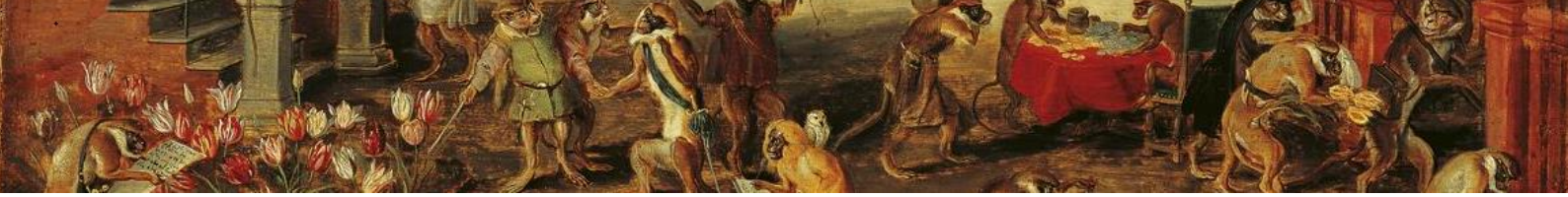


AMD confirms CTS vulnerabilities, downplaying to avoid the financial implications.

Discoveries by CTS Labs' research into AMD flaws eliminate AMD's competitive advantage in enterprise server segments and the company's price competitiveness in retail aspects can no longer be justified.

The company's rhetoric is that this is a non-issue hinges on the non-argument that administrator access must be established in order to exploit the vulnerabilities identified by CTS. This is short-sighted as the surrounding statement that *most* hackers will not have the know-how to exploit these vulnerabilities.

As detailed by CTS[1]:

> *"Attackers think of machines not as individual nodes but as part of a network. Gaining local administrative access on a compromised computer inside an organization is easy for attackers. The challenge is moving laterally from there to other machines and maintaining access for the future. That is exactly what these vulnerabilities provide."*

CTS have recently released a video showing the exploitation of AMD's vulnerabilities to completely circumvent Windows Credential Guard and obtain decrypted passwords. AMD management specifically highlighted Windows Credential Guard as a key obstacle to the execution of CTS Labs' identified exploits.

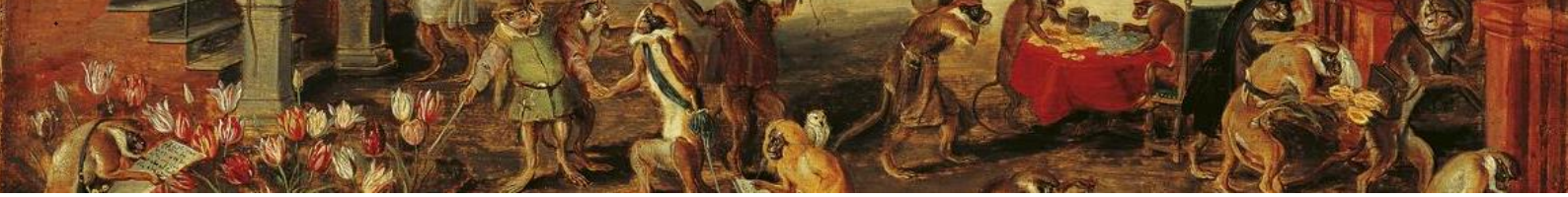
The video can be viewed in full here: https://www.youtube.com/watch?v=8YQaWIWbzhI&feature=youtu.be

Viceroy believes the practice of **giving AMD discretion as to when, if and how it reports its own vulnerabilities facilitates poor corporate disclosure and keeps stakeholders in the dark**. This is **not** how free financial markets operate for a reason and is validated by the SEC's most recent statement[2] relating to cybersecurity flaws: we would similarly not give fraudulent companies the discretion as to if and when they inform their investors they are a fraud.

- **Ryzen and Epyc processors facilitate tremendous freedom of access to customer's data –**The identified vulnerabilities in AMD's EPYC and Ryzen processors give hackers the ability to entrench malware at the hardware level, making them **virtually *undetectable and untouchable*** by security products. By abusing these vulnerabilities at the Secure Processor level, malware characteristics **can give hackers *unlimited control* over entire networks.** None of the vulnerabilities identified by CTS, both firmware and hardware, require physical access to computers to be exploited. The continued sale of these processors puts customers at significant risk.
- **The security protocols that AMD have been promoting put customers at unacceptable risk to vulnerabilities identified by CTS –** We expect AMD cloud customers including Microsoft Azure, Baidu, DellEMC and TenCent will flee in the short term given the serious nature of chip flaws. AMD is unlikely to be trusted in this space again.
- **One Ryzen chip could endanger an entire enterprise network –** Vulnerabilities identified in the Ryzen chip allow hackers to perform credential dumps on infected Ryzen workstations even if the latest security mitigations are employed. Malware can quickly spread to other workstations throughout enterprise networks, regardless of whether they use a Ryzen chip or Intel. No prudent CISO or CTO will risk their network or their security by buying a Ryzen chip over more secure competitors.

