State of Illinois
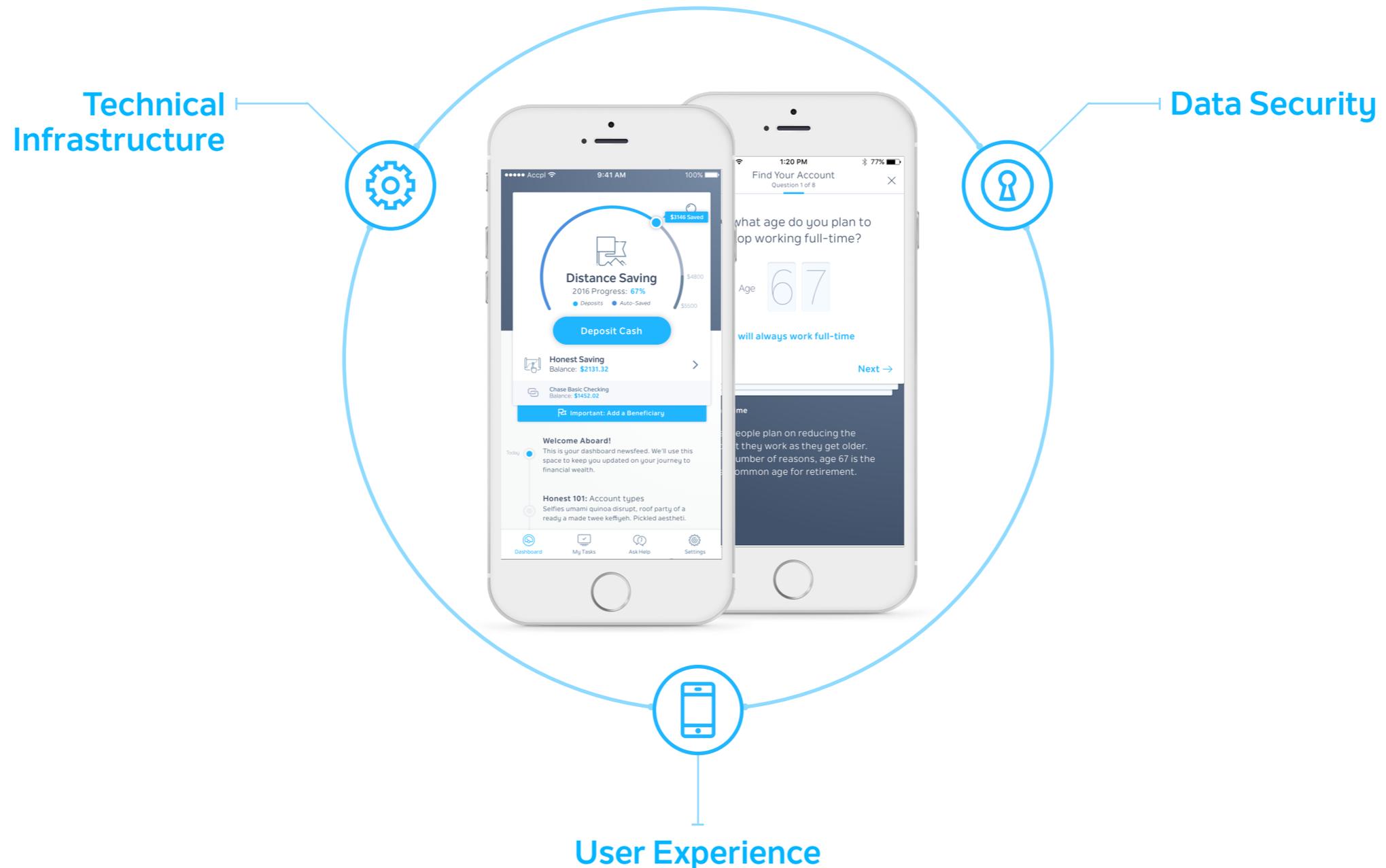# Secure Choice Program
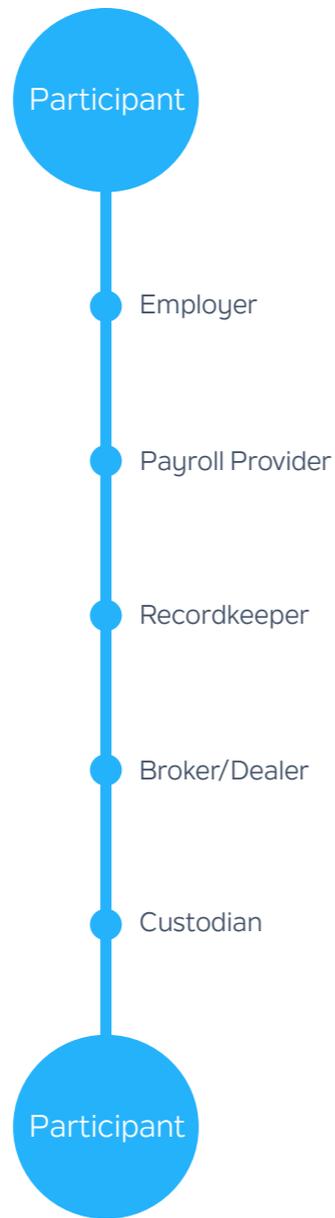
