as governance, University of Toronto Press

FBI, 2021, "Internet Crime Report, 2021," Federal Bureau of Investigation

Florencio, D., and C. Herley, 2013, "Sex, lies and cyber-crime surveys," in Schneider, B. (ed.), Economics of information security and privacy III, Springer

Franke, U., 2017, "The cyber insurance market in Sweden," Computers & Security 68, 130-144

Graeber, D., 2012, Debt: the first 5000 years, Penguin

Heurix, J., P. Zimmermann, T. Neubauer, and S. Fenz, 2015, "A taxonomy for privacy enhancing technologies," Computers & Security 53, 1-17

Kshetri, N., and J. Voas, 2019, "Thoughts on cyberbullying," Computer 52:4, 64-68

Lemnitzer, J. M., 2021, "Why cybersecurity insurance should be regulated and compulsory," Journal of Cyber Policy 6:2, 118-136

Lior, A., 2022, "Insuring AI: the role of insurance in artificial intelligence regulation," Harvard Journal of Law and Technology 1:in print

Maochao, X., M., K. M. Schweitzer, R. M. Bateman, and S. Xu, 2018, "Modeling and predicting cyber hacking breaches," IEEE Transactions on Information Forensics and Security 13:11, 2856-2871

Nurse, J. R. C., L. Axon, A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese, 2019, "The data that drives cyber insurance: a study into the underwriting and claims processes," in 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), IEEE

Romanosky, S., A. Kuehn, L. Ablon, and T. Jones, 2019, "Content analysis of cyber insurance policies: how do carriers price cyber risk?" Journal of Cybersecurity 5:1

Solove, D. J., and D. K. Citron, 2017, "Risk and anxiety: a theory of data-breach harms," Texas Law Review 96, 737

Stemler, S., 2000, "An overview of content analysis," Practical Assessment, Research, and Evaluation 7:1, 17

Talesh, S. A., and B. Cunningham, 2021, "The technologization of insurance: an empirical analysis of big data and artificial intelligence's impact on cybersecurity and privacy," Utah Law Review 5

Thoyts, R., 2010, Insurance theory and practice, Routledge

Wolff, J., and W. Lehr, 2018, "Roles for policy-makers in emerging cyber insurance industry partnerships," 46th Research Conference on Communication, Information and Internet Policy (TPRC 46)

Woods, D. W., I. Agrafiotis, J. R. C. Nurse, and S. Creese, 2017, "Mapping the coverage of security controls in cyber insurance proposal forms," Journal of Internet Services and Applications 8:1, 8

Woods, D. W., and R. Bohme, 2021a, "How cyber insurance shapes incident response: A mixed methods study," in Workshop on the Economics of Information Security

Woods, D. W., and R. Bohme, 2021b, "Incident response as a lawyers' service," IEEE Security & Privacy 18:1

Woods, D. W., and L. Walter, 2022, "Reviewing estimates of cybercrime victimisation and cyber risk likelihood," in 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 150-162, IEEE

Woods, D. W., and J. Weinkle, 2020, "Insurance definitions of cyber war," Geneva Papers on Risk and Insurance-Issues and Practice 45, 639-656

Zuckerman, A., 2021, "Insuring crypto: The birth of digital asset insurance," University of Illinois Journal of Law, Technology & Policy, 75