This report expands on the financial impact of the CTS Labs vulnerabilities, specifically the impact of future earnings and possible legal liabilities that Viceroy believes will arise against the company. Viceroy have appointed lawyers to assess the reliability of the security claims made by AMD considering the basic level flaws that have been identified.

[1] https://www.techpowerup.com/242386/cts-labs-responds-to-a-techpowerup-technical-questionnaire
[2] https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21



Important Disclaimer – Please read before continuing

This report has been prepared for educational purposes only and expresses our opinions. This report and any statements made in connection with it are the authors' opinions, which have been based upon publicly available facts, field research, information, and analysis through our due diligence process, and are not statements of fact. All expressions of opinion are subject to change without notice, and we do not undertake to update or supplement any reports or any of the information, analysis and opinion contained in them. We believe that the publication of our opinions about public companies that we research is in the public interest. We are entitled to our opinions and to the right to express such opinions in a public forum. You can access any information or evidence cited in this report or that we relied on to write this report from information in the public domain.

To the best of our ability and belief, all information contained herein is accurate and reliable, and has been obtained from public sources we believe to be accurate and reliable, and who are not insiders or connected persons of the stock covered herein or who may otherwise owe any fiduciary duty or duty of confidentiality to the issuer. We have a good-faith belief in everything we write; however, all such information is presented "as is," without warranty of any kind – whether express or implied.

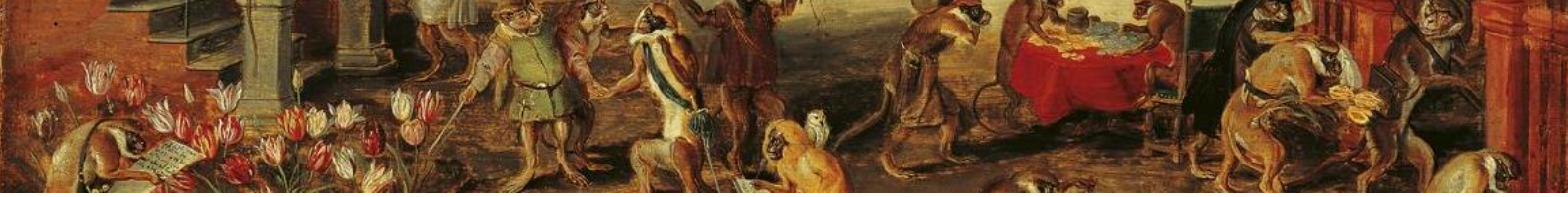
In no event will we be liable for any direct or indirect trading losses caused by any information available on this report. Think critically about our opinions and do your own research and analysis before making any investment decisions. We are not registered as an investment advisor in any jurisdiction. By downloading, reading or otherwise using this report, you agree to do your own research and due diligence before making any investment decision with respect to securities discussed herein, and by doing so, you represent to us that you have sufficient investment sophistication to critically assess the information, analysis and opinions in this report. You should seek the advice of a security professional regarding your stock transactions.

This document or any information herein should not be interpreted as an offer, a solicitation of an offer, invitation, marketing of services or products, advertisement, inducement, or representation of any kind, nor as investment advice or a recommendation to buy or sell any investment products or to make any type of investment, or as an opinion on the merits or otherwise of any particular investment or investment strategy.

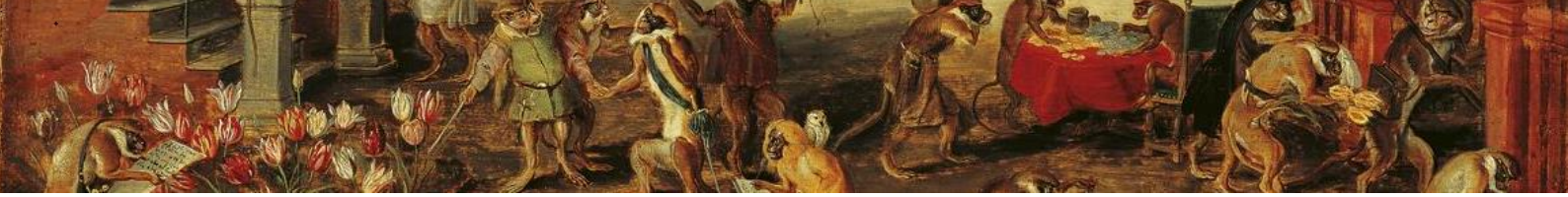
Any examples or interpretations of investments and investment strategies or trade ideas are intended for illustrative and educational purposes only and are not indicative of the historical or future performance or the chances of success of any particular investment and/or strategy.

As of the publication date of this report, you should assume that the authors have a direct or indirect interest/position in all stocks (and/or options, swaps, and other derivative securities related to the stock) and bonds covered herein, and therefore stand to realize monetary gains in the event that the price of either declines.

The authors may continue transacting directly and/or indirectly in the securities of issuers covered on this report for an indefinite period and may be long, short, or neutral at any time hereafter regardless of their initial recommendation.