We do the work behind the scenes to make saving toward retirement simple, intuitive and effective.
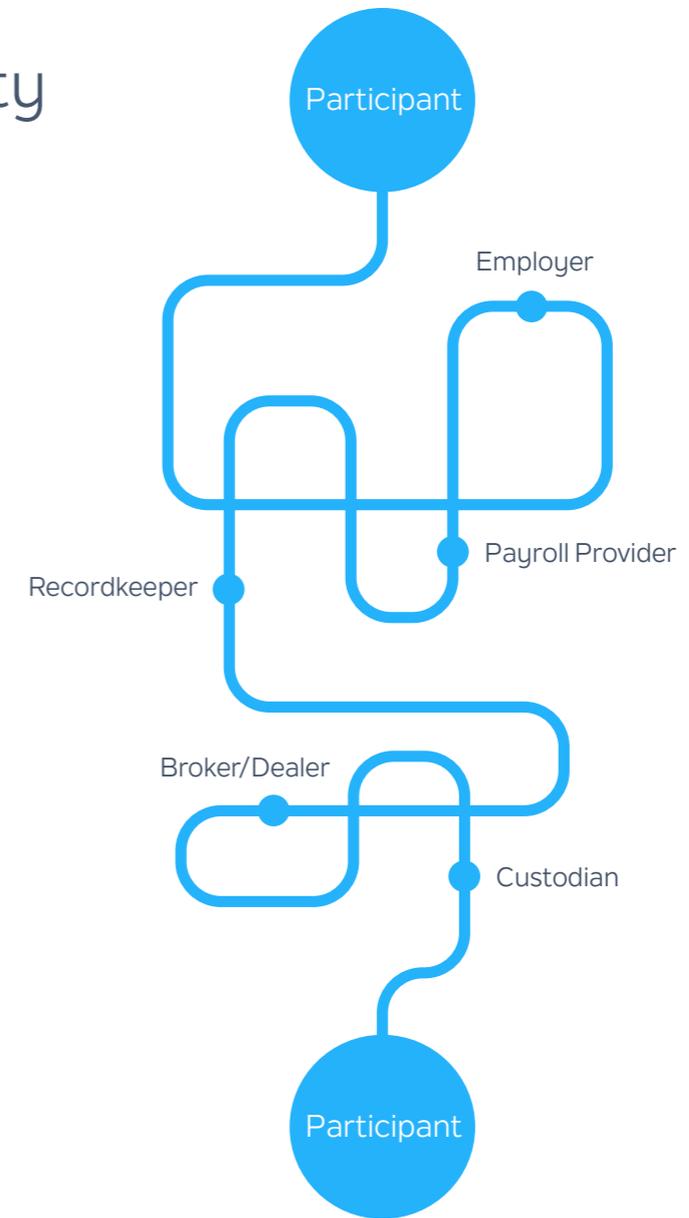