Contents



Projected loss of Revenues

AMD has two reporting segments related to its products: Computer and Graphics; and Enterprise, Embedded and Semi-Custom.

before interest, other income (expense), net, income taxes and equity loss of investee. These performance measures include the allocation of expenses to the operating segments based on management's judgment. The Company has the following two reportable segments:

- the Computing and Graphics segment, which primarily includes desktop and notebook processors and chipsets, discrete and integrated graphics processing units (GPUs), professional GPUs and licensing portions of its IP portfolio; and
- the Enterprise, Embedded and Semi-Custom segment, which primarily includes server and embedded processors, semi-custom System-on-Chip (SoC) products, development services, technology for game consoles and licensing portions of its IP portfolio.

Figure 1 Extract of AMD 2017 Annual Report

AMD has been historically reluctant to provide further detail on revenues and growth of particular products or product categories within these segments. As such Viceroy and other analysts have had to make educated guesses of the composition and performance of particular products, for example, GPUs.

The product lines affected by the vulnerabilities of CTS labs are spread throughout these two operating segments.

Revenues derived from Enterprise, Embedded and Semi-Custom segment

We believe that revenues from AMD's Enterprise, Embedded and Semi-Custom segments will fall at least 88% based on the heavy concentration of the segment's sales on two customers.

The extent of the vulnerabilities and the difficulty and impracticality of patches we believe make the products unpurchaseable at a commercial level. Any competent Chief Information Security Officer (CISO) or Chief Technology Officer (CTO) would not willingly subject their businesses to unnecessary risk. That is their job.

The sellside currently value AMD on either a sale/EV or future earnings multiple basis. The loss of this service line would make future earnings unattainable for the foreseeable future.

According to AMD's 2017 annual report, the company's two top customers made up 38% of revenue and consisted of products in the Enterprise, Embedded and Semi-Custom segments.

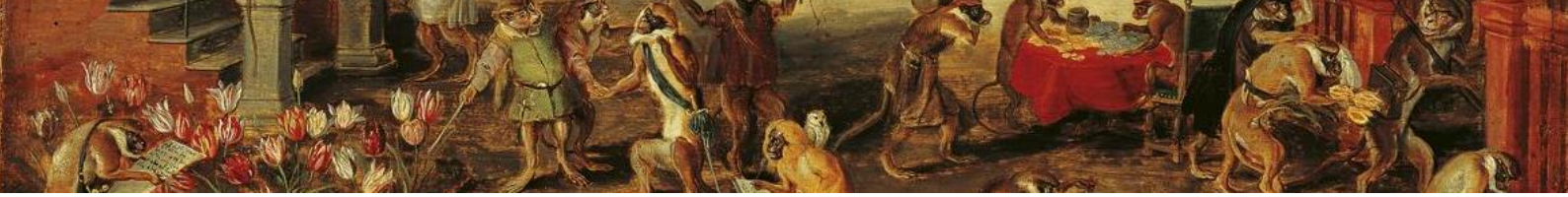
The following table summarizes sales to major customers that accounted for at least 10% of the Company's consolidated net revenue for the respective years:

	2017	2016	2015
Customer A	23%	33%	31%
Customer B	15%	16%	18%
Customer C	6%	10%	8%

Sales to customers A and B consisted of products from the Company's Enterprise, Embedded and Semi-Custom segment and sales to customer C consisted primarily of products from the Company's Computing and Graphics segment.

Figure 2 Extract of AMD 2017 Annual Report

This figure amounts to roughly US$2.025B, and represents ~88% of the Enterprise, Embedded and Semi-Custom segment's revenue.



The following table provides a summary of net revenue and operating income (loss) by segment for 2017, 2016 and 2015.

	2017	2016	2015
		(In millions)	
Net revenue:			
Computing and Graphics	$ 3,029	$ 1,967	$ 1,805
Enterprise, Embedded and Semi-Custom	2,300	2,305	2,186
Total net revenue	$ 5,329	$ 4,272	$ 3,991
Operating income (loss):			
Computing and Graphics	$ 147	$ (238)	$ (502)
Enterprise, Embedded and Semi-Custom	154	283	215
All Other	(97)	(417)	(194)
Total operating income (loss)	$ 204	$ (372)	$ (481)

Figure 3 Extract of AMD 2017 Annual Report

While further details are undisclosed, the nature of the Enterprise, Embedded and Semi-Custom segment products suggests customers A and B are at a significant risk from the vulnerabilities disclosed by CTS Labs. Accordingly we expect them to discontinue business with the company given the many alternatives available on the market, resulting in the segment's revenue falling by at least 88%.

On a Sales/EV multiple of 2.71 (based on sell side consensus target price per Bloomberg Terminal), the loss of 88% of this segment line represents a 27% downside from the current price.

Revenues derived from Computing and Graphics

We make a preliminary note that AMD's Computing and Graphics segment reporting line acts as a "catch-all" between products with very separate markets, making it extremely difficult for stakeholders to gauge actual business unit performance of the segments affected by the CTS Labs vulnerabilities.