Technical Infrastructure

Data Security

User Experience

Honest Dollar is not providing legal, tech or any other advice.

Expectation vs. Reality

Expectation

Participant

Employer

Payroll Provider

Recordkeeper

Broker/Dealer

Custodian

Participant

Reality

Participant

Employer

Payroll Provider

Recordkeeper

Broker/Dealer

Custodian

Participant

HonestDollar | Goldman Sachs

Multiple Points of Contact

All Parties Reconcile Data

Employer	Payroll Provider	Recordkeeper	Broker/Dealer	Custodian

• Creates Employee data based on compensation and hiring strategy
 	
• Passes data to Payroll Provider & Recordkeeper
 	
• Responsible for reporting to State Agency in compliance with legislation
	• Collects participant income data from Employer
	
	• Sends data to Recordkeeper & Accountant
	
	• Reconciles data from Recordkeeper
	
	• Provides contribution data to Recordkeeper
		• Collects & reconciles data
		
		• Instructs trades to Broker/Dealer
		
		• Provides portal for plan sponsor & employee
			• Brokers trades
			
			• Reconciles trade activity
			
			• Sends trades to market/ fund company
			
			• Reports trades to Self-Regulatory Organization
			   • SEC
			   • FINRA
			   • Etc.
				• Holds Plan Assets
				   • Cash
				   • Investments
				
				• Issues Statements/ Confirms
				
				• Reports Balances to Recordkeeper

InfoSec

Deep dive into security incident data by industry.

Vulnerable Code Is Everywhere

VULNERABILITY CLASS BY LANGUAGE (PERCENTAGE)

	ASP	ColdFusion	.NET	Java	Perl	PHP
Cross-Site Scripting	49	46	35	57	67	56
Information Leakage	29	24	44	15	11	17
Content Spoofing	5	4	5	8	6	7
SQL Injection	8	11	6	1	3	6
Cross-Site Request Forgery	2	2	2	4	4	2
Insufficient Transport Layer Protect	0.8	1	0.9	1	0.3	4
Abuse of Functionality	0.3	0.6	0.3	0.9	0.5	0.2
HTTP Response Splitting	0.9	3	0.8	2	0.8	0.3
Predictable Resource Location	0.1	0.1	0.0	0.2	0.1	1
Brute Force	0.7	0.3	1	2	0.8	1
URL Redirector Abuse	0.7	0.4	0.5	1	1	0.9
Insufficient Authorization	0.2	0.3	0.5	0.9	1	0.2
Fingerprinting	0.3	0.1	0.5	0.6	0.3	0.1
Session Fixation	0.2	0.3	0.2	0.6	0.1	0.3
Directory Indexing	–	–	0.0	0.0	–	0.3

It Gets Fixed Slowly

REMEDIATION TIME ON AVERAGE

	ASP	ColdFusion	.NET	Java	Perl	PHP	Ruby
Cross-Site Scripting	220	220	238	235	265	111	233
Information Leakage	354	110	250	180	292	136	687
Content Spoofing	267	187	232	238	185	99	79
SQL Injection	206	211	142	118	66	75	–
Cross-Site Request Forgery	226	195	207	209	76	114	–
Insufficient Transport Layer Protect	94	95	83	64	97	111	–
Abuse of Functionality	321	283	243	233	174	171	–
HTTP Response Splitting	751	188	228	73	155	27	–
Predictable Resource Location	674	53*	328*	120	3*	73	2
Brute Force	247	239	174	183	344*	149	–
URL Redirector Abuse	189	104	148	113	115	141	–
Insufficient Authorization	182	21	198	99	89	143	–
Fingerprinting	144	202*	155	118	0*	63*	–
Session Fixation	240	119	255	143	–	117	–
Directory Indexing	–	–	0*	41*	–	119	–

*Limited Amount of data available

Source: WhiteHat Security Stats Report 2015

HonestDollar | Goldman Sachs

Security Incidents

Table 1.

Number of security incidents by victim industry and organization size, 2015 dataset.

Industry	Total	Small	Large	Unknown
Accomodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31–33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (53)	159	102	20	37
Trade (42)	15	3	7	5
Transportation (48–49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

Source: Verizon DBIR – 2016

Monitoring

Figure 9.

Breach discovery methods over time, (n=6,133).