Sales in this segment include:

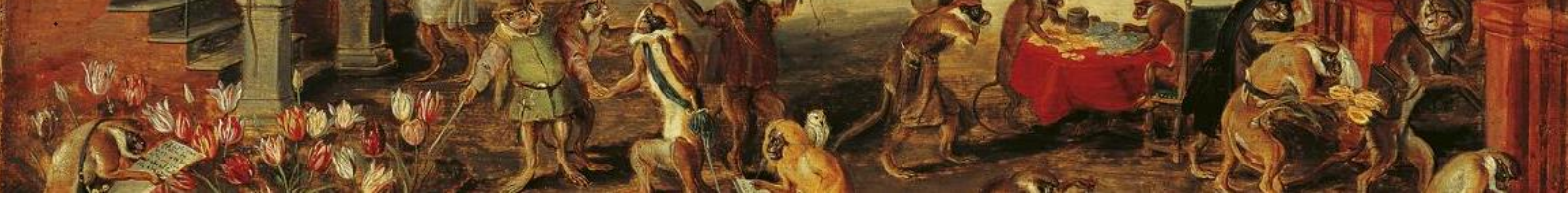
- **GPUs -** We expect flat/negative growth from GPU sales as cryptocurrency miners substantially transition from GPUs to Application-Specific Integrated Circuits (ASICs), which are designed to mine far more efficiently. Major ASIC players such as Bitmain are speculated to release Etherium ASIC hardware later this year and Samsung has also confirmed its intention to enter the cryptocurrency mining space[3].
  Readers should note that AMD management have refused to corroborate or comment on analyst questions regarding GPU sales as a percentage of the Computing and Graphics segment, in particular cryptocurrency related GPU sales.

> "Management did not comment on our attempt to quantify AMD's cryptocurrency sales last quarter, but was sympathetic our notion that the cryptocurrency risk is lower than 2014 due to the emergence of a commercial cryptocurrency mining market which appears more stable (and to which it sells crypto-specific GPUs directly)," he wrote.

Figure 4 Extract from CNBC.com article "AMD shares to surge on its cloud computing chip share gains: Analyst"[4]

However, AMD CEO Lisa Su claimed in the company's' Q4 2017 earnings call that an estimated 33% of the year's growth in the Computing and Graphic segment was attributable to cryptocurrency gains.

[3] https://techcrunch.com/2018/01/31/samsung-confirms-asic-chips/
[4] https://www.cnbc.com/2017/09/13/amd-shares-to-surge-on-its-cloud-computing-chip-share-gains-analyst.html?view=story&%24DEVICE%24=native-android-mobile



> **Dr. Lisa Su**
>
> Yeah absolutely Mark. So, look on the Computing and Graphic segment, we grew about $140 million sequentially. And if I look at that growth, it was across Ryzen and Radeon. If you look at block chain in particular, our estimates are that it was about a third of the growth, a third of the $140 million. And then the rest of the two thirds are around the GPUs, the other segments of GPUs and Ryzen.

Figure 5 Extract from SeekingAlpha.com transcript of AMD Q4 2017 Earnings Call [5]

Susquehanna analyst Christopher Rolland claimed that the remaining GPU sales were being used 95% of the time for cryptocurrency mining.

> Rolland, who has Neutral ratings on both AMD and Nvidia, cut his price target on AMD to $13 from $15, after concluding that many people are buying GPUs as "**gamers**," but then **using the cards just 5% of the time** to play video games and 95% of the time to mine crypto-currencies.

Figure 6 Extract of Barron's article "AMD, Nvidia: Risk from 'Gamers' Who Are Really Coin Miners, Says Susquehanna"[6]

Conservative, we expect GPUs to consist of ~40% of AMD's Computing and Graphics revenue and for GPU revenue to remain flat as their prices stabilizes due to cryptocurrency miners transition into ASICs.

- **Desktop and notebook processors and chipsets** – We expect AMD's inclusion in retail desktops and notebooks to end imminently, notably with HP and Dell. We believe the flaws identified by CTS eliminate any the benefit of price competitiveness as manufacturers will look to protect their interests.

Accordingly, we expect a combination of flat or declining GPU revenues and a complete end to desktop and notebook processor revenues**. We believe that a 60% short term decline in AMD's Computing and Graphics segment revenues is warranted.**

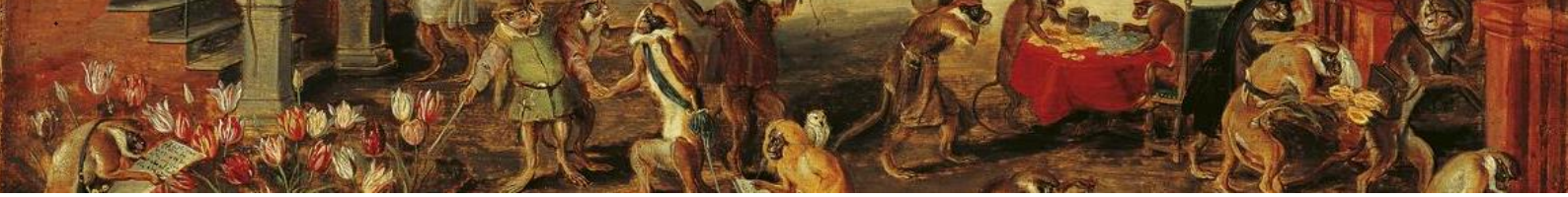
Segment	% of revenue	% drop forecasted	% of revenue lost
Computer and Graphics	56.8%	60.0%	34.1%
Enterprise, Embedded and Semi-Custom	43.2%	88.0%	38.0%
Total			**72.1%**

Collectively, the loss of Enterprise, Embedded and Semi-Custom segment line and 60% of Computing and Graphics revenues represents a 65% downside from the current price on a Sales/EV multiple of 2.71 (based on sell side consensus target price per Bloomberg Terminal).

At this stage, AMD would also be bleeding cash.

[5] https://seekingalpha.com/article/4141484-advanced-micro-devices-amd-ceo-dr-lisa-su-q4-2017-results-earnings-call-transcript?part=single

[6] https://www.barrons.com/articles/amd-nvidia-beware-the-gamers-really-coin-miners-says-susquehanna-1516324763



AMD Valuation Analysis (US$m)		
Share Price		11.26
Shares Outstanding		969
Market Cap		**10,911**
Net Cash	-	210
EV		11,121
Current EV/Sales		**2.09**
Sellside consensus PT		14.87
Consensus EV/Sales		**2.74**
Revenue		5,329
Less: Enterprise solutions (88%)	-	2,024
Less: Computing and Graphics (60%)	-	1,817
Adjusted revenues		**1,488**
Consensus EV/Sales		2.74
Adjusted Price		**3.99**
Downside		65%

Figure 7 Viceroy AMD valuation analysis

Liabilities arising from vulnerabilities

We believe the financial liabilities detailed in the section below will arise as a result of the vulnerabilities CTS exposed and erode AMD's residual value.

AMD faces a raft of potential lawsuits, a reality of competitor Intel after the release of the Meltdown and Spectre exploits. Reuters reported on February 17, 2018 that Intel was facing 32 lawsuits from both customers and shareholders: the city of Providence allegedly filed a lawsuit for US$5B[7].

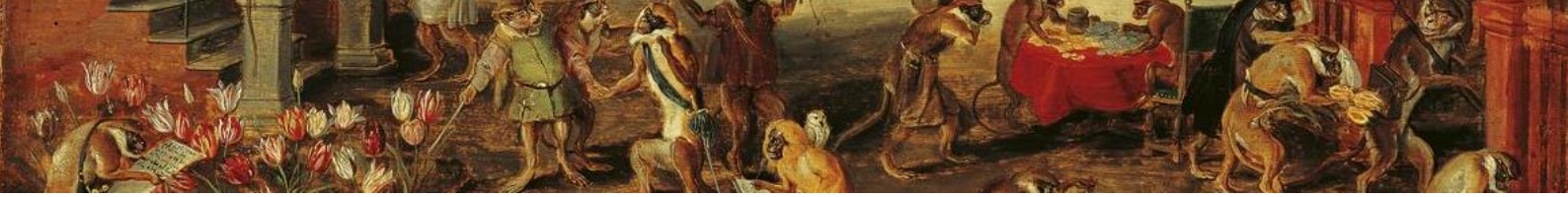
Viceroy believes that in light of the vulnerabilities brought forward by CTS Labs, AMD will face a similar predicament. While the speed and quality of the company's response are mitigating factors, we believe that previous events highlight how the company may not react quickly enough to appease customers.

AMD recently struggled to patch an fTPM flaw identified by google cloud security team member Cfir Cohen. Despite the vulnerability being reported to AMD in September 2017, a spokesperson for AMD claimed that a patch would only be available in January 2018, after the existence of the vulnerability was disclosed according to a 90-day disclosure deadline.

```
Timeline
========
09-28-17 - Vulnerability reported to AMD Security Team.
12-07-17 - Fix is ready. Vendor works on a rollout to affected partners.
01-03-18 - Public disclosure due to 90 day disclosure deadline.
```

Figure 8 Extract from seclists.org post "AMD-PSP: fTPM Remote Code Execution via crafted EK certificate"[8]

[7] https://www.reuters.com/article/us-cyber-intel-lawsuit/intel-hit-with-32-lawsuits-over-security-flaws-idUSKCN1G01KX
[8] http://seclists.org/fulldisclosure/2018/Jan/12



> A firmware update emerged for some AMD chips in mid-December, with an option to at least partially disable the PSP. However, a spokesperson for the tech giant said on Friday this week that the above fTMP issue will be addressed in an update due out this month, January 2018.