Legend:
- Law Enforcement
- Fraud Detection
- Third Party
- Internal

MAY 2015
Healthcare
Data breaches cause problems for insurance providers

JUN
OPM Breach
21 million victims

JUL
Social Media Company
100 GB of stolen data in high-profile compromise

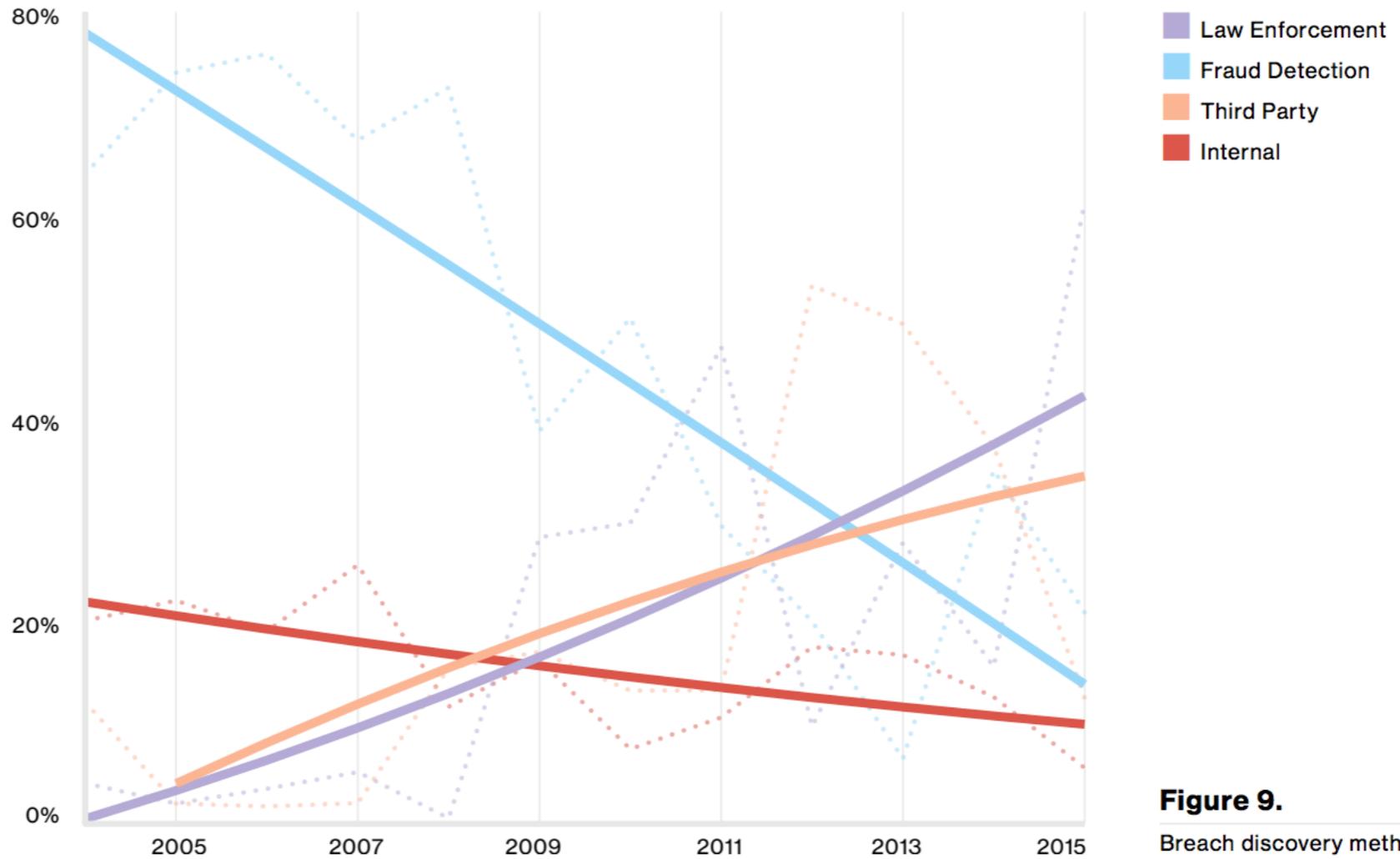AUG 2015
Ubiquiti
$47 million business email compromise