Figure 9 Extract from The Register article "Security hole in AMD CPUs' hidden secure processor code revealed ahead of patches"[9]

As such we do not believe the company will react quickly enough to adequately limit associated liabilities. AMD has not yet confirmed that the company was previously unaware of the vulnerabilities identified by CTS Labs.

Vulnerabilities are difficult to patch if patching is possible at all. Product recalls are warranted

CTS identified several vulnerabilities at the hardware level ("logic gates"[10]) which may be not addressable through conventional patching.

From discussions with experts: in the most optimistic of scenario it will take AMD many months to patch vulnerabilities on its devices. If AMD fails to find a workaround in the near term, we believe a full recall in the interest of public safety would be necessary and enforced if need be, as the chips are mostly under 12 months of age.

Voluntary recalls by semiconductor companies are not without precedent. Intel has recalled its Pentium FDIV in 1994 and Cougar Point in 2011[11] at significant cost (US$475M and US$700M respectively). While a deep analysis of these two recalls is beyond the scope of this follow-up, the security flaws in AMD's products are likely to far exceed the defects identified in Intel's processors which necessitated a recall.

We believe that AMD will likely have to recall its Ryzen chips given the scope and severity of the vulnerabilities, the lengthy period to provide patches and work-arounds, and the prospect of more vulnerabilities being discovered.

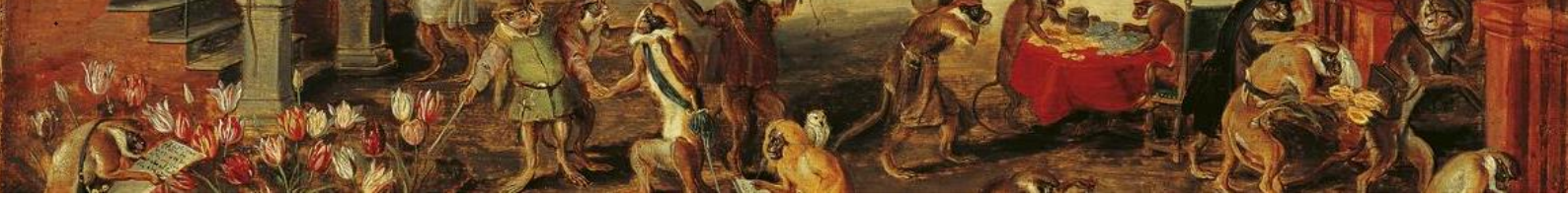
Product liability

A consumer's cause of action is usually based on common law as no federal product liability law exists, except for the False Claims Act. This cause of action revolves around three types of claims:

1. **Breach of warranty**: the ability to seek remedy when a product fails to satisfy express representations, is not merchantable, or is unfit for its particular purpose.[12]
2. **Negligence**: the ability to seek remedy from the defendant for failing to use due care[13]
3. **Strict liability**: the ability to seek remedy for product defect regardless of steps the manufacturer has taken[14]

AMD passed on ASMedia's flawed technology to customers with little in the way of due diligence or effective security review[15,16]

[9] https://www.theregister.co.uk/2018/01/06/amd_cpu_psp_flaw/
[10] https://www.coursera.org/learn/build-a-computer/lecture/Aqrh6/unit-1-3-logic-gates
[11] http://www.tomshardware.com/reviews/cougar-point-recall-sata-6gbps,2896.html
[12] https://www.law.cornell.edu/wex/breach_of_warranty
[13] http://www.courts.state.ny.us/reporter/archives/macpherson_buick.htm
[14] https://www.cozen.com/admin/files/publications/kiernan1954533.pdf?embed
[15] http://www.mondaq.com/unitedstates/x/89684/Product+Liability+Safety/Developments+In+US+Product+Liability+Law+And+The+Issues+Relevant+To+Foreign+Manufacturers
[16] https://www.kreamlaw.com/Frequently-Asked-Questions-Products-Liability.shtml



Warranties[17]

Implied warranties are unspoken and unwritten promises created by state law between a seller or merchant, to their customers. There are two types of implied warranties that occur in consumer product transactions; the implied warranty of merchantability and the implied warranty of fitness for a particular purpose.

1. The implied warranty of merchantability is a merchant's basic promise that the goods sold will do what they are supposed to do and that there is nothing significantly wrong with them. In other words, it is an implied promise that the goods are fit to be sold.
2. The implied warranty of fitness for a particular purpose is a promise sellers make when their customers rely on their advice that a product can be used for some specific purpose.

Based on the ease with which the vulnerabilities in AMD's products are exploitable, we do not believe these products conform with the basic promise of a safe, secure product fit for use, essentially the product claims are likely to be making "false claims."

False claims

Based on the ease with which the vulnerabilities in AMD's products are exploitable, we do not believe AMD's products were sufficiently tested and audited to justify its promotional competitive advantage of superior security. We believe AMD may be subject to legal action under the false claims act.

Regulatory issues may exacerbate problems for AMD

While cybersecurity regulation is still in its nascent stages, it is becoming an increasingly important issue for company boards and management teams. This includes heightened scrutiny by the SEC, who recently released guidelines on timely cybersecurity disclosure following Spectre and Meltdown issues. Do not forget the AMD's initial response was to deny any impact from Spectre and Meltdown. It was only after Intel highlighted the issues for AMD and that they were working with them did AMD admit to the impact of such vulnerabilities.

Homeland security have recently outlined proposals to integrate vetting of cyber-risks to the Government supply chains. We believe that AMD's misleading representation of the security of its products have a wide host of potential regulatory and legal repercussions, including but not limited to product liability issues, warranty protections, and false advertising, which may all lead to various fines and lawsuits.

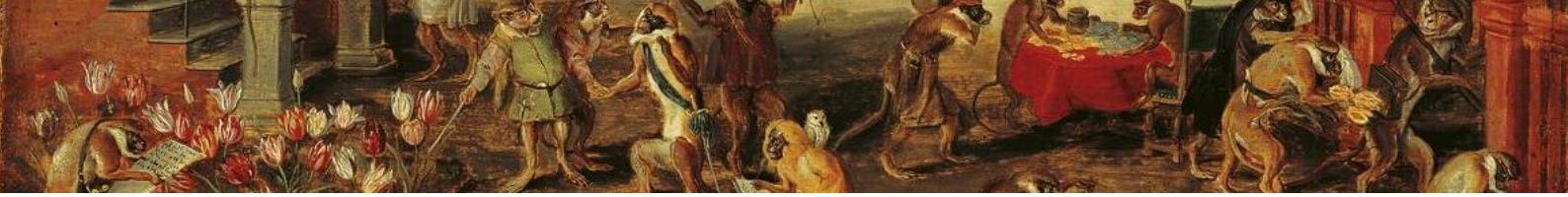
Viceroy believe legal liabilities that will arise for AMD due to discoveries by CTS Labs will exceed any residual value of the company, and accordingly maintain that the Company will file for Chapter 11 in the short term in order to more effectively deal with claims.

AMD possible prior knowledge of issues

Since the publication of our report, a number of sources close to AMD have reached out to Viceroy alleging that all matters identified by CTS had been known to AMD since at least Q4 2017. While we are not able to evaluate this data, AMD should clarify whether or not it was aware of these issues prior to communications by CTS and if so, why the issues not disclosed as per the SEC Guidance[18][19]

[17] https://www.ftc.gov/tips-advice/business-center/guidance/businesspersons-guide-federal-warranty-law

[19] https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21



The issues have also been relayed to Microsoft, US-CERT, Dell, HP, Cisco, Symantec, FireEye, and CrowdStrike. CTS have advised it took CrowdStrike one day to have a good understanding of the issues, and Microsoft Security only two days to be completely on top of the vulnerabilities identified[20].

Given the time frame, this begs the question as to why AMD's customers have not also dismissed claims.

In our opinion, it is irresponsible for AMD to request voting slips for executive remuneration (or hold the meeting altogether) until these issues are addressed, especially given that significant portions of management compensation are bound to top line sales, which we have discussed may bring substantial contingent liabilities.

Insider Sales – Chief Technology Officer insider sales of options after CTS Expose

It is concerning that AMD's CTO has chosen to exercise and immediately sell 150,000 shares of AMD two days after the publication of our report. We find it strange that despite serious flaws being highlighted, AMD's Chief Technology Officer (CTO) sold options during such a critical time.

1. Name and Address of Reporting Person*	2. Issuer Name and Ticker or Trading Symbol	5. Relationship of Reporting Person(s) to Issuer (Check all applicable)
Papermaster Mark D	ADVANCED MICRO DEVICES INC [AMD]	Director: 10% Owner; X Officer (give title below): Other (specify below)
(Last) (First) (Middle): 2485 AUGUSTINE DRIVE	3. Date of Earliest Transaction (Month/Day/Year): 03/15/2018	Chief Technology Officer & SVP
(Street): SANTA CLARA CA 95054	4. If Amendment, Date of Original Filed (Month/Day/Year)	6. Individual or Joint/Group Filing (Check Applicable Line): X Form filed by One Reporting Person; Form filed by More than One Reporting Person
(City) (State) (Zip)		

Table I - Non-Derivative Securities Acquired, Disposed of, or Beneficially Owned

1. Title of Security (Instr. 3)	2. Transaction Date (Month/Day/Year)	2A. Deemed Execution Date, if any (Month/Day/Year)	3. Transaction Code (Instr. 8)		4. Securities Acquired (A) or Disposed Of (D) (Instr. 3, 4 and 5)			5. Amount of Securities Beneficially Owned Following Reported Transaction(s) (Instr. 3 and 4)	6. Ownership Form: Direct (D) or Indirect (I) (Instr. 4)	7. Nature of Indirect Beneficial Ownership (Instr. 4)
			Code	V	Amount	(A) or (D)	Price			
Common Stock	03/15/2018		M		150,000(1)	A	$5.76	1,207,949	D	
Common Stock	03/15/2018		S		150,000(2)	D	$11.38(3)	1,057,949	D	