HonestDollar | Goldman Sachs

Continuous Integration
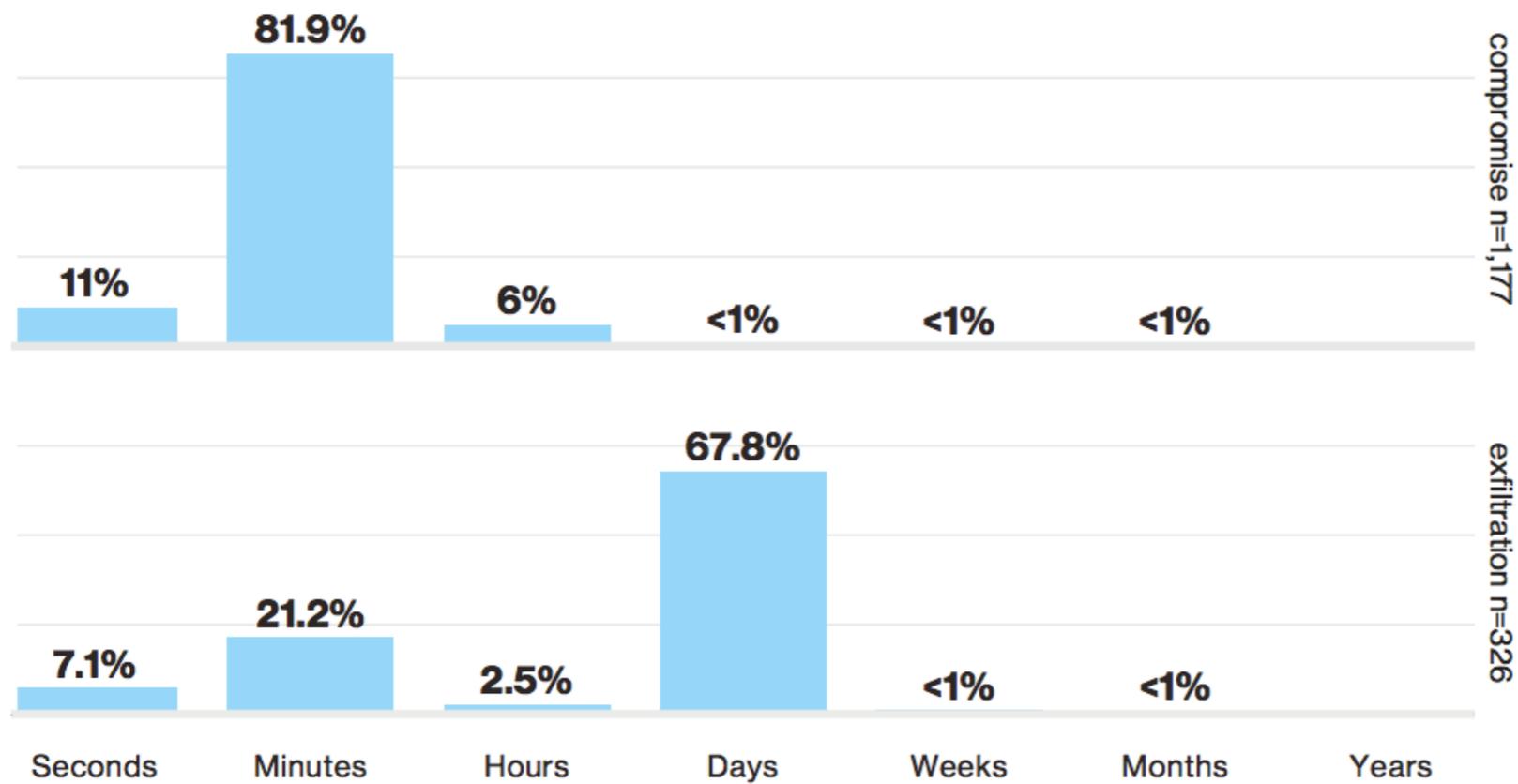
Figure 7.

Time to compromise and exfiltration.

Thank You