Table II - Derivative Securities Acquired, Disposed of, or Beneficially Owned (e.g., puts, calls, warrants, options, convertible securities)

1. Title of Derivative Security (Instr. 3)	2. Conversion or Exercise Price of Derivative Security	3. Transaction Date (Month/Day/Year)	3A. Deemed Execution Date, if any (Month/Day/Year)	4. Transaction Code (Instr. 8)		5. Number of Derivative Securities Acquired (A) or Disposed of (D) (Instr. 3, 4 and 5)		6. Date Exercisable and Expiration Date (Month/Day/Year)		7. Title and Amount of Securities Underlying Derivative Security (Instr. 3 and 4)		8. Price of Derivative Security (Instr. 5)	9. Number of derivative Securities Beneficially Owned Following Reported Transaction(s) (Instr. 4)	10. Ownership Form: Direct (D) or Indirect (I) (Instr. 4)	11. Nature of Indirect Beneficial Ownership (Instr. 4)
				Code	V	(A)	(D)	Date Exercisable	Expiration Date	Title	Amount or Number of Shares				
Stock Option Grant	$5.76	03/15/2018		M			150,000	(4)	11/15/2018	Common Stock	150,000	$0	296,993	D	

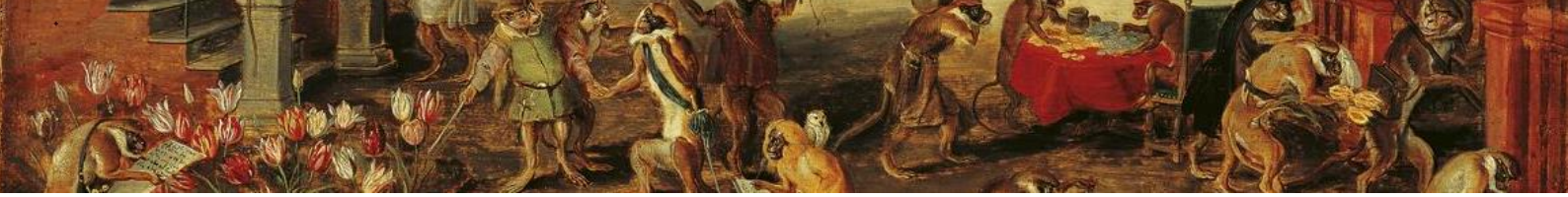
Figure 10 Extract of Form 4: Mark Papermaster dated March 15, 2018[21]

Papermaster's sale of a 150,000 shares is material, especially after the disclosures and concerns raised by CTS Labs. The SEC guidance on the matter, applicable from February 18, 2018, is extremely clear:

> Additionally, directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company. Public

Extract of SEC Statement and Guidance on Public Company Cybersecurity Disclosures[22]

[20] https://www.techpowerup.com/forums/threads/cts-labs-responds-to-a-techpowerup-technical-questionnaire.242386/
[21] https://www.cnbc.com/amp/2018/01/03/amd-rebukes-intel-says-flaw-poses-near-zero-risk-to-its-chips.html
[22] https://www.sec.gov/rules/interp/2018/33-10459.pdf



Similar questions were raised regarding Intel CEO Brian Krzanich's insider sales executed last year in the midst of the Spectre fiasco: Krzanich's sales have been alleged to be illegal.

Of concern is that the SEC Chairman Jay Clayton statement on the aforementioned guidance regarding the sale of stock: a statement heavily applicable to Papermaster's involvement with AMD's attempt to downplay the risks of the vulnerabilities:

> In today's environment, cybersecurity is critical to the operations of companies and our markets. Companies increasingly rely on and are exposed to digital technology as they conduct their business operations and engage with their customers, business partners, and other constituencies. This reliance on and exposure to our digitally-connected world presents ongoing risks and threats of cybersecurity incidents for all companies, including public companies regulated by the Commission. Public companies must stay focused on these issues and take all required action to inform investors about material cybersecurity risks and incidents in a timely fashion.
>
> In 2011, the Division of Corporation Finance issued guidance that provided the Division's views regarding disclosure obligations that relate to cybersecurity risks and incidents. Yesterday, the Commission voted to provide guidance to public companies that reinforces and expands the Division's prior guidance. The guidance highlights the disclosure requirements under the federal securities laws that public operating companies must pay particular attention to when considering their disclosure obligations with respect to cybersecurity risks and incidents. It also addresses the importance of policies and procedures related to disclosure controls and procedures, insider trading, and selective disclosures. I believe that providing the Commission's views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors. In particular, I urge public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives.

Figure 11 Extract of Release by SEC Chairman Jay Clayton February 21, 2018[23]

AMD were aware of the CTS Labs vulnerabilities when Papermaster's sales took place, similar to Intel's CEO Krzanich. We expect the media to take a similarly dim view as to whether these sales could have been illegal.

[23] https